Introduction to Quantum Computing

(It'll be "Fine Man")

Dr. Randal Allen
Chief Scientist
Lone Star Analysis
2 December 2024

Learning Objectives

- *Identify* the three aspects of quantum information science
- *Describe* the difference between a quantum bit (qubit) and a classical (0/1) bit
- *Explain* how superposition facilitates quantum cryptography and makes quantum computing relevant today
- *Explain* how entanglement facilitates quantum teleportation and makes quantum computing relevant today
- *Tell* the truths about quantum computing myths
- *Identify* different computational models for quantum optimization and their applications
- *Describe* the four families of quantum machine learning and variations of quantum neural networks

Outline

- Introduction
  - Why should I care, quantum info science, physical implementations and challenges, software interfaces, concepts from quantum mechanics and important properties, various computational models, and myths
- Single Qubits and Cryptography
  - The qubit and the Bloch sphere, the property of superposition, operators for gate-based QC, cryptography application
- Multiple Qubits and Teleportation
  - Multiple qubits, the property of entanglement, more operators for gate-based QC, teleportation application
- Quantum Optimization
  - Quantum Unconstrained Binary Optimization (QUBO) and the Ising model, adiabatic QC and gate-based quantum annealing, Quantum Approximate Optimization Algorithm (QAOA), Variational Quantum Eigensolver (VQE), and Grover's adaptive search
- Quantum Machine Learning
  - Quantum Neural Networks (QNN)
- Closing
  - More Information and references

Introduction

Concepts from Quantum Mechanics

Quantum Computing: Who Cares?

Quantum Information Science

Physical Implementations/Challenges

Software Interfaces

Computational Models

Myths

1927 Solvay Conference on Quantum Mechanics

Concepts from Quantum Mechanics

- **Quantization of Matter – Max Planck (photon), Albert Einstein (photoelectric effect)**
  - Quantum bits (qubits) operate using the properties of subatomic particles
- **Wave Function Collapse – The Copenhagen Interpretation of Neils Bohr and Max Born**
  - A qubit may be in a superposed state, but when a qubit is measured, the result is always either 0 or 1
- **Eigenstates and Eigenvalues – Linear Algebra**
  - Used to determine if an operator is Unitary (reversible gate) and/or Hermitian (irreversible measurement)
- **Exclusion Principle – Wolfgang Pauli**
  - The Pauli Exclusion Principle defines the conduct of qubits; X, Y, and Z operators (gates) are the Pauli matrices
- **Quantum Superposition and Entanglement - Spooky action at a distance (Einstein)**
  - Superposition: qubits exist in multiple states simultaneously, offering an exponential increase in computational power
  - Entanglement: qubits linked in such a way that the state of one (no matter the distance) instantly influences its partner, enabling unparalleled data synchronization
  - Interference uses the probability nature of quantum mechanics to reinforce or cancel out pathways, guiding algorithms towards the correct solution

> "If you think you understand quantum mechanics, you don't understand quantum mechanics." – Feynman

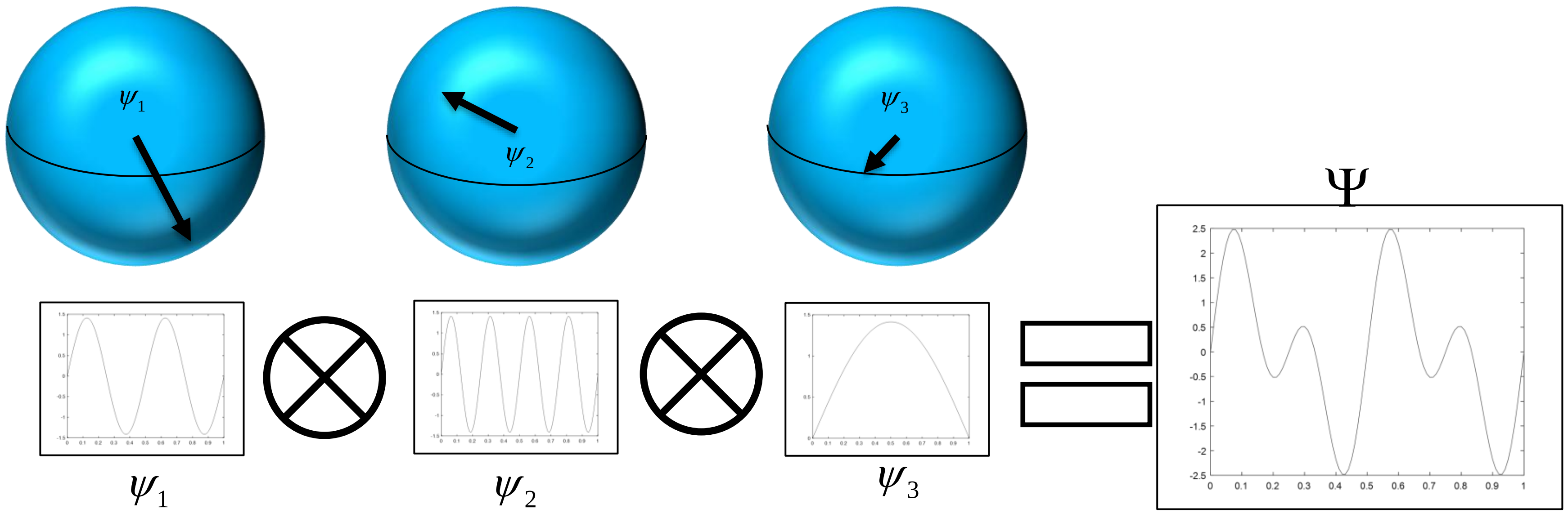
Quantum Properties

P(0)=15%
P(1)=85%

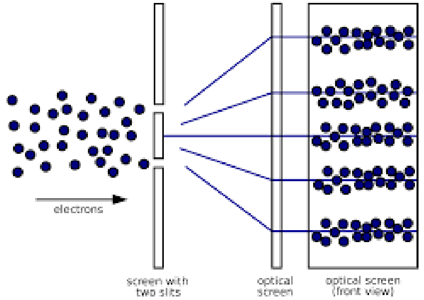
P(0)=70%
P(1)=30%

P(0)=50%
P(1)=50%

Superposition without entanglement

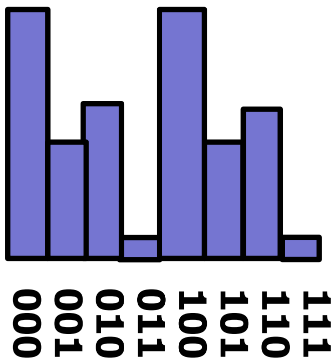


Individual wavefunctions constructively/destructively interfere



Quantum Algorithm

1. Create superposition
2. Entangle qubits
3. Apply interference
4. Measure result



Entangled probabilities - If you change the state of one qubit, the probability of all other states changes

Classical computers can be in any state, but they can only be in <u>one</u> state at a given time

Quantum computers are in a superposition of <u>all</u> states at a given time

Quantum Computing: Who Cares?

