Building Blocks for Quantum Computing: The Quantum Mechanics and Mathematics of Qubits and Gates

Special Topics in Computer Science:
Quantum Computing

CSC591/ECE592 – Fall 2018

Building Blocks for Quantum Computing (QC)

OUTLINE

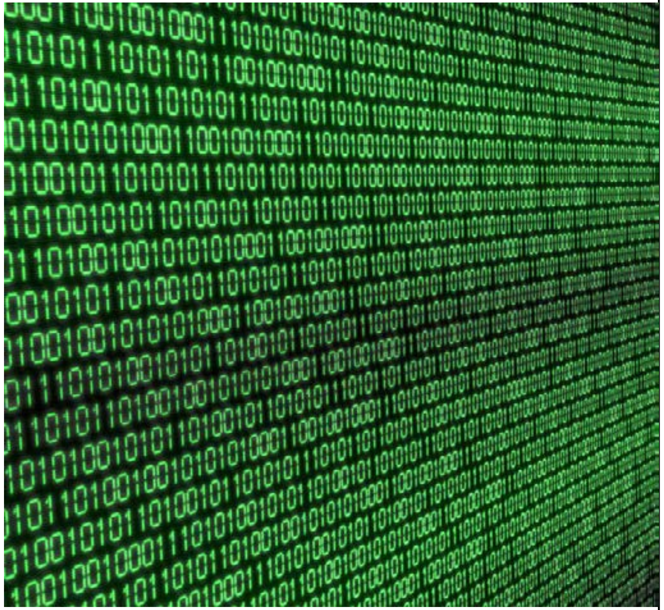
- How is Information Represented on a Classical Computer
- The Quantum Mechanics and Mathematics Needed for QC
  - Linear Algebra Applicable for Quantum Computing
  - Postulates of Quantum Mechanics (QM)
- Basic Concepts of Bits and Qubits
- Building Quantum Gates From Qubits That Obey the Physics Postulates of Quantum Mechanics
- Challenges of Quantum Computing and Summary

Representing Information on a Computer

- Classical computer has two states (“off” and “on”)
- Define two states “0” and “1” (“bits”) that represent the state of a system on a computer in only terms of “0”s and “1”s
- How are these “0”s and “1”s represented in a classical computer
- How are bits transformed in a classical computer when an operation is applied to them

Basic Characteristic of a Classical Computer

- Uses a 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
- CPUs manipulate the classical bits



Single Component Representation

- Identify general rules for transforming the state of a single classical 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 classical bit

The Quantitative Language and Vocabulary of Quantum Computing

Properties of Linear Algebra Required to Describe Quantum Computing Operations

Review Basic Linear Algebra

- 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

- 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; if no vector in the set can be written in this way, then the vectors are said to be linearly independent.

- 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 and every vector in the vector space is a linear combination of this set. In more general terms, a basis is a linearly independent spanning set. A basis is a linearly independent spanning set

Properties and Definitions of a Vector Space

- Vector Space V containing vectors A, B, C must have the following properties
  - 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
  - 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

- 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 liner combination of that set

Dirac Notation

- Many texts use Dirac "ket" notation |a> to denote 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 the row vector $\vec{a}$

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

[#] The **transpose a^T** of a column vector a is a row vector

[#] The **adjoint $a^\dagger$** is the complex conjugate transpose of a column vector a and is sometimes called the Hermitian conjugate

[#] **Unitary matrix U** is a complex square matrix whose adjoint equals its inverse and the product of U adjoint and the matrix U is the identity matrix

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

Dirac Notation

- In Dirac notation a single qubit is written as

  a = α|0> + β|1> $|\alpha|^2 + |\beta|^2 = 1$

  (α and β are complex coefficients)
- α and β are the complex probability amplitudes of measuring the |0> and |1> states
- Pure state basis is represented as $|0>=\binom{1}{0}$ and $|1>=\binom{0}{1}$
- Probability to measure the |0> state is $|\alpha|^2$
- Probability to measure the |1> state is $|\beta|^2$

Examples of Normalized Vectors in Dirac Notation

$$|a\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle] = \frac{1}{\sqrt{2}}\ [\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\ ] = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$|b\rangle = [\ \frac{3}{5}|0\rangle - \frac{4}{5}|1\rangle] = \frac{3}{5}\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \frac{4}{5}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{3}{5} \\ \frac{-4}{5} \end{pmatrix}$$

$$|c\rangle = \frac{3i}{5}|0\rangle - \frac{4i}{5}|1\rangle = \frac{3i}{5}\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \frac{4i}{5}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{3i}{5} \\ \frac{4i}{5} \end{pmatrix}$$

Comment

- Note that |b> and |c> vectors differ by a “phase” which has no analog in classical description of bits

Tensor Product

- The outer product of two coordinate vectors **a** and **b** (represented by $\mathbf{a} \otimes \mathbf{b}$) is a matrix **c** such that the coordinates satisfy $c_{ij} = a_i \, b_j$
- The outer product for general tensors is also called the tensor product
- The tensor product of (finite dimensional) vector spaces A and B has dimension equal to the product of the dimensions of the two factors $\dim(A \otimes B) \dim(A) \text{ x } \dim(B)$

Mathematics of a Tensor Product

- Example: Given 2x2 matrices X and Y

$$X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \qquad Y = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}$$

