Properties of Linear Algebra Applicable to Quantum Computing

Patrick Dreher

CSC591 / ECE592 – Fall 2019

Outline/Goals for Next Few Lectures

- Course introduction
  - Illustrated how D-Wave hardware can be programed for a specific type of optimization problem
  - One of many different types of problems that may potentially be exploited by quantum computing
- Next few lectures will develop the rigorous mathematical and physics foundations that permit such constructions

Mathematical and Physics Foundations Required to Describe a Quantum Computing System

- Mathematical foundations applicable to quantum computing
- The quantum mechanics postulates that can be described by this mathematics
- Introduce some tools that will allow one to exploit ideas applicable to quantum computing
- With these foundations can now begin to discuss
  - Quantum algorithms and their implementation
  - Using quantum gates to build quantum circuits that can run on quantum computing simulators and quantum computing hardware

Theory of Quantum Mechanics Describes Behavior Observed in a Non-classical World

- Quantum theory is a mathematical model of the physical world at a scale where the size of the observation mechanism is of the same order as the size of the object being observed

- The behaviors of the physical world at the quantum level have no analogs in people's everyday (classical) experiences

- In order to properly design quantum computing devices, algorithms and programs one should
  - Understand the properties and behavior of quantum mechanics and
  - Construct the mathematics that can properly describe it

Building a Rigorous Mathematical Foundation for Describing Quantum Computing

----

Utilizing the Mathematics of Linear Algebra to Represent Quantum Computing Processes *

* The choice of the linear algebra will become clear when we discuss the postulates of quantum mechanics that describe the behavior of the quantum (non-classical) world

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]

Dirac "bra" and "ket" Notation

Dirac "ket" notation |a> represents a column vector $\vec{\boldsymbol{a}}$

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

a Dirac "bra" notation <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

Examples of Normalized Vectors in Dirac Notation

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

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

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

Hilbert Space

- A Hilbert Space is a vector space over the complex numbers with an inner product <b|a>
- The 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|(α|a> + β|b>) = α<c|a> + β<c|b> where α and β are complex constants
  - Skew symmetry <b|a> = (<a|b>)*
- The **adjoint** $a^{\dagger}$ is the complex conjugate transpose of a column vector "**a**" and is sometimes called the Hermitian conjugate
- The space is complete as expressed by the norm

  ||a|| = (<a|a>)$^{1/2}$

Mathematical Representation of Binary States and Superposition

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

Mathematical Representation of 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

Mathematical Representation of 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”

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

Basis Vectors for One Qubit

- In Dirac notation this the vector is represented by

  $a = \alpha|0> + \beta|1>$ $\quad\quad |\alpha|^2 + |\beta|^2 = 1$ (modulus)

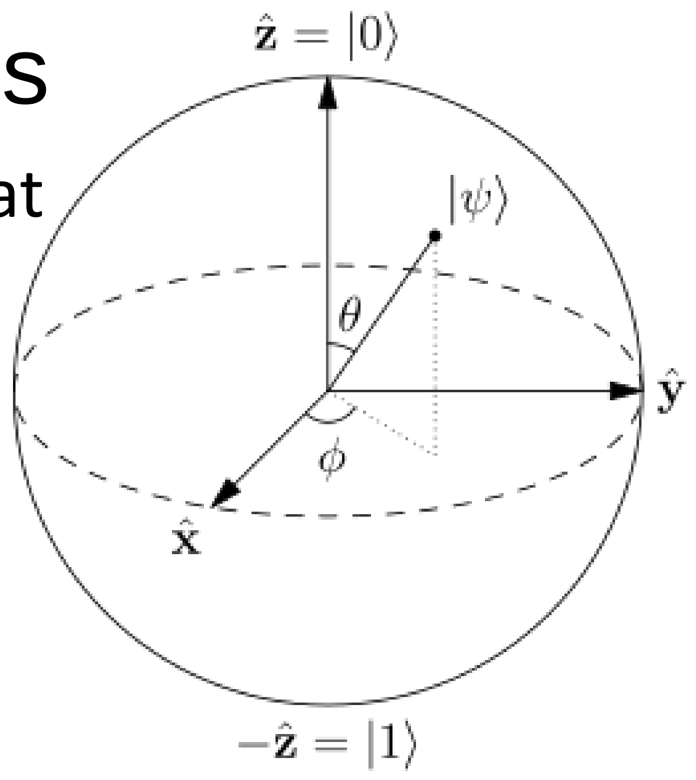
  where α and β are complex coefficients
- α is the probability amplitude of measuring the |0> state and β is the probability amplitude of measuring the |1> state
- Common basis is $|\mathbf{0}>= \begin{pmatrix}\mathbf{1}\\\mathbf{0}\end{pmatrix}$ and $|\mathbf{1}>= \begin{pmatrix}\mathbf{0}\\\mathbf{1}\end{pmatrix}$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