- Recent quantum technological breakthroughs not achievable by classical (digital) computing
  - Quantum cryptography (implemented/fielded)
  - Quantum teleportation

- Department of Energy (DOE) exploring applications of quantum simulation (energetics)

- Modeling, Simulation, and Training
  - Optimization applications to MS&T (e.g., training and human performance optimization)
  - I/ITSEC Knowledge Repository returned 1618 papers with keyword "machine learning"
  - Quantum optimization leads to quantum machine learning

> "For the intelligence community, some areas "where you might be able to take advantage of quantum computing" include operations research, decision-making and optimization, …"
> - Algorithmic Warfare by Josh Luckenbaugh, National Defense Magazine 2024

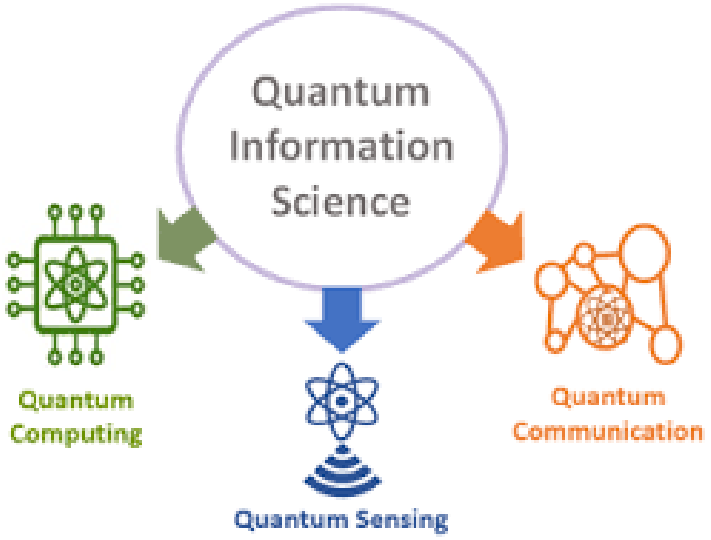
Quantum Information Science

- “Military confrontation capabilities have been upgraded to basic research related to synthetic biology, quantum information science, cognitive neuroscience, human behavior modeling, and new engineering materials.” – Integrated Human-Machine Intelligence: Beyond Artificial Intelligence, Wei Liu 2023

- Quantum Sensing
  - Quantum devices for PNT
  - For use in GPS-denied environments
  - Also, electromagnetic and gravitational field sensing

- Quantum Communication (Networking)
  - Cryptography
  - Teleportation

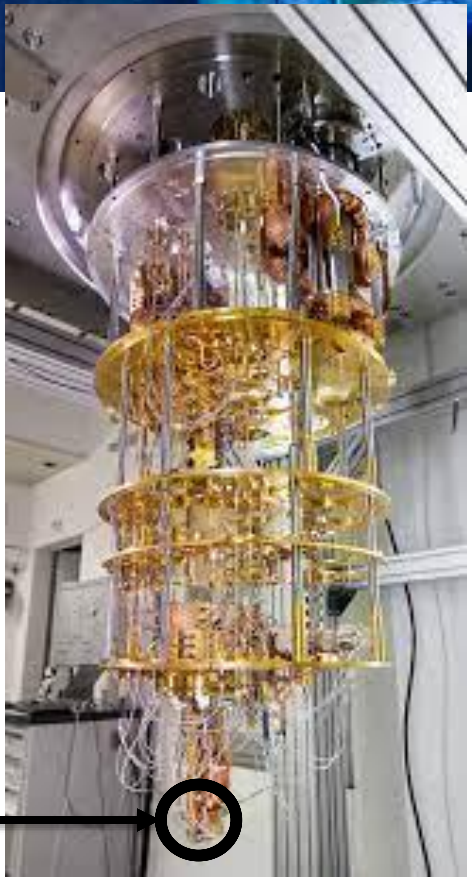
- Quantum Computation



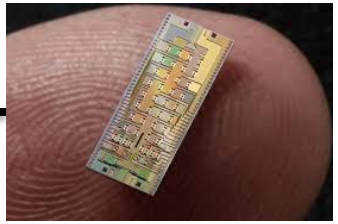
The focus of this presentation will be quantum computing, with networking examples of quantum cryptography and quantum teleportation

Physical Implementations

Company	Technology	Encoding	State
Xanadu PsiQuantum	Nanophotonics	Polarization	Polarization filters
Honywell IonQ	Trapped Ions	Energy Levels	Spin (up/down)
IBM Intel Google D-Wave	Superconducting Josephson Junction	Charge Current	Charged/uncharged Current (CW/CCW) Ground state/first excited state
Microsoft	Hypothetical	quasi-particle (anyon)	No hardware at this time



Xanadu's nanophotonic chip powered by laser pulses



Quantum Computers - Challenges

- Noise – In the sense of error (not audio or signal-to-noise ratio)

- Noise and Decoherence
  - At the subatomic level, electromagnetic field fluctuations and radiation result in environmental changes
  - Most of today's quantum computers are Noisy Intermediate-Scale Quantum (NISQ) computers
  - Quantum cryptography can be performed with single qubits, which is why there are commercial applications

- Quantum Error Correction
  - Because of the fragility (incoherence) of qubits, <u>~100 physical</u> qubits make up <u>one logical</u> qubit
  - Physical qubits are necessary for error checking and error correction (checksum)
  - IBM announced Condor, with <u>1121 physical</u> qubits, the world's largest quantum chip (Jan 2024)
  - Compare with the bits in an average laptop (8 core) numbering about 24,576
  - We're sort of at the equivalent of the Babbage stage when it comes to quantum computers

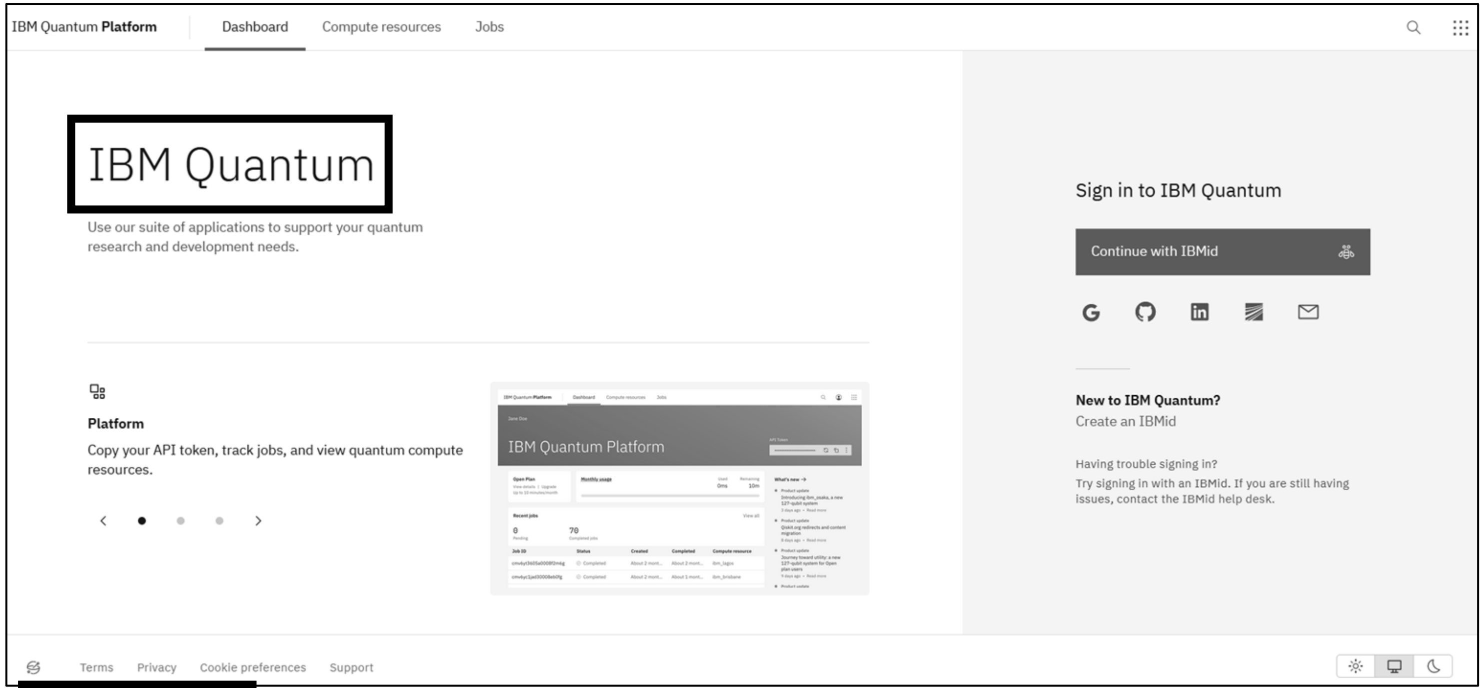
Notional Example
3 physical qubits for
1 logical qubit