- The tensor product of $X \otimes Y$ is

$$X \otimes Y = \begin{bmatrix} x_{11} \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} & x_{21} \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} \\ x_{12} \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} & x_{22} \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} \end{bmatrix}$$

Additional Mathematical Tools for QC
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

Postulates of Quantum Mechanics

Design principles for a QC Using the Properties of Quantum Mechanics

- Quantum theory is a mathematical model of the physical world
- The physical world at the quantum level exhibits behaviors that have no analog to our everyday experiences
- It is the physics and mathematical properties and describe the behavior and measurements of quantum mechanical systems that forms the structure required to properly design QC devices, algorithms and programs

Bad News and Good News When Working with QC Systems

- Bad News
  - Applying the physics of quantum mechanics has no classical analog in our everyday experience
  - As a result, our intuition and expected reasoning that is based on those everyday experiences fail us when building systems based on the physics of the quantum world
- Good News
  - Most of the physics and mathematical complexity of QM involves continuous systems in space-time
  - QM of continuous systems are not needed to describe quantum computing systems
  - A quantum computer can be described by discrete systems and discrete (unitary) transformations

Postulates of Quantum Mechanics

- A quantum system can be represented mathematically
  - A unit (orthonormal) vector in the system's state space (Hilbert space) is a state vector that is a complete description of the physical system
  - This complex vector is represented by a linear sum of terms
  - Written in a Dirac bra-ket notation (example$< \psi|$ or $|\phi >$)
- Dirac "ket" notation |a> is denoted by a column vector

$$|a>= \begin{pmatrix} a_1 \\ a_2 \\ : \\ a_n \end{pmatrix}$$

and a Dirac "bra" notation is a row vector with each term complex conjugated $< a| = (a_1^* \quad a_2^* \quad \ldots \quad a_n^*)$

Properties of a Hilbert Space

- Hilbert space is a vector space over the complex numbers with an inner product $<b|a>$
- Hilbert space maps an ordered pair of vectors to the complex numbers with the following properties
  - Positivity $<a|a> > 0$ for $|a> > 0$
  - Linearity $<c|(\alpha|a> + \beta|b>) = \alpha<c|a> + \beta<c|b>$ where α and β are complex constants
  - Skew symmetry $<b|a> = (<a|b>)^*$
- It is complete as expressed by the norm $||a|| = (<a|a>)^{1/2}$
- Every isolated system has an associated complex vector space with an inner product that is the state space of the system

Basis Vectors

- A set of elements in a vector space V is called a basis (or a set of basis vectors) if the vectors are linearly independent and every vector in the vector space is a linear combination of this set
- A set of basis vectors is defined {e$_i$} i=1,…n written in "bra-ket" notation satisfies $< e_i|e_j >= \delta_{ij}$
- 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

$$< e_k|a >=< e_k|\sum_i \alpha_i \, e_i >= \sum_i \alpha_i < e_k|e_i >= \alpha_k$$

$$a = \sum_i e_i < e_i|a >$$

Postulates of Quantum Mechanics

Dynamics - Time Evolution of a QM 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

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

Postulates of Quantum Mechanics
Dynamics - Time Evolution of a QM System

- Expand the Hamiltonian [$1-iH(t) = U(t+dt, t)$]
  - – Expansion (to 1st order) is the time evolution Hamiltonian that describes the system
  - – $H(t)$ has dimensions of energy (expressed as a matrix)
  - – $H(t)$ is self-adjoint because it satisfies $U^\dagger U=1$
- Some definitions

The transpose a^T of a column vector a is a row vector
The adjoint $a^\dagger$ is the complex conjugate transpose of a column vector a and is sometimes called the Hermitian conjugate
Unitary matrix U is a complex square matrix whose adjoint equals its inverse and the product of $U^\dagger$ and the matrix U is the identity matrix $U^\dagger U = U^{-1} U = 1$

Postulates of Quantum Mechanics

Measurements on a Quantum Mechanical System

- Quantum measurements are the result of operators $\mathbb{Q}$ acting on the state space of the system being measured
  - A quantum system in a state |a> before a measurement will have a probability of measuring an expectation value "x" given by P(x)=<a| $\mathbb{Q}_x^\dagger \mathbb{Q}_x$ |a>
  - The state of the system after the measurement is

$$\frac{\mathbb{Q}_x|a>}{\sqrt{< a|\mathbb{Q}_x^\dagger \mathbb{Q}_x|a >}}$$

  - The operator $\mathbb{Q}$ satisfies the completeness relation

$$\sum_x \mathbb{Q}_x^\dagger \mathbb{Q}_x = I$$

(i.e. the probabilities sum to one $\sum_x P(x) = I$)

Postulates of Quantum Mechanics

Measurements on a Quantum Mechanical System

- The measurement of an observable "X" prepares an eigenstate of "X" and the observer discovers the value of the corresponding eigenvalue
- If the quantum state prior to measurement is |a> then the measured value a_n has a probability of occurrence of

$$\text{Prob}(a_n)=||E_n|a>||^2=<a|E_n|a>$$

- If a_n is the measured result then the normalized quantum state immediately after measurement is

$$\frac{E_n|a>}{||E_n|a>||}$$

Postulates of Quantum Mechanics

Measurements on a Quantum Mechanical System

- If many identically prepared systems are measured each described by the state |a> then the expectation value of the outcomes is

$$< a >\equiv \sum_n a_n \,\mathrm{Prob}(a_n) = \sum_n a_n < a|E_n|a >=< a|A|a >$$