Mathematical Representation of Many Different Basis States

- Represent combination of "0"s and "1"s in a way that many different values can be expressed
- Define $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$
- Can re-write $|a\rangle = \alpha|0\rangle + \beta|1\rangle$ as $|\alpha|^2 + |\beta|^2 = 1$

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

- 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

Combinations of Dirac Bra and Ket

- Calculate an inner product
- Reminder that |0> = $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and |1> = $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Calculate <0|0> (gives an answer of 1 – a single number)

Matrices as Outer Products

If the bra and ket are placed in the opposite order

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

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

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

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

Outer products are a useful mechanism for writing matrices, especially unitaries because they capture state transformations

Matrices as Rotations Acting on Qubits

- 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

Bra and Ket Vectors can be Constructed into Matrices

- **The matrix representation of the expression** $\sum_i |input_i >< output_i|$

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

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

$$Z = |0><0| - |1><1| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$$

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

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

General Statement - Outer Products

- Any matrix can be written purely in terms of its outer products (example)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|$$

- This is a useful formulation to express linear transformations
- Select an original set of basis states (orthogonal) and express in this outer product representation
- Can directly read the effect of the unitary on the basis stated

Properties of Outer Products

- Given vectors **U, V**, and **W** and a scalar c

$(\mathbf{U} \otimes \mathbf{V})^{T} = (\mathbf{V} \otimes \mathbf{U})$

$(\mathbf{V}+\mathbf{W}) \otimes \mathbf{U} = \mathbf{V} \otimes \mathbf{U} + \mathbf{W} \otimes \mathbf{U}$

$\mathbf{U} \otimes (\mathbf{V} + \mathbf{W}) = \mathbf{U} \otimes \mathbf{V} + \mathbf{U} \otimes \mathbf{W}$

$c\,(\mathbf{V} \otimes \mathbf{W}) = (c\,\mathbf{V}) \otimes \mathbf{W} = \mathbf{V} \otimes (c\,\mathbf{W})$

NOTE: The outer product of tensors also satisfies an additional associativity property

$\mathbf{U} \otimes (\mathbf{V} \otimes \mathbf{W}) = (\mathbf{U} \otimes \mathbf{V}) \otimes \mathbf{W}$

Properties of Complex Matrices

If some of the matrix elements are complex there are specific definitions to describe these types of matrices

- **Hermitian Matrix** – A matrix is defined to be a Hermitian matrix if it is a complex square matrix that is equal to its own conjugate transpose—(the element in the i-th row and j-th column is equal to the complex conjugate of the element in the j-th row and i-th column, for all indices i and j)
- **Unitary matrix -** a complex square matrix whose adjoint equals its inverse
  - the product of $U^\dagger$ and the matrix U is the identity matrix
  - Note: a complex square matrix U is unitary if its conjugate transpose is also its inverse U^{-1}) $U^\dagger U = U^{-1} U = I$

State Transformations

- Outer products are a useful mechanism for writing matrices, especially unitaries because they capture state transformations
- Pick an orthogonal set of states (ex pair of $|0>$ and $|1>$) and define a set of states $\{|u_{00}>,|u_{01}> ,|u_{10}>,|u_{11} \}$ to which to which the unitary rotates the original set of orthogonal states

$$U=|u_{00}><00|+|u_{01}><01 +|u_{10}><10| + |u_{11} ><11|$$

- This expression is not unique
- This is a general expression that can be constructed for every possible set of orthogonal input states

State Transformations and Concept of a Phase

- There will be at least one set of orthogonal input states that will take the form of eigenstates of the matrix

$$A = \sum_j \alpha_j \, |e_j >< e_j|$$

where $\alpha_j = \sum_j .\exp(\mathrm{i}\ e_j)$

- The unitary maps each state of the basis $|e_j> \rightarrow \exp(\mathrm{i}\ e_j)|e_j >$
- The transformed state is also a valid basis
  - Implies that the exponential terms must be complex number of magnitude 1
  - The e_j are real numbers
- This formalism also introduces a relative phase when a superposition of these states are combined

Hermitian Matrices and Unitaries

- Hermitian matrices have well defined eigenvalues and eigenstates
- They can be written in the same form as the unitary matrix "A"

$$\mathrm{H} = \sum_j h_j \, |h_j >< h_j|$$

- Hermitian matrices have the property that $H=H^{\dagger}$
- This requirement forces the eigenvalues and eigenvectors to have specific properties