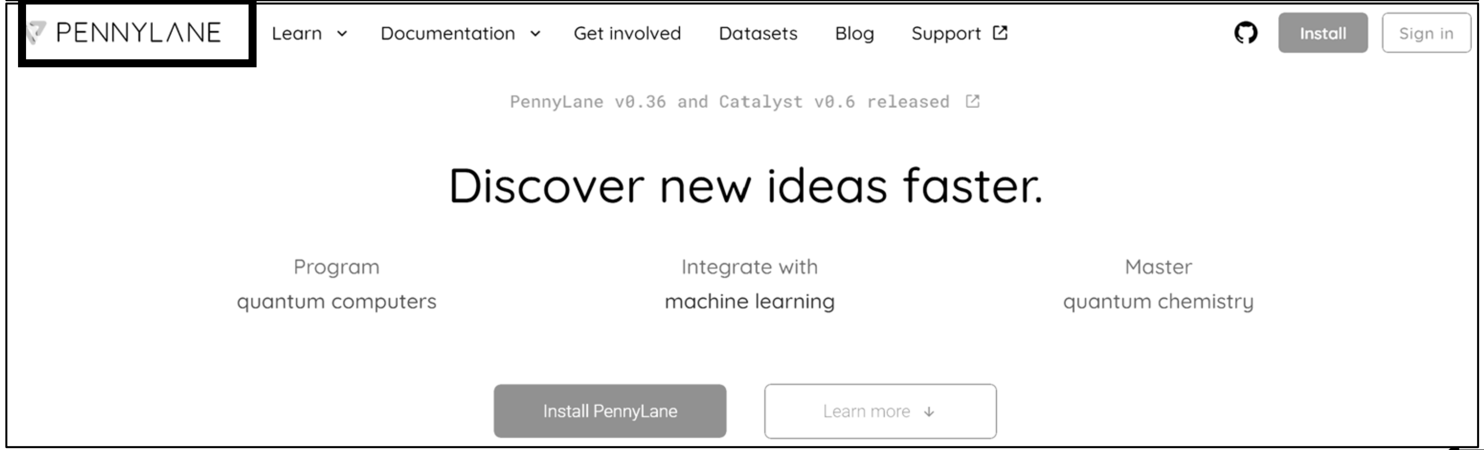
PQ		LQ
000	→	0
001	→	0
010	→	0
011	→	1
100	→	0
101	→	1
110	→	1
111	→	1

Software Interfaces

- **Software**
  - **QDK/Q# (Microsoft)**
  - **Cirq/Python (Google)**
  - **Qiskit/Python (IBM)**
  - **PennyLane/Python (Xanadu)**
  - **Ocean/Python (D-Wave)**

- **Personal Experience**
  - **Qiskit for Quantum Optimization**
  - **PennyLane for Quantum ML**
  - **Python can be problematic: deprecations because the technology is moving so fast!**





Computational Models

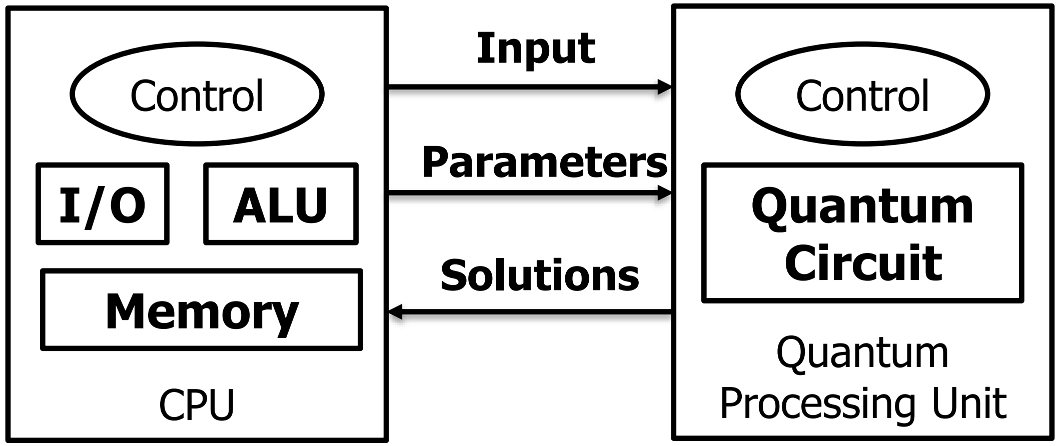
- Quantum Circuit Model (Quantum Cryptography & Quantum Teleportation)
  - Application of quantum gates (universal quantum computing)

- Adiabatic Quantum Computing (Quantum Optimization and Quantum Machine Learning)
  - Adiabatic evolution: begin in ground state, not enough energy added to jump to excited state
  - Implemented as quantum annealing, it’s <u>restricted</u>, therefore <u>not</u> universal quantum computing

- Other
  - Quantum Turing Machines
  - Measurement-Based Quantum Computing (One-Way Quantum Computing)
  - MBQC has given way to Fusion-Based QC, as pursued by PsiQuantum

Debunking Myths

- Myth: Quantum computers will render classical computers obsolete
  - Truth: For most tasks running on your personal computer, a quantum computer performs no better
  - Only very specific classes of algorithms are currently known to benefit from quantum computing
- From a programmer's perspective, a quantum computer is but a co-processor
  - Classical computers handle input and output and call the "QPU" for specific tasks



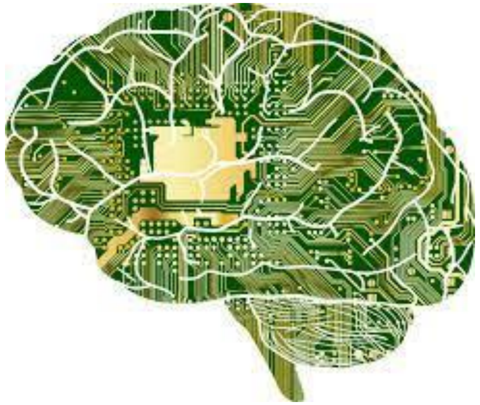
- Quantum computers excel at optimization problems and since AI/ML is nothing more than fancy curve-fitting (Judea Pearl), quantum computing may play a significant role in AI/ML

Today, all quantum computing (hardware) is hybrid, i.e., quantum computers receive input from classical computers and provide output to classical computers; plus, some software applications are hybrid too (classical/quantum algorithms)

Debunking Myths

- **Myth: There is no practical use for quantum computers**
  - Truth: Even with NISQ QCs, there are already applications (as will be shown)
  - Think of Radio Shack's TRS-80 (Z-80, 2 MHz processor with 4K RAM), we did a lot with it!
  - However, practical advantages? Not really.

- **Myth: Quantum computers will develop their own minds**
  - Truth: We've heard this (for a while now) about AI/ML
  - For quantum computing (and AI/ML for that matter), how can this be if humans do not fully understand how consciousness works?
  - For that matter, can AI reflect on a decision it has made?



Single Qubits

Qubits

Superposition

Bloch Sphere

Operators/Gates

Application: Cryptography

Single Qubits

- **Classical Bit**
  - Either 0 or 1
- **Quantum Bit (Qubit)**
  - Superposition of pure states 0 and 1
  - Dirac's $\langle bra | ket \rangle$ notation

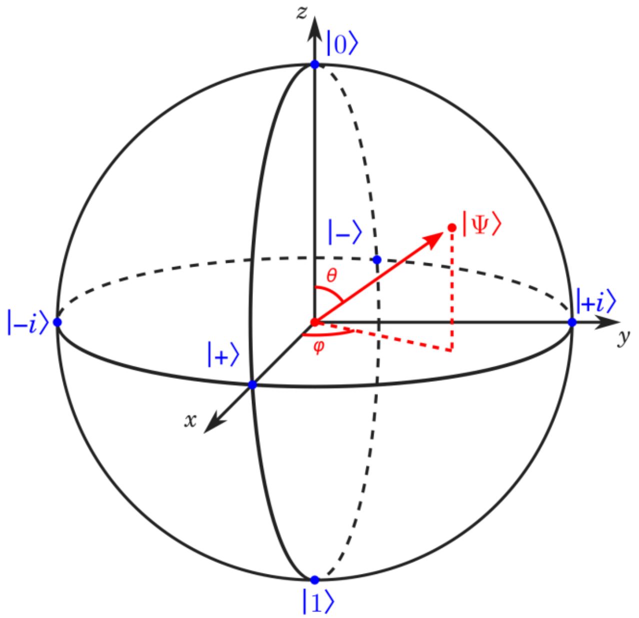
$$|\mathbf{0}\rangle \equiv \begin{bmatrix} \mathbf{1} \\ \mathbf{0} \end{bmatrix} \quad |\mathbf{1}\rangle \equiv \begin{bmatrix} \mathbf{0} \\ \mathbf{1} \end{bmatrix}$$