- There is an additional property of quantum mechanical measurement constraint called the No Cloning Theorem
- The theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state and that will be discussed later in the lecture

Postulates of Quantum Mechanics

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 $H_A \otimes H_B$

The Properties of Quantum Mechanics Summary

- Quantum mechanics of a closed quantum system can be described in terms of
  - Linearity
  - Reversibility
  - Unitarity – mathematical completeness describing quantum states
  - Hermiticity – real eigenvalue measurements
  - Dynamical evolution of a quantum mechanical system
  - Composite Properties

Basic Concepts of Classical Bits and Quantum Mechanical Qubits

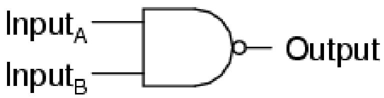
Classical Bits

- Classical bit will be in a state defined by the values of either “0” or “1”
- Properties of classical bits can be used to construct classical logic gates

Classical Logic Gates

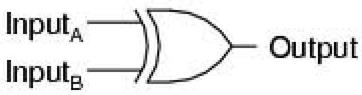
- There are several well known logic gates
- **PROBLEM:** None of these gates operate under the quantum mechanical reversibility requirement

NAND gate



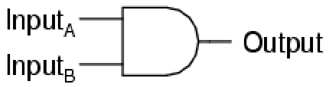
A	B	Output
0	0	1
0	1	1
1	0	1
1	1	0

Exclusive-OR gate



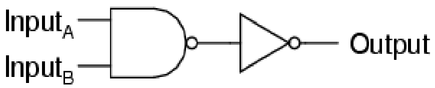
A	B	Output
0	0	0
0	1	1
1	0	1
1	1	0

AND gate

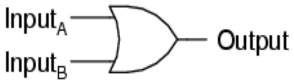


A	B	Output
0	0	0
0	1	0
1	0	0
1	1	1

Equivalent circuit

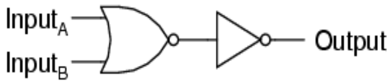


OR gate



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

Equivalent circuit



- The classical NOT gate is reversible but the AND, OR and NAND gates are not

The Classical Gate's Shortcomings for Use as a Quantum Gate

- Quantum physics puts restrictions on the types of gates that can be incorporated into a quantum computer
- The requirements that
  - ***A quantum gate must incorporate the linear superposition of pure states that includes a phase***
  - ***All closed quantum state transformations must be reversible***
- These requirements restrict the type of logic gates available for constructing a quantum computer

Quantum Property of Reversibility and Constraints of Gate Operations

- Reversibility can be quantified mathematically through the matrix representation of the logic gate
- The matrix has the property of preserving the length of vectors, (implying that the matrices are unitary, thereby satisfying the Axiom 4 requirement for quantum mechanics)
- For gates represented by a matrix, the unitarity condition is necessary and sufficient for ensuring that pure orthonormal state vectors get mapped to other pure orthonormal state vectors within the Hilbert space
- The *IDENTITY* operation and *NOT* gates are “reversible” (The outcome of the gate can be undone by applying other gates, or effectively additional matrix operations)

Qubits

- A quantum bit (Qubit) will have the possibility of a state value of either a “0” or “1” but can also be in a linear combination of states other than the classical value of either a “0” or “1”
- A qubit can be said to form a superposition state that can be represented by a linear combination of probability amplitudes associated with each component vector describing that state vectors in that Hilbert space
- Qubits can be described by the mathematics of linear algebra and matrices

Mathematics of Qubits

- Quantum Computer
  - 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

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

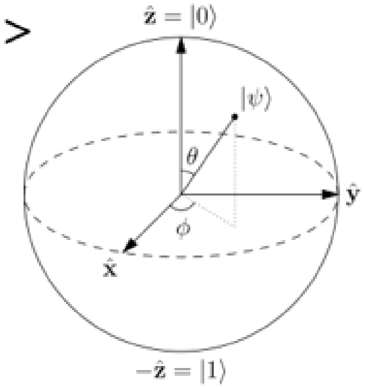
$$| a >= e^{i\gamma}[\cos(\frac{\theta}{2}) | 0 > + e^{i\phi} \sin(\frac{\theta}{2}) | 1 >]$$

  - Design hardware and software based on the properties of qubits and quantum mechanics
  - A QC is made of multiple qubits
  - Output is an expectation value measured through many system samplings
- The classical and QC architectures approach a computational problem from very different perspectives ➔ they each have very different hardware architectures and software environments

Representation for a Single Qubit Bloch Sphere

- From $|\alpha|^2 + |\beta|^2 = 1$ can re-write $|\psi> = \alpha|0> + \beta|1>$

$$|\psi>= e^{i\gamma}(\cos\frac{\theta}{2}|0> + e^{i\phi}\sin\frac{\theta}{2}|1>\Big)$$