Hermitian Matrices and Unitaries

- Using the property $|h_j>^{\dagger} = <h_j|$ examine the inner product

$$(|h_j><h_j|)^{\dagger} = (<h_j|^{\dagger})(|h_j>^{\dagger}) = |h_j><h_j|$$

- For this to be true the eigenvalues h_j of a Hermitian matrix must be real

Relationship between Unitary and Hermitian

- A unitary matrix (U) has complex exponentials of real numbers for eigenvalues
- Hermitian matrix (H) must have real numbers for eigenvalues
- Based on above 2 statements it is possible to define a Hermitian matrix from every unitary
- The eigenvalues can be related through exponentiation using the definition for exponentiation of a matrix*

$$U=\exp(iH)$$

* An entire family of unitaries can be constructed for each Hermitian

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

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

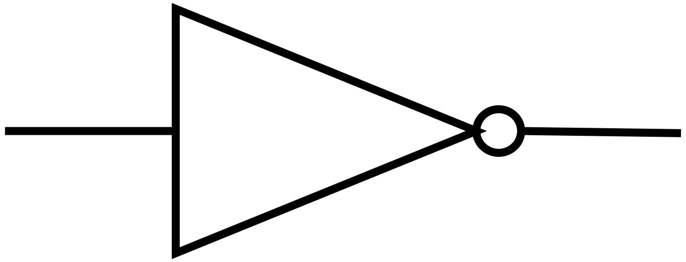
Quantum Computing Gate Operations Under the Constraints of Quantum Mechanics

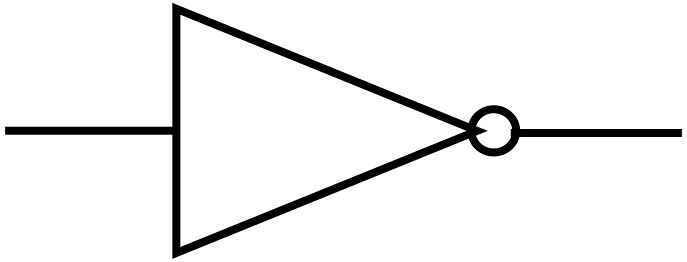
- A quantum gate must incorporate
  - Unitarity - states evolve over time and are expressed mathematically by a unitary operator (transformation) for a closed quantum mechanics system
    - Unitary operator U is expressed as a complex square matrix whose adjoint equals its inverse and the product of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

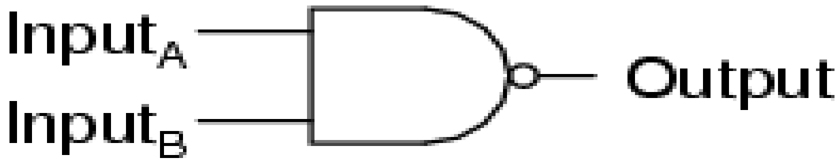
$$|a\rangle \otimes |a\rangle, \ |a\rangle \otimes |b\rangle, \ |b\rangle \otimes |a\rangle, \ |b\rangle \otimes |b\rangle$$

- These states can also be represented by

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

Consequences for Quantum Computing

NAND gate



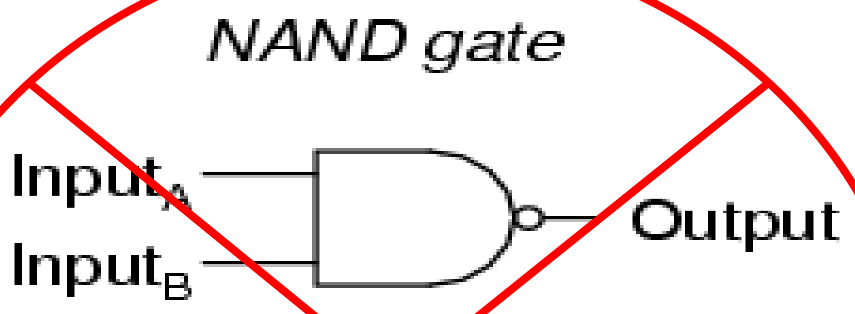
- NAND gate is a fundamental building block for digital computers

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)



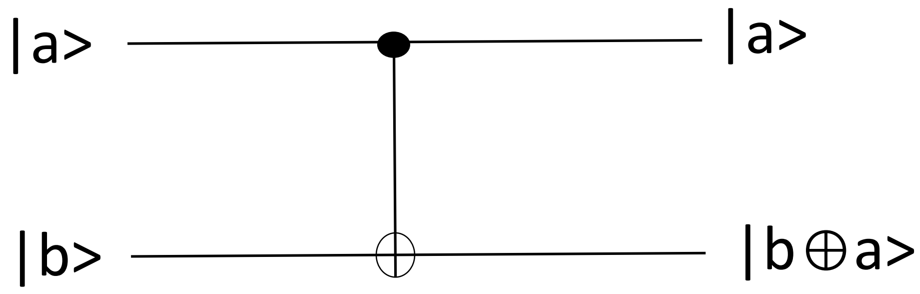
A	B	Output
0	0	1
0	1	1
1	0	1
1	1	0

Design Reversible 2 Qubit Gate
Controlled-NOT Gate
Matrix representation rules for the CNOT gate