← **Standard (Computational) Basis**

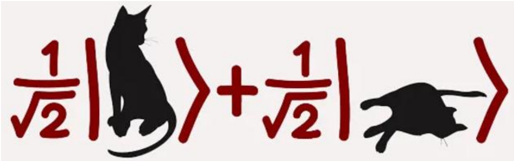
  - Some qubits could be an equal superposition of 0 and 1
  - These states are on the "equator" of the Bloch sphere
  - While the superpositions are equal in magnitude, in some cases, their phase differs

$$|+\rangle \equiv \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{0}\rangle + |\mathbf{1}\rangle) \qquad |-\rangle \equiv \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{0}\rangle - |\mathbf{1}\rangle)$$

$$|+\boldsymbol{i}\rangle \equiv \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{0}\rangle + \boldsymbol{i}|\mathbf{1}\rangle) \quad |-\boldsymbol{i}\rangle \equiv \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{0}\rangle - \boldsymbol{i}|\mathbf{1}\rangle)$$

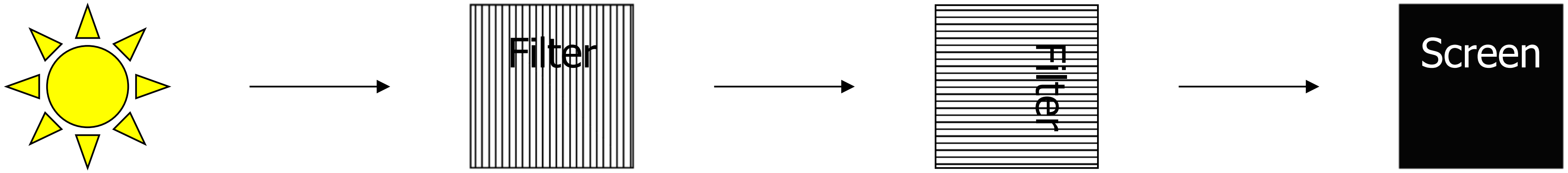


Bloch Sphere

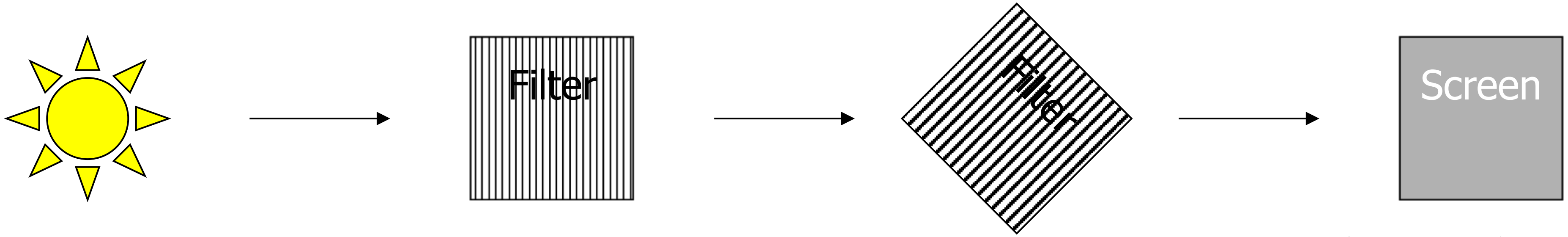


Single Qubits

- Light polarization
  - Sunlight has no preferred polarization, however a filter can set the preferred polarization
  - Let vertical polarization be represented by $|1\rangle$ and horizontal polarization be represented by $|0\rangle$
  - Then the state of sunlight may be represented by $|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$
- Vertical polarization $|1\rangle$
  - If sunlight is vertically polarized, what happens if we introduce a second perpendicular (horizontal) filter?



  - If sunlight is vertically polarized, what happens if we introduce a second filter at 45 degrees?



  - Vertical polarization is a superposition of +45° diagonal and -45° diagonal filtering $|1\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$
  - Since the $|+\rangle$ state is only one term in the superposition, half of the light gets through to the screen

Single Qubits

- **Myth: A qubit is both 0 and 1 at the same time**
  - Truth: A qubit is a superposition of both states
- Quantum Bit (qubit)
  - In general, a qubit may lie *anywhere* on the surface of the (Bloch) sphere

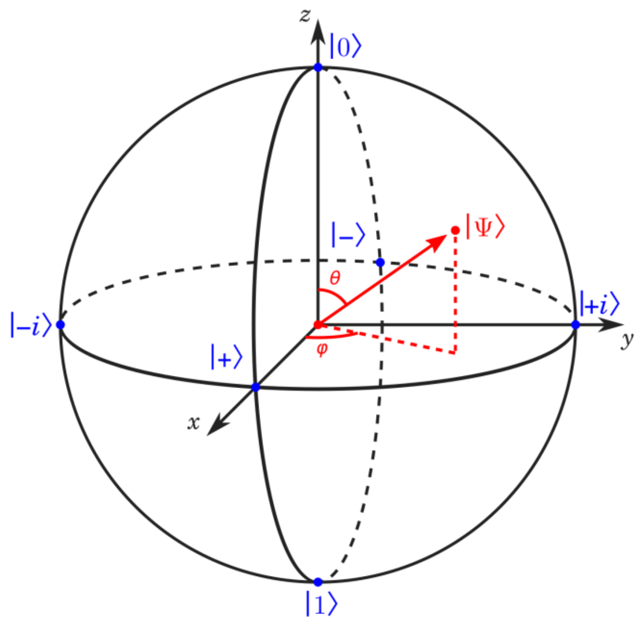
$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \quad 0 \le \theta \le \pi \quad 0 \le \varphi < 2\pi$$

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

  - Note: The coefficients (α and β) are amplitudes, and their squares (complex norm or modulus) are the probabilities associated with each state
  - $|\alpha|^2$ is the probability of $|\Psi>$ being in the $|0>$ state
  - $|\beta|^2$ is the probability of $|\Psi>$ being in the $|1>$ state
    $|\alpha|^2 + |\beta|^2 = 1$
  - If $\alpha > \beta, P(|0\rangle) > P(|1\rangle)$
  - Note: In general, the coefficients are complex numbers. As such they have phase. Relative phase between the complex coefficients plays a role in quantum computing.

$$\alpha = a_1 + ia_2 \qquad \beta = b_1 + ib_2$$

$$\phi_\alpha = \tan^{-1}\frac{a_2}{a_1} \qquad \phi_\beta = \tan^{-1}\frac{b_2}{b_1}$$



Bloch Sphere

Quantum Gates

- Digital computers have finite logic gates (AND, OR, etc.)
- The situation is similar with quantum computing
- There are different operations applied to qubits
  - When initializing a qubit, the process is irreversible (Hermitian)
  - When performing quantum computations, the process is reversible (Unitary)
  - When measuring qubits, the process is irreversible (Hermitian)
- Because the systems are linear, the operators are matrix multiplications

Quantum Gates

- **Hadamard Gate (Unitary)**
  - Used to create a superposed state
  - When applied to |0>, the result is |+>
  - When applied to |1>, the result is |->
  - |+> and |-> comprise the Hadamard Basis

$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle \qquad |1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$$

$$\begin{bmatrix}1\\1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}$$

$$\left\{\begin{aligned}
\mathbf{H} &= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\\
\mathbf{H}|0\rangle &= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle\\
\mathbf{H}|1\rangle &= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle
\end{aligned}\right.$$