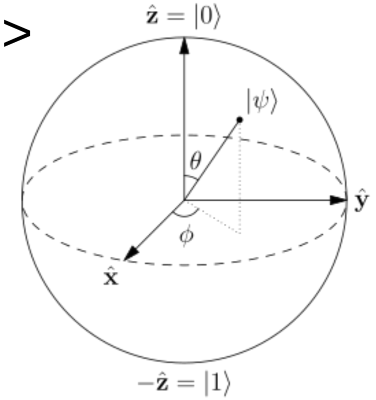


- This representation is visualized by states that lie of the surface of a sphere (Bloch Sphere)

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

Representation for a Single Qubit Bloch Sphere

- From $|\alpha|^2 + |\beta|^2 = 1$ can re-write $|\psi> = \pm|0> + {}^2\,|1>$



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

- This representation is visualized by states that lie of the surface of a sphere (Bloch Sphere)

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

Rotation Operators

- Qubit can be altered by rotating the state vector in the Hilbert space
- Construct a mathematical description of rotations
- Given a general exponentiated operator A perform a Taylor series expansion

$$e^{A} = \sum_{k=0}^{\infty} \frac{1}{k!} A^{k}$$

$$e^{-i\sigma\cdot\hat{n}\frac{\phi}{2}} = \cos\left(\frac{\phi}{2}\right)\mathbf{1} - i\sin(\frac{\phi}{2})\sigma\cdot\hat{n}$$

- The $\sigma\cdot\hat{n}$ are 3 useful classes of unitary matrices (rotation operators) when they are exponentiated

Rotation Gates

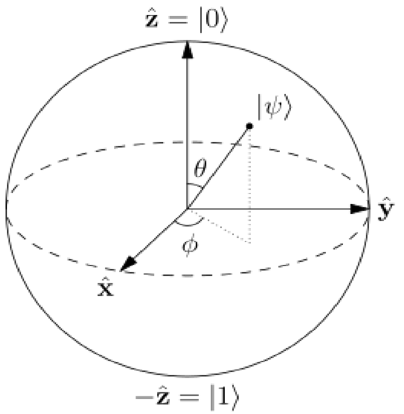
- The matrices σ_x, σ_y and σ_z are associated with rotations about the x, y, and z axes

$$R_{\hat{n}}(\theta) \equiv e^{-i\theta \hat{n}\cdot\frac{\sigma}{2}} = \cos(\frac{\theta}{2})I - i\sin(\frac{\theta}{2})(n_xX + n_yY + n_zZ\Big)$$

- The R gate can specify a rotation in a specific direction by a specific angle

example

$\boxed{R_y(\pi/4)}$



- Reversible one qubit gates can be viewed as rotations in this 3 dimensional representation

Quantum Mechanical Implications for Gates in Terms of Rotations

- Comments
  - These rotation gates often get associated with spins and/or ions interacting with radio frequency pulses or lasers (quantum computing devices)
  - For physics and chemistry problems implemented on a QC these sigma matrices (Pauli Spin Matrices) represent particles that carry a property known as "spin"

Mathematical Construction of 1 Qubit Quantum Gates

- The matrix representation of a quantum gate

$$\sum_i |input_i >< output_i|$$

- 2x2 matrix representation of some 1-bit quantum gates

$$I = |0 >< 0| + |1 >< 1| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$$

$$X = |0 >< 1| + |1 >< 0| = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} + \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$$

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

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

- There are many other 1 qubit gates each having a 2x2 matrix representation that transform an orthonormal state vector in a Hilbert space to another orthonormal state vector in that Hilbert space

Symbols for Single Qubit Gates

Pauli X —X— $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \sigma_x$

Pauli Y —Y— $\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} = \sigma_y$

Pauli Z —Z— $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = \sigma_z$

Pauli Spin Matrices

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

$\frac{\pi}{8}$ —T— $\begin{pmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{pmatrix}$

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

Ancilla Qubit

- During a computation it may be useful to control the state of a bit of information
- Classical computation allows such a process to occur without disturbing the entire computation
- In quantum computation there is no way to deterministically put qubits in a specific prescribed state during the computation without collapsing the wavefunction unless one is given access to qubits whose original state is known in advance
- In a quantum computer states that are known in advance are ancilla qubits
- In quantum computing ancilla qubits are used to store entangled states that enable tasks that would not normally be possible and for quantum error correction

Multiple Qubits

Multi-bit Representation of States

- One cannot do much with one-bit classical gates
- Two states are represented by a pair of orthonormal 2 vectors |a> = $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, |b> = $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- The four states are four orthogonal vectors in four dimensions formed by the tensor products

  |a>⊗|a>, |a>⊗|b>, |b>⊗|a>, |b>⊗|b>
- Two states can also be represented by

  |aa>, |ab>, |ba>, |bb>
- With this construct, can now examine two state gates

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>	|00>
|01>	|01>
|10>	|11>
|11>	|10>

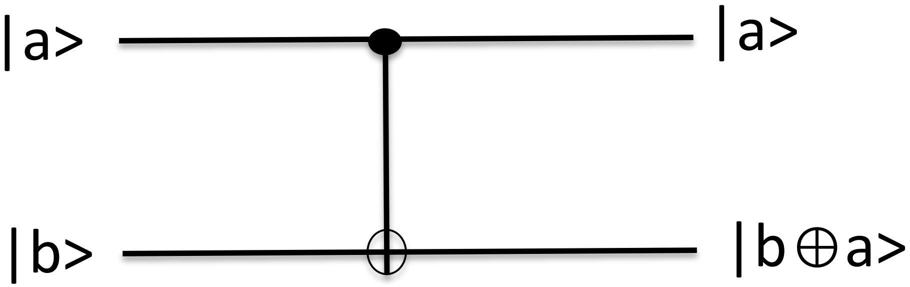
- Can be expressed as $|a, b> \longrightarrow |a, b \oplus a>$
- This type of gate is called a CNOT gate
- The CNOT gate is generally used in quantum computing to generate entangled states