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

|aa> → |aa>
|ab> → |ab>

|ba> → |bb>
|bb> → |ba>



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

Identity Matrix → Reversibility

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

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

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

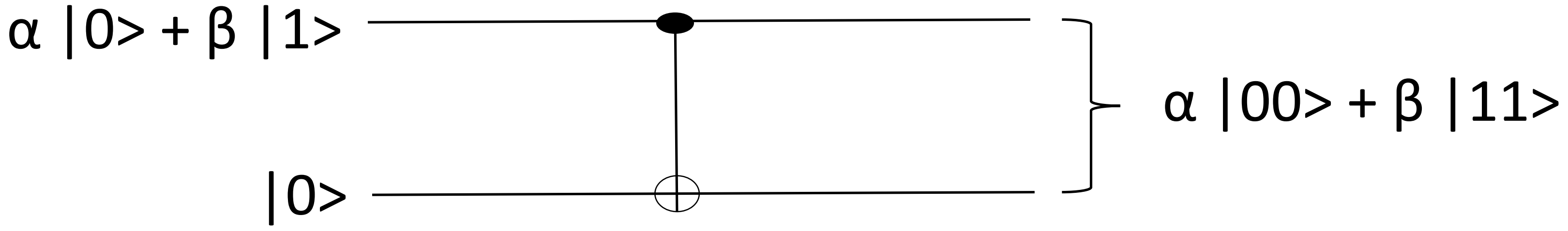
- A two qubit quantum logic gate has a control qubit and a target qubit
- The gate is designed such that if
  - the control bit is set to 0 the target bit is unchanged
  - The control bit is set to 1 the target qubit is flipped

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 α |00> + β |11>

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 $|\alpha >_P$ 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")

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

Can we Duplicate Quantum States For Programming Quantum Computers?

- Need to demonstrate that there is no unitary operator that can be constructed for all states $|\alpha>_P$ and any arbitrary state $|\beta>_Q$

$$U(|\alpha>_P|\beta>_Q) = \exp(i\Upsilon(\alpha, \beta)\ |\alpha>_P|\ \alpha >_Q$$

where ϒ is some real number depending on α and β

- If it is possible to fully copy two states then the combined state should obey the time evolution relations connecting unitary and Hermitian states $U(t) = \exp(iH(t)) \rightarrow = \exp(iH \otimes H)$

Proof of the No Cloning Theorem

- Start with arbitrary pair of states from P and Q ($|\alpha>_P$ and $|\lambda>_Q$) in the Hilbert space

- Because U is unitary

$$<\alpha|\lambda> < \beta|\beta> \equiv < \alpha|_P<\beta|_Q| \lambda >_P|\beta>_Q = < \alpha|_P<\beta|_Q U^{\dagger}U | \lambda >_P|\beta>_Q$$

$$= \exp -i(\Upsilon(\alpha, \beta)- \Upsilon(\lambda, \beta)) < \alpha|_P< \alpha |_Q | \lambda >_P| \lambda >_Q$$

$$\equiv \exp -i(\Upsilon(\alpha, \beta)- \Upsilon(\lambda,\beta)) < \alpha| \lambda >^2$$

No Cloning Theorem

- Assuming that the arbitrary state $|\beta>$ that was picked is normalized then $|<\alpha|\lambda>|^2 = |<\alpha|\lambda>|$
- Can now argue that there are only 2 options
  1. $\alpha = \exp(i\mu)\lambda$ for any μ
  2. α is orthogonal to β
- For any arbitrary states the two options above cannot be the only possible choices *
- This implies that it is impossible to create an identical copy of an arbitrary unknown quantum state

*Cauchy Schwarz inequality states that for all vectors **a** and **b** the following must be true for the inner product space

$$|\langle \mathbf{a},\mathbf{b}\rangle| \leq \langle \mathbf{a},\mathbf{a}\rangle \cdot \langle \mathbf{b},\mathbf{b}\rangle$$

Conclusion - No Cloning Theorem

- There is no unitary operator U on $H \otimes H$ such that for all normalized states $|\alpha>_P$ and $|\beta>_Q$

$$U(|\alpha>_P|\beta>_Q) = \exp(i\Upsilon(\alpha, \beta)\ |\alpha>_P|\ \alpha>_Q$$

Questions