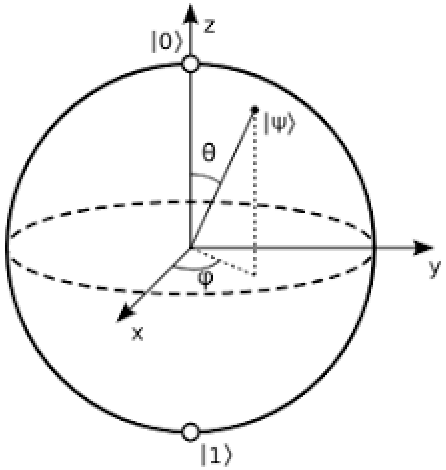
- **X, Y, and Z (Pauli) Gates (Unitary)**
  - X is referred to as the "not" gate

    $X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle$
  - Z is referred to as the phase shift gate

    It's a rotation about Z of the Bloch sphere, i.e., φ
  - Y completes the trio

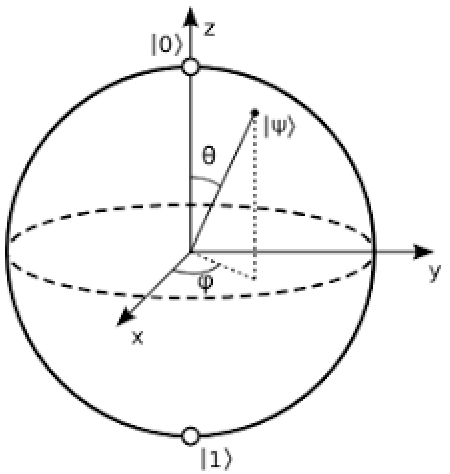
    $iY|+\rangle = |-\rangle \qquad iY|-\rangle = -|+\rangle$

$$\left\{\begin{aligned}
\mathbf{X} &= \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\\
\mathbf{Z} &= \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}\\
\mathbf{Y} &= \begin{bmatrix}0 & -i\\i & 0\end{bmatrix}
\end{aligned}\right.$$



Quantum Gates

- **X, Y, and Z (Pauli) Gates (Unitary)**
  - **X, Y, and Z are all rotations of π radians (180 deg)**



- **Generalized Rotations**

$$R_X(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_Y(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_Z(\theta) = \begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

$$R_X(\pi) = -iX \equiv X$$

$$R_Y(\pi) = iY \equiv Y$$

$$R_Z(\pi) = Z$$

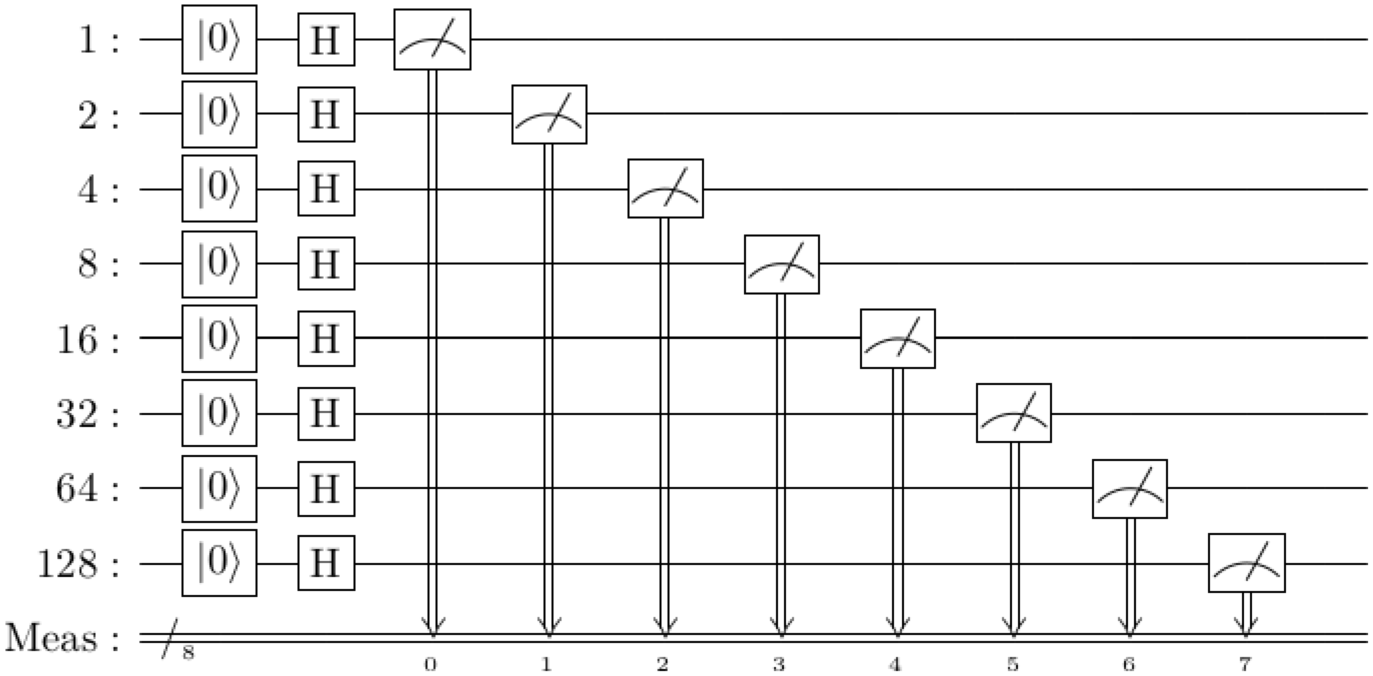
≡ denotes equivalent action up to a global phase

True Random Number Generator

- Random Byte (no need for *pseudo-random* number generators)
  - H|0> produces a superposition, with a 50/50 chance of resulting in a 0 or a 1
  - 1*Meas0 + 2*Meas1 + 4*Meas2 + 8*Meas3 + 16*Meas4 + 32*Meas5 + 64*Meas6 + 128*Meas7

$$\mathbf{H}|\mathbf{0}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{0}\rangle + |\mathbf{1}\rangle)$$

```
from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister, Aer
from qiskit.tools.visualization import circuit_drawer
from qiskit.visualization import plot_histogram

qr1 = QuantumRegister(1, 'qr1'), qr2 = QuantumRegister(1, 'qr2')
qr3 = QuantumRegister(1, 'qr3'),qr4 = QuantumRegister(1, 'qr4')
qr5 = QuantumRegister(1, 'qr5'),qr6 = QuantumRegister(1, 'qr6')
qr7 = QuantumRegister(1, 'qr7'),qr8 = QuantumRegister(1, 'qr8')
cr  = ClassicalRegister(8, 'cr')
qc = QuantumCircuit(qr1,qr2,qr3,qr4,qr5,qr6,qr7,qr8,cr)

qc.reset(0),qc.reset(1),qc.reset(2),qc.reset(3)
qc.reset(4),qc.reset(5),qc.reset(6),qc.reset(7)

qc.h(0),qc.h(1),qc.h(2),qc.h(3)
qc.h(4),qc.h(5),qc.h(6),qc.h(7)

qc.measure(0, 0),qc.measure(1, 1),qc.measure(2, 2),qc.measure(3, 3)
qc.measure(4, 4),qc.measure(5, 5),qc.measure(6, 6),qc.measure(7, 7)

circuit_drawer(qc, output='latex', style={'backgroundcolor': '#EEEEEE'})
```



NIST's New Quantum Method Generates *Really* Random Numbers - 2018

Qubit Summary

- Qubits are a superposition of both states simultaneously

- Because of superposition, there is a relative phase (quantum interference) between α and β
  - This has implications for Deutch's algorithm and Grover's algorithm

- Entanglement (to be discussed) is a property of multiple qubits

- Because of these properties, qubits are more powerful than classical bits

- https://javafxpert.github.io/grok-bloch/

- One drawback is the "No Cloning Theorem" which states that <u>a qubit cannot be copied</u>
  - This has implications for cryptography which we will explore next…