Controlled-NOT Gate

Matrix representation of the CNOT gate

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

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



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

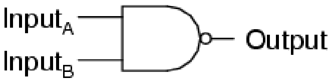
|aa> → |aa>
|ab> → |ab>

|ba> → |bb>
|bb> → |ba>

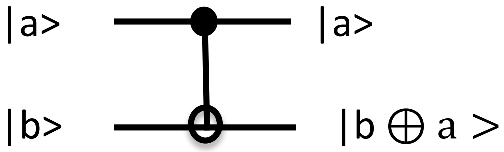
Differences in Basic Computer Logic Structure Between Conventional and a Quantum Computer

- Classical computer uses standard logic gates (NAND, etc.)
- Quantum computer
  - *Differs from a conventional computer because the design must* ***enforce the postulates of quantum mechanics***
  - *Qubits obey the postulates of quantum mechanics -* ***properties of reversibility and unitarity***
  - *Manipulation of the qubits also accomplished through gates*

NAND gate



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



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

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

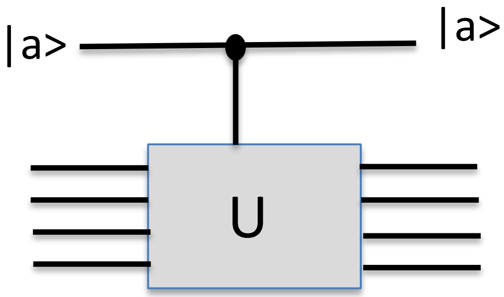
$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

|aa> → |aa> |ba> → |bb>

|ab> → |ab> |bb> → |ba>

Controlled U Gate

- Extension of the controlled CNOT gate
- Given any unitary matrix U can construct a universal gate with the properties
  - Single control qubit
  - N target qubits



- Outputs
  - If the control bit is set to “0” the target bits are unchanged
  - If the control bit is set to “1” then the gate U is applied to the target bits

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> → |00>

  |01> → |01>

  |10> → |1>⊗ U|0> =|1>⊗ (u_{00}|0>+u_{10}|1>)

  |11> → |1>⊗ U|1> =|1>⊗ (u_{01}|0>+u_{11}|1>)

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

- U represents one of the Pauli matrices $\sigma_x \quad \sigma_y \quad \sigma_z$
- Controlled-X, Controlled-Y, Controlled-Z gates

A Reversible Universal Logic Gate

- A controlled SWAP can be defined as

  $F=|0\rangle\langle 0| \otimes \mathbb{1} \otimes \mathbb{1} + |1\rangle\langle 1| \otimes S$

  where S is the usual swap operation

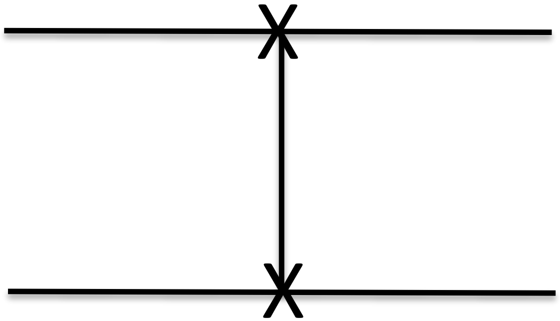
  $S=|00\rangle\langle 00| + |01\rangle\langle 01| = |10\rangle\langle 10| + |11\rangle\langle 11|$
- The number of 1s is conserved between the input and output (conservative reversible logic gate)
- This reversible universal logic gate and can be constructed as a 3-bit gate that performs a controlled swap

Matrix Representation of the SWAP Gate

Truth Table for the SWAP Gate

Input	Output
|00>	|00>
|01>	|10>
|10>	|01>
|11>	|11>

SWAP Gate circuit representation



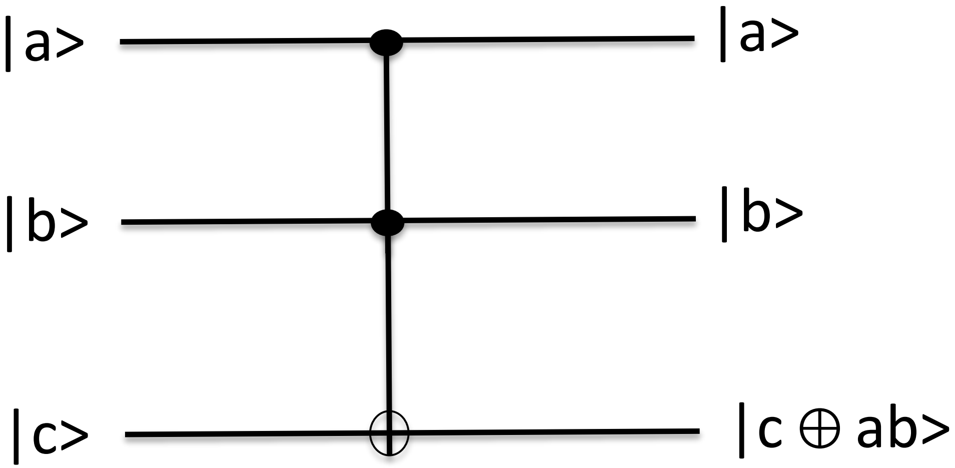
$$U_{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Postulates of Quantum Mechanics and Universal Reversible Gates

