Building Blocks for Quantum Computing PART 1

Patrick Dreher

CSC801 – Seminar on Quantum Computing

Spring 2018

Building Blocks for Quantum Computing

OUTLINE

- Challenges of Quantum Computing
- Basic Concepts of Bits and Qubits
- Properties of Linear Algebra Applicable for QC
- Properties of Quantum Mechanics
- Quantum Circuits
- Quantum Computation - Design of a Quantum Computer

Objectives for this Module

- Build a common based of knowledge because students come from varied backgrounds
- Start with the fundamental representation of information and build a comparison of classical vs quantum formulation
- Outline/review the postulates of quantum mechanics
- Combine the representation of information with the constraints of quantum mechanics to build basic quantum logic circuits
- (Informational lecture)
  - Describe an actual experimental quantum computer and illustrate how it is "programmed" using quantum logic
  - Compare to the D-Wave annealing machine approach
- Get to a point at the end of this module where this information can be used as a backdrop for building quantum algorithms and programs

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 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

Basic Concepts of Bits and Qubits

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

What is the Difference a “Bit” and a “Qubit”?

- Classical bit will be in a state defined by the values of either “0” or “1”
- A quantum bit (Qubit) will also have a state but a qubit can be in a state other than the classical value of either a “0” or “1”
- Qubit can be said to form a superposition state that can be represented by a vector that can be represented as a superposition or linear combination of both a “0” or “1”
- Qubits can be described by the mathematics of linear algebra and matrices

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 $\vec{a}$

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

# The **transpose aᵀ** 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

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

Examples of Normalized Vectors in Dirac Notation

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

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

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

Comments

- Dirac notation
- |b> and |c> vectors differ by a “phase” –no analog in classical description of bits

1-bit Quantum Gates

- The matrix representation of a quantum gate

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

- 2x2 matrix representation of some 1-bit quantum gates
- There are additional 1-bit quantum gates
- Re-visit this in the Quantum Circuit module

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

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

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

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

Symbols for Single Qubit Gates

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

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

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

Pauli Spin Matrices*

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

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

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

* Pauli spin matrices give a hint toward potential designs for a building a quantum computer

Basis vectors 1-bit Quantum Gate

- In Dirac notation this is (± and ² are complex coefficients)

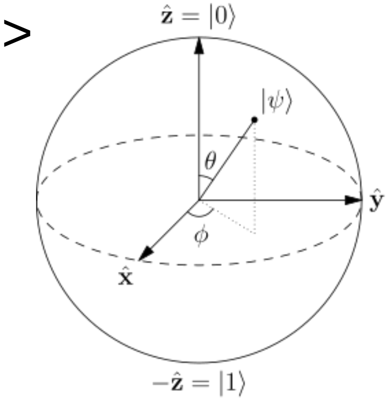
  a = ±|0> + ² |1> |±|^2 + |² |^2 = 1

- ± is the amplitude of measuring the |0> state and ² is the amplitude of measuring the |1> state
- Common basis is $|0>= \begin{pmatrix}1\\0\end{pmatrix}$ and $|1>= \begin{pmatrix}0\\1\end{pmatrix}$
- Probability to measure the |0> state is |±|^2
- Probability to measure the |1> state is |² |^2

Bloch Sphere

- From $|\alpha|^2 + |\beta|^2 = 1$ can re-write |a> = ±|0> + ^{2} |1>

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



- 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

Implications for Gates in Terms of Rotations

- The one qubit states can be represented as points on the Bloch sphere
- The matrices σ_x, σ_y and σ_z are associated with rotations about the x, y, and z axes
- Reversible one qubit gates can be viewed as rotations in this 3 dimensional representation

- Comments
  - These sigma matrices (Pauli Spin Matrices) have a special relationship in physics to particles that carry a property known as “spin”
  - These rotation gates often get associated with spins and/or ions interacting with radio frequency pulses or lasers

Rotation Operators

- Construct a mathematical description of rotations
- Pauli matrices give rise to 3 useful classes of unitary matrices (rotation operators) when they are exponentiated

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

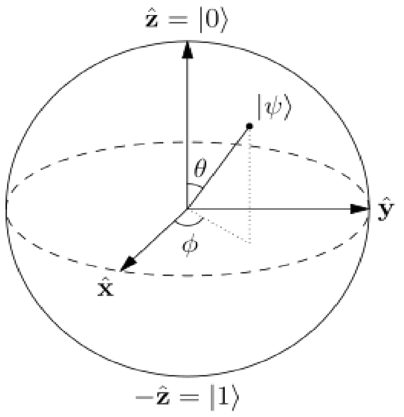
$$e^{-i\sigma\cdot\hat{n}\frac{\phi}{2}} = \cos\left(\frac{\phi}{2}\right)\mathbf{1} - i\sin(\frac{\phi}{2})\sigma\cdot\hat{n}$$

Rotation Gates

- Use the identity

$$R_{\hat{n}}(\theta) \equiv e^{-i\theta \hat{n}\cdot\frac{\sigma}{2}} = \cos(\frac{\theta}{2})I - i\sin(\frac{\theta}{2})(n_x X + n_y Y + n_z Z\Big)$$

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



example

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

Additional Mathematical Tools for QC Outer Product and Tensor Product

- The outer product of two coordinate vectors **a** and **b** (represented by **a** $\otimes$ **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) x dim(B)

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

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

Mapping Logic Gates to the Axioms of Quantum Mechanics

- Constructed both single input and multi input logic gates
- Next - incorporate properties of quantum mechanics to design logic gate building blocks for a quantum computer

Properties of Linear Algebra Applicable for Quantum Computing

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

Review of Linear Algebra

- 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

Computation 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 the lifetime of everyday experiences
- If the properties of quantum mechanics are going to be applied for computations, it is important to understand the properties and behavior of quantum mechanics in order to properly design devices, algorithms and programs

Bad News and Good News

- Bad News
  - – Quantum mechanics is a difficult subject
  - – Our intuition and expected reasoning that is based on our everyday experience fails us when applied to the quantum world
- Good News
  - – Most of the complexity of quantum mechanics deals with continuous systems in space or time
  - – A quantum computer can be described by discrete (2-state) systems and discrete (unitary) transformations

The Properties of Quantum Mechanics

- Quantum mechanics of a closed quantum system can be described in terms of
  - States
  - Observables
  - Measurements
  - Dynamics
  - Rules to combine two systems to obtain a composite system.

Postulates of Quantum Mechanics

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

Postulates of Quantum Mechanics

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

$$i\hbar \frac{d}{dt} |\Psi >= H|\Psi >$$

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

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 $H_A \otimes H_B$

Properties of a Hilbert Space

- It is a vector space over the complex numbers with an inner product <b|a>
- It maps an ordered pair of vectors to the complex numbers with the following properties
  - Positivity <a|a> > 0   for |a> > 0
  - Linearity <c|(±|a> + ^{2} |b>) = ±<c|a> + ^{2} <c|b> where ± and ^{2} are complex constants
  - Skew symmetry <b|a> = (<a|b>)*
- It is complete as expressed by the norm ||a|| = (<a|a>)$^{1/2}$

Last Slide