Application: Quantum Cryptography

- A quantum computer with several thousand qubits can solve a strategic problem (encryption and decryption) that classical computers have no hope of solving
  - This is one of those “special applications” where quantum computing outperforms classical computers
  - Peter Shor’s algorithm cracks the widely used RSA encryption scheme
  - But quantum computing also has some clever ways to solve this problem with single qubits…

- Cryptography aims to hide the meaning of a message through encryption
  - BB84 was developed by Charles Bennett and Gilles Brassard in 1984
  - Goal: to share symmetric keys, securely
  - The qubits themselves are not used to send messages

Application: Quantum Cryptography

- Alice and Bob want to share a secret
  - Alice generates 20 qubits and sends them to Bob
  - Eavesdropper (Eve) listens-in, makes note of the qubits, and forwards them to Bob
  - The secret has been compromised, hmmm…

- But Alice and Bob know about quantum computing
  - Alice applies the Hadamard gate before sending her qubits
  - Since the Hadamard gate is its own inverse, Bob can recover each qubit

- Unfortunately, Eve knows about quantum computing too
  - Eve applies the Hadamard gate twice, once to recover the qubits and again before forwarding them to Bob
  - Alas, Hadamard gates alone don't help, hmmm…

- Unfortunately, just as Eve can't figure out what Alice meant to send, neither can Bob
  - If Alice tells Bob which qubits had been Hadamarded, Eve could intercept that message, hmmm…

Application: Quantum Cryptography

- **BB84**
  - **Both Alice and Bob decide to randomly apply the Hadamard gate with two possible outcomes:**
    - They both applied the Hadamard gate, or neither applied the Hadamard gate
    - One applied the Hadamard gate, and the other didn’t
  - **Bob publicly announces which qubits he applied the Hadamard gate to**
    - If Eve is listening-in, the information Bob provides is or no use to her
  - **Alice publicly announces which of her choices agrees with Bob**
    - If Eve is listening-in, the information Alice provides is or no use to her
  - **Bob publicly announces the results of the first-half of their agreement as “test qubits”**
    - If Eve is listening-in, there is little chance that all “test qubits” match
  - **The second-half of the results form the “shared secret”**

Qubit #	Alice		
1	1		
2	0	H	$\frac{1}{\sqrt{2}}(\vert 0\rangle + \vert 1\rangle)$
3	1	H	$\frac{1}{\sqrt{2}}(\vert 0\rangle - \vert 1\rangle)$
4	0	H	$\frac{1}{\sqrt{2}}(\vert 0\rangle + \vert 1\rangle)$
5	0		
6	1		
7	0	H	$\frac{1}{\sqrt{2}}(\vert 0\rangle + \vert 1\rangle)$
8	0		
9	1		
10	1	H	$\frac{1}{\sqrt{2}}(\vert 0\rangle - \vert 1\rangle)$
11	1	H	$\frac{1}{\sqrt{2}}(\vert 0\rangle - \vert 1\rangle)$
12	1		
13	0	H	$\frac{1}{\sqrt{2}}(\vert 0\rangle + \vert 1\rangle)$
14	1	H	$\frac{1}{\sqrt{2}}(\vert 0\rangle - \vert 1\rangle)$
15	1	H	$\frac{1}{\sqrt{2}}(\vert 0\rangle - \vert 1\rangle)$
16	1		
17	0	H	$\frac{1}{\sqrt{2}}(\vert 0\rangle + \vert 1\rangle)$
18	1		
19	0	H	$\frac{1}{\sqrt{2}}(\vert 0\rangle + \vert 1\rangle)$
20	0		

Qubit #	Bob	
1	H	?
2		?
3		?
4	H	0
5		0
6		1
7	H	0
8	H	?
9		1
10		?
11		?
12		1
13	H	0
14	H	1
15		?
16	H	?
17		?
18	H	?
19	H	0
20		0

Bob publishes all 20 of his decisions

Alice publishes when she agrees, namely qubits 4, 5, 6, 7, 9, 12, 13, 14, 19, 20

Bob publishes results of the first-half, namely [0, 0, 1, 0, 1] as "test qubits"

The second-half, namely [1, 0, 1, 0, 0] form the "shared secret"

Application: Quantum Cryptography

- Suppose we want to encrypt the message, "LSA"
  - In ASCII L=1001100, S=1010011, A=1000001
  - The bit stream is 1001100 1010011 1000001
  - Alice repeatedly applies the XOR "shared secret" 10100 (key)
  - Then she sends the encrypted message to Bob

Message	1	0	0	1	1	0	0		1	0	1	0	0	1	1		1	0	0	0	0	0	1
Key	1	0	1	0	0	**1**	**0**		**1**	**0**	**0**	1	0	1	0		0	**1**	**0**	**1**	**0**	**0**	1
Encrypted	0	0	1	1	1	1	0		0	0	1	1	0	0	1		1	1	0	1	0	0	0

  - Upon receipt, Bob repeatedly applies the XOR "shared secret" and recovers the message

Encrypted	0	0	1	1	1	1	0		0	0	1	1	0	0	1		1	1	0	1	0	0	0
Key	1	0	1	0	0	1	0		1	0	0	1	0	1	0		0	1	0	1	0	0	1
Message	1	0	0	1	1	0	0		1	0	1	0	0	1	1		1	0	0	0	0	0	1
	"L"								"S"								"A"						

Application: Quantum Cryptography

- **Myth: Quantum computers will put cybersecurity at risk**
  - **Truth: While the power and speed of quantum computers could crack RSA public key encryption (Shor's algorithm), there are already quantum-resistant cryptography algorithms**

- **We just showed a simple (BB84) example using only single qubits and the Hadamard gate for superposition to establish a post-quantum encryption algorithm**
  - **Perhaps this could be extended for secure distributed simulation**

- **What is Post-Quantum Cryptography (PQC)?**
  - **The development of novel classical cryptographic schemes, believed to be resistant to future quantum computers employing Shor's algorithm**
  - **The NSA is taking this seriously to safeguard data against future hackers**
  - **Efforts are already underway to incorporate these new schemes (some of which have already been hacked)**
  - **Note: Encrypted data is being collected now for future decryption (What is the "shelf-life" of your data?)**

NIST SP 1800-38B, Migration to Post-Quantum Cryptography Quantum Readiness: **Cryptographic Discovery**
NIST SP 1800-38C, Migration to Post-Quantum Cryptography Quantum Readiness: **Testing Draft Standards for Interoperability and Performance**

Multiple Qubits

Multi-Qubit Operators/Gates

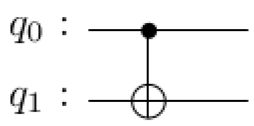
Entanglement

Application: Teleportation

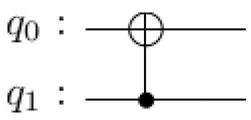
Multiple Qubits

- The Hadamard and Pauli gates operate on a singe qubit
- Some gates operate on multiple qubits in parallel
- Qubits are combined according to the tensor product $|q_0 q_1\rangle$
- Caution! Some literature uses different ordering
- Controlled NOT (CNOT)
  - If the control qubit is 0, do nothing
  - If the control qubit is 1, flip the other (target) qubit
  - Assume: left qubit |x> is Control, right qubit |y> is Target

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{bmatrix} = \begin{bmatrix} |00\rangle \\ |01\rangle \\ |11\rangle \\ |10\rangle \end{bmatrix}$$



  - Caution! Sometimes the control/target qubits are opposite



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{bmatrix} = \begin{bmatrix} |00\rangle \\ |11\rangle \\ |10\rangle \\ |01\rangle \end{bmatrix}$$