- 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
- There is no universal reversible gate with fewer than three inputs
-

Construct Reversible AND and NAND Gates

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

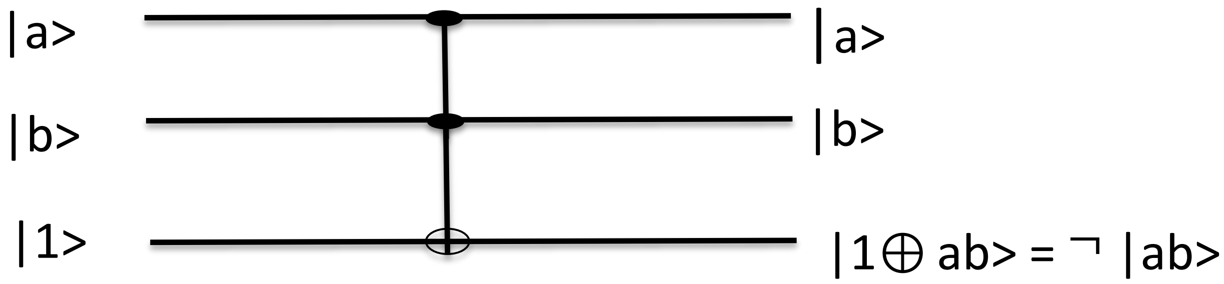


Properties of Toffoli Gates

- 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> and |b>) and target bit |c> is flipped as per the truth table

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

- Toffoli gate and be used to simulate a NAND Gate



Toffoli Gate Truth Table and Matrix

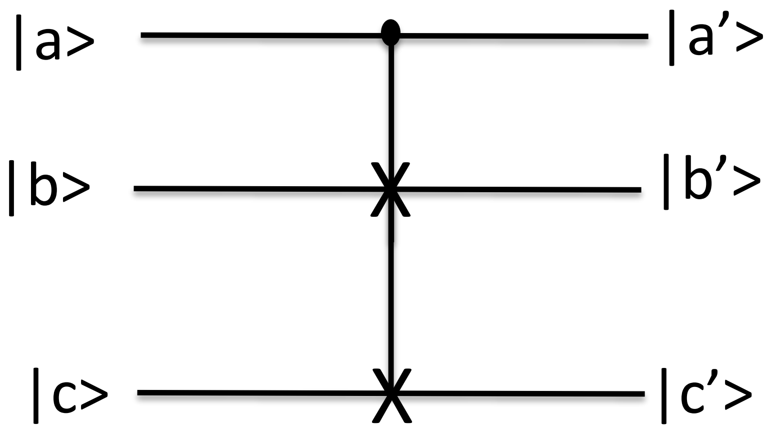
INPUT			OUTPUT		
a	b	c	a’	b’	c’
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	1
1	1	1	1	1	0

$$\left(\begin{array}{cccccc|cc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}\right)$$

X Gate
Pauli σ_x rotation matrix

Fredkin Gate (CSWAP) Properties

- Property that the |c> is the control bit and is not changed by the Fredkin gate
- If |c>=0 then |a> and |b> are unchanged
- If |c>=1 then |a> and |b> are swapped
- The original Fredkin Gate settings can be recovered by applying the Fredkin gate twice



Fredkin Gate Truth Table and Matrix

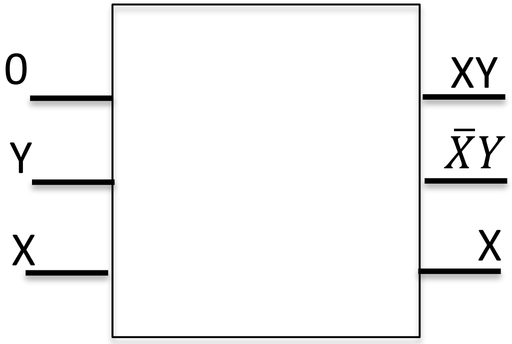
INPUT			OUTPUT		
a	b	c	a’	b’	c’
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	1	0
1	1	0	1	1	1
1	1	1	1	1	1

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

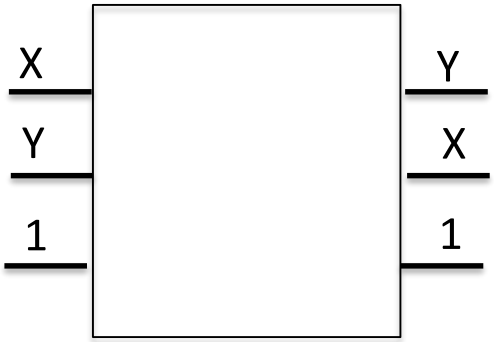
X Gate

Pauli σ_x rotation matrix

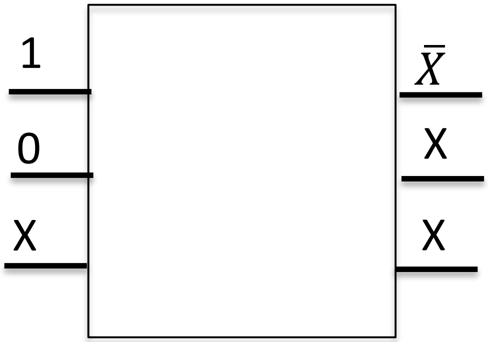
Fredkin Gates Mapping Classically Irreversible Gates