Label

Math

$$|q_1 q_0\rangle = |q_1\rangle \otimes |q_0\rangle$$

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

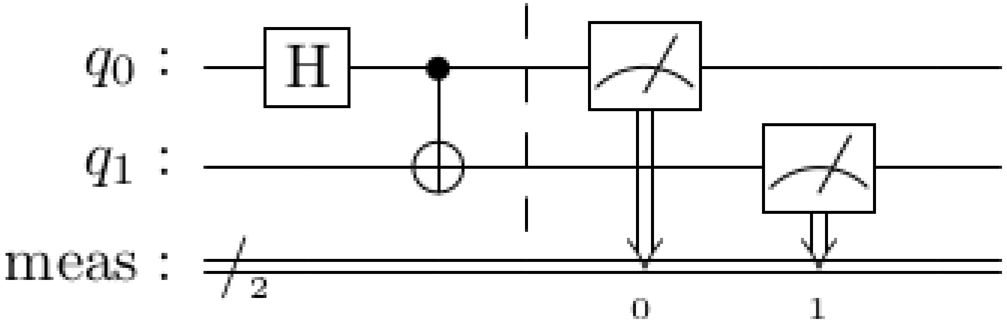
$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Gate-Based/Universal Quantum Computing

- **Create wires and associate qubits with them**
- **Gates interact with the qubits to perform calculations**
  - **The Hadamard gate interact with a single qubit**
  - **The CNOT gate interacts with multiple qubits**
- **In the end, measurements are made**
  - **Remember: The result is either a 0 or a 1**

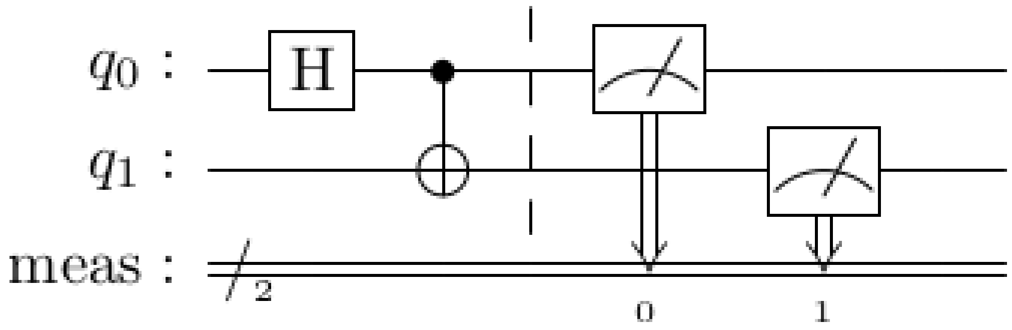


- **Example in Qiskit**

from qiskit import QuantumCircuit	*Import the library*
circuit = QuantumCircuit(2)	*Create a quantum circuit with two qubits, q0 and q1*
circuit.h(0)	*Apply the Hadamard operator to qubit 0*
circuit.cnot(0,1)	*Apply the CNOT operator q0(C), q1(T)*
circuit.measure_all()	*Measure both qubits*
display(circuit.draw('latex'))	*Draw the circuit*

Circuitry and Mathematics

- What is the result of the previous example?
- Let's "do the math…"
  - Assume each qubit is in the initial pure state |0>



$$|q_1\rangle \otimes |q_0\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} = |00\rangle$$

Math

Label

  - We want to apply to Hadamard operator to q0 while maintaining q1 in parallel

$$(I \otimes H)\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \left(\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\right)\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1 & 0 & 0\\1 & -1 & 0 & 0\\0 & 0 & 1 & 1\\0 & 0 & 1 & -1\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\\0\\0\end{bmatrix}$$

  - Next, we apply the CNOT operator

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\\0 & 1 & 0 & 0\end{bmatrix}\begin{bmatrix}1\\1\\0\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

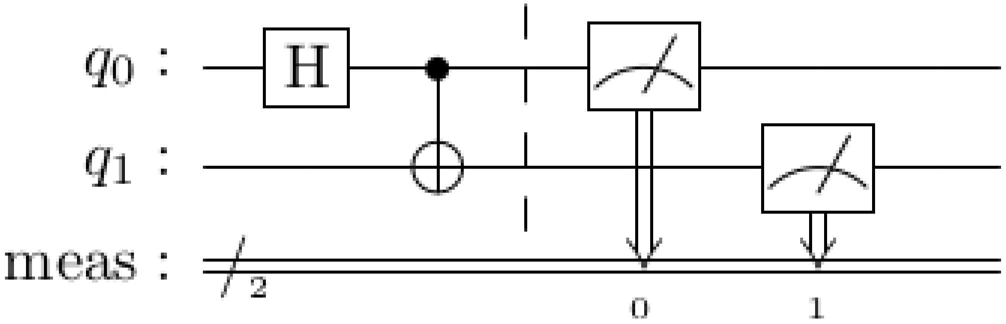
Math

Label

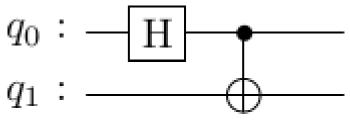
Note: You could begin by applying the Hadamard operator to q0, perform the tensor multiplication, then apply the CNOT operator

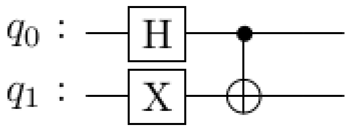
Circuitry and Mathematics

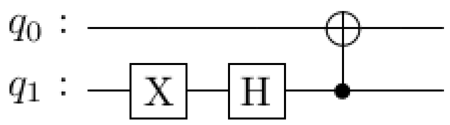
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

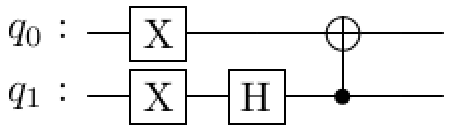


- At this point, the qubits are equally likely (50/50) to be in either the |00> or the |11> state
- If q0 is measured to be 0, then q1 must be 0; likewise, if q0 is measured to be 1, q1 must be 1
- The qubits are known to be *entangled*
- Similarly…









$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

- …these are known as EPR* pairs or Bell states (after John Bell who proved the EPR paradox)

*EPR refers to a paper written by Einstein, Podolsky, and Rosen challenging the concept of entanglement (hidden variables)