AND Gate



Crossover Gate



NOT Gate

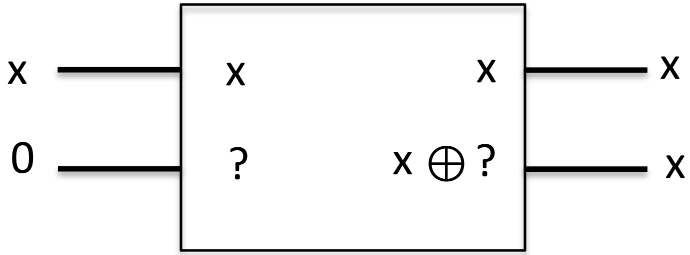
Summary – Quantum Gates Must Adhere to Postulate of Quantum Mechanics

- Any quantum gate that is used to construct quantum computing operations must have a truth table that preserves the following
  - The gates must operate in a complex vector space
  - Complex vector space linear transformations that preserve orthogonality are unitary transformations
  - The dynamics that takes states from t_1 to t_2 are restricted to transformations that preserve this orthogonality and are therefore represented by unitary matrices

Quantum Mechanics Constraints for Quantum Computing Algorithms and Codes

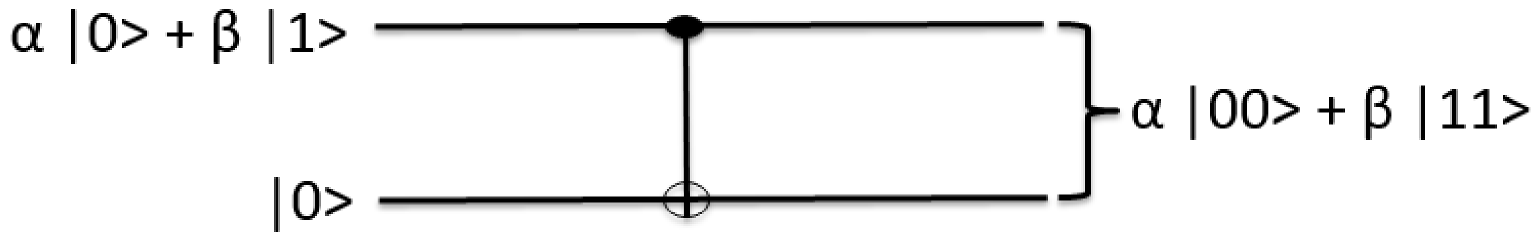
Quantum Information No Cloning Theorem

- A CNOT gate can copy a classical bit in some unknown state “x” and an additional bit initialized to zero and provide an output where both bits are in a state “x”



Quantum Information No Cloning Theorem

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



- Quantum mechanically this output is not possible because the general state vector $|a>|a> = (\alpha |0> + \beta |1>) (\alpha |0> + \beta |1>)$

$$|a>|a> = \alpha^2|00> + \alpha\beta|01> + \beta\alpha|10> + \beta^2|11>$$

- In general $\alpha\beta \neq 0$ and $\beta\alpha \neq 0$ and so the quantum circuit does not copy the part of the state vector with the terms $\alpha\beta|01> + \beta\alpha|10>$
- The no-cloning theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state
- This implies that signal fanout is not permitted

Measurements with a Quantum Computer

Modifications Needed to Map From Classical to Quantum Computing

Measurements

- Measurements in a classical computer are not a factor in the overall computational process
- This is not true for quantum computing
- From axiom 4 of quantum mechanics

  a state evolves over time and is expressed mathematically by a unitary operator (transformation) for a closed quantum mechanics system

- This requires that a quantum gate must be reversible under unitary time evolution

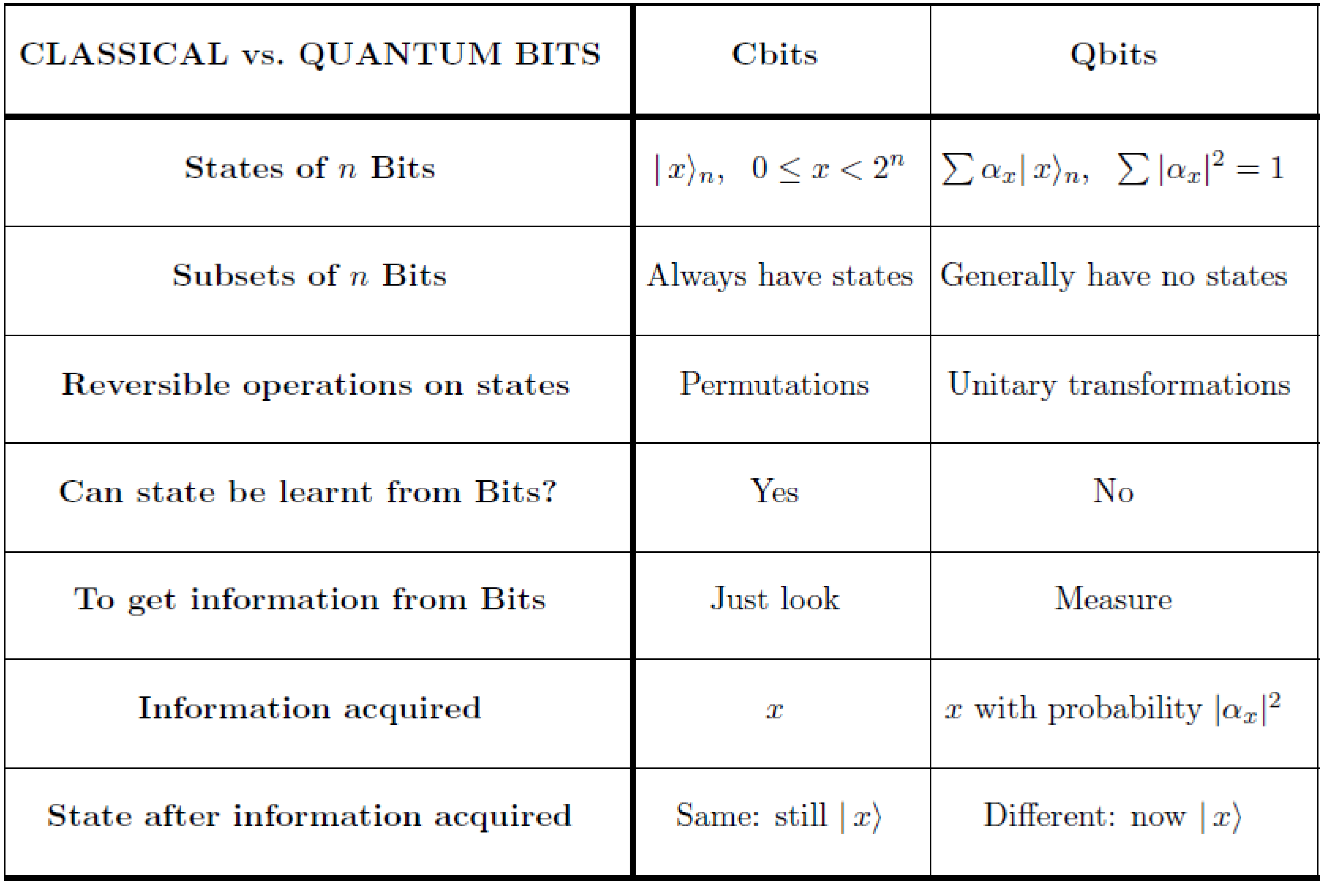
Measurements from Algorithms and Codes Running on a Quantum Computer

- Cannot output results in a similar manner to methods using on a classical computer
- Start with two quantum systems 1 and 2 that can interact with each other
- The act of measurement entangles the two systems quantum mechanically
- Entanglement destroys the superposition of states of system 1 so that some of the relative phases of the system 1 superposition are no longer present
- Result is a collapse of the states of system 1 that cannot be re-constructed

Coding the QM Property of Reversibility into Quantum Gates

- Quantum gates can be represented in matrix formulations
- Quantum gate interactions mathematically described by matrix multiplications that have the property of preserving the length of vectors.
- Such matrices are called “unitary” and are characterized by the equation $A^{\dagger}A = I$
- For gates represented by a matrix, the unitarity condition is necessary and sufficient for ensuring that pure states get mapped to pure states
- 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. This is why such quantum gates are often called “rotations”
- Quantum circuits are constructed from the combined actions of unitary transformations and single bit rotations

Comparison of Classical and Quantum Aspects of Computation *



CLASSICAL vs. QUANTUM BITS	Cbits	Qbits
States of n Bits	$\lvert x\rangle_n, \quad 0 \le x < 2^n$	$\sum \alpha_x \lvert x\rangle_n, \quad \sum \lvert\alpha_x\rvert^2 = 1$
Subsets of n Bits	Always have states	Generally have no states
Reversible operations on states	Permutations	Unitary transformations
Can state be learnt from Bits?	Yes	No
To get information from Bits	Just look	Measure
Information acquired	x	x with probability $\lvert\alpha_x\rvert^2$
State after information acquired	Same: still $\lvert x\rangle$	Different: now $\lvert x\rangle$

* arXiv:quant-ph/0207118v1 19 Jul 2002

Challenges of Quantum Computing

Difficulties in Developing Algorithms for Quantum Computers

- Problem 1
  - If one wants to use quantum mechanics to build a computer, one must understand workings of the quantum world to know how a quantum computer will process a problem
  - However
    - All human experiences rooted in the classical world
    - Human experience and intuition will tend to think of ideas and approaches that are biased toward past experiences and expected behaviors
    - Quantum computers behave in ways that have no classical analog
    - There is no prior direct human experience on which to rely for intuition
- Problem 2
  - 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 better than the classical equivalent

Summary

- The mathematics and quantum mechanics used to construct quantum computing building blocks can be customized and applied to specific specific quantum computer designs and constructions
- The details of how to implement a rotation gates and unitary transformations are specific to each quantum computer architecture
- Future lectures will elaborate on the details of how
  - Gates are constructed on specific quantum computing devices
  - Quantum computing state vectors are manipulated on individual quantum computer architectures

Last Slide