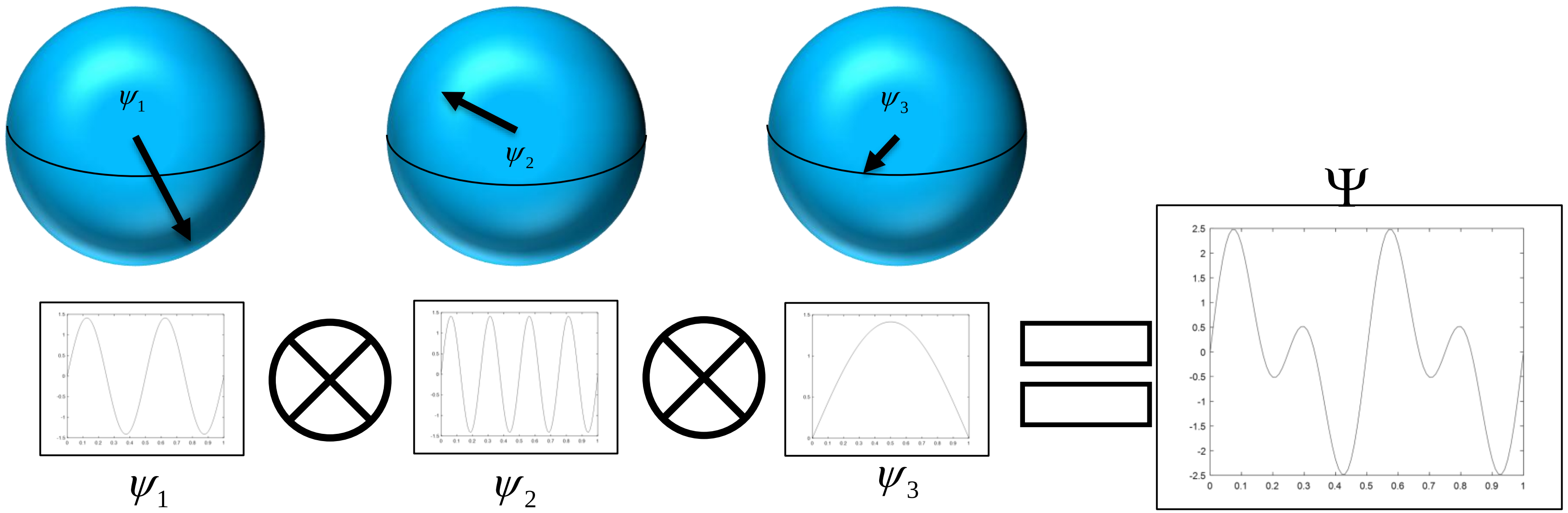
Quantum Properties

P(0)=15%
P(1)=85%

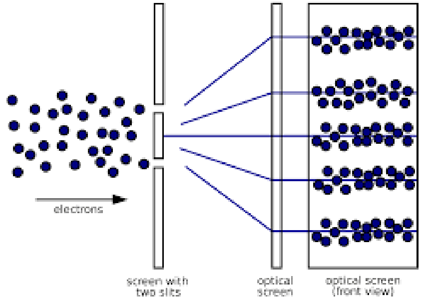
P(0)=70%
P(1)=30%

P(0)=50%
P(1)=50%

Superposition without entanglement

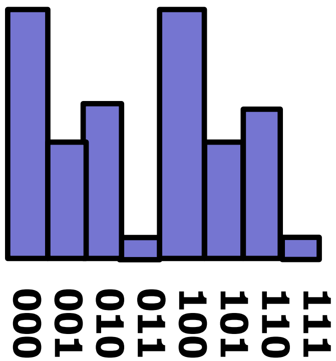


Individual wavefunctions constructively/destructively interfere



Quantum Algorithm

1. Create superposition
2. Entangle qubits
3. Apply interference
4. Measure result



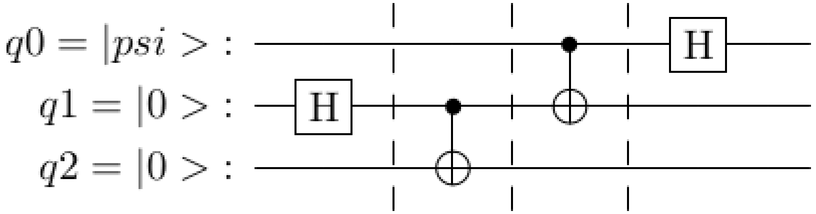
Entangled probabilities - If you change the state of one qubit, the probability of all other states changes

Classical computers can be in any state, but they can only be in <u>one</u> state at a given time

Quantum computers are in a superposition of <u>all</u> states at a given time

Application: Quantum Teleportation

- **Practical Application: Quantum Networking**
  - **Goal: Alice wants to send the <u>state</u> of her qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob**
  - **Problem: If Bob tries measuring Alice's qubit, he'll get either $|0\rangle$ or $|1\rangle$**
  - **Problem: Because of the No Cloning Theorem, it cannot be copied**
  - **Solution: Quantum Teleportation through an entangled EPR pair (Bell state)**



- **From the circuit, before applying the first CNOT operator, we need the tensor product**

$$|q_2\rangle \otimes |q_1\rangle \otimes |q_0\rangle = |0\rangle \otimes H|0\rangle \otimes |\psi\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \otimes \begin{bmatrix}\alpha\\\beta\end{bmatrix} = \frac{1}{\sqrt{2}}[\alpha \quad \beta \quad \alpha \quad \beta \quad 0 \quad 0 \quad 0 \quad 0]'$$

- **$CNOT \otimes I$ with q1(C) and q2(T)**

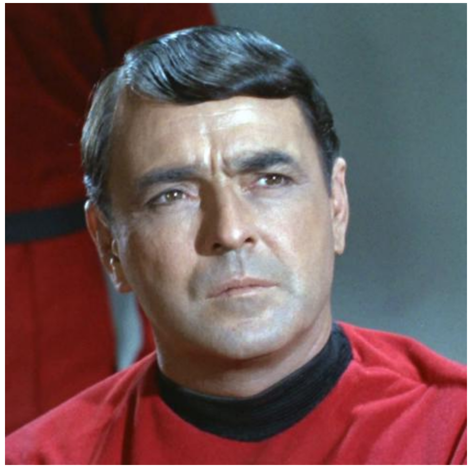
$$\frac{1}{\sqrt{2}}[\alpha \quad \beta \quad 0 \quad 0 \quad 0 \quad 0 \quad \alpha \quad \beta]'$$

- **$\mathrm{I} \otimes CNOT$ with q0(C) and q1(T)**

$$\frac{1}{\sqrt{2}}[\alpha \quad 0 \quad 0 \quad \beta \quad 0 \quad \beta \quad \alpha \quad 0]'$$

- **$\mathrm{I} \otimes I \otimes H$**

$$\frac{1}{\sqrt{2}}[\alpha \quad \alpha \quad \beta \quad -\beta \quad \beta \quad -\beta \quad \alpha \quad \alpha]'$$

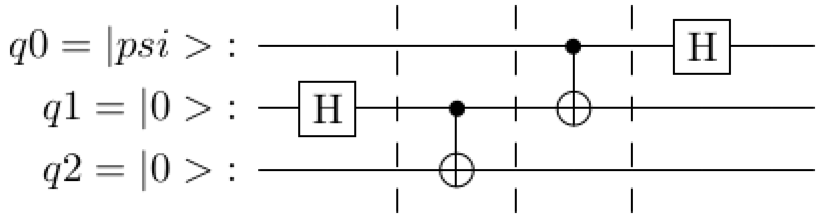


While the term "teleportation" is used, matter is not being displaced. There's no need to call Scotty.

Application: Quantum Teleportation

- Recall the qubit order is $|q_2q_1q_0\rangle$
- If Alice measures $|q_2 00\rangle$, the state is $\alpha|0\rangle + \beta|1\rangle = |\psi\rangle$

$$\begin{bmatrix}\alpha\\ \alpha\\ \beta\\ -\beta\\ \beta\\ -\beta\\ \alpha\\ \alpha\end{bmatrix} \quad \begin{bmatrix}|000\rangle\\ |001\rangle\\ |010\rangle\\ |011\rangle\\ |100\rangle\\ |101\rangle\\ |110\rangle\\ |111\rangle\end{bmatrix}$$



$|\psi\rangle$ is the original state Alice wanted to send to Bob!
It has been quantum teleported through entanglement.

Alice	Bob
$\|00\rangle$	$\|\psi\rangle = I\|q_2\rangle$
$\|01\rangle$	$\|\psi\rangle = Z\|q_2\rangle$
$\|10\rangle$	$\|\psi\rangle = X\|q_2\rangle$
$\|11\rangle$	$\|\psi\rangle = ZX\|q_2\rangle$

- If Alice measures $|q_2 01\rangle$, the state is $\alpha|0\rangle - \beta|1\rangle$, Bob just needs to apply the Z gate
- If Alice measures $|q_2 10\rangle$, the state is $\beta|0\rangle + \alpha|1\rangle$, Bob needs to apply the X gate
- If Alice measures $|q_2 11\rangle$, the state is $-\beta|0\rangle + \alpha|1\rangle$, Bob needs to apply the X gate, then the Z gate

Re: Spooky Action at a Distance, an entangled system may be separated by great distance e.g., part of the system may be in orbit and the other part may be ground-based. Since there is no communication network, there is nothing to be hacked. This is certainly an advantage over classical computing!

Quantum Optimization

Quantum Unconstrained Binary Optimization

Adiabatic Quantum Computing/Quantum Annealing

Quantum Approximate Optimization Algorithm

Variational Quantum Eigensolver

Grover Adaptive Search

Quantum Unconstrained Binary Optimization

- **Quadratic Objective Function with Linear Equality/Inequality Constraints**
  - **Begin with Quantum Unconstrained Binary Optimization (QUBO)** $x_j \in \{0,1\}$
  - **Convert any Inequality Constraints to Equality Constraints via Slack Variables**
  - **Append Equality Constraints to the Objective Function (typical Lagrangian approach)**
  - **Change variables** $x_j = (1 - z_j)/2$ **,** $z_j \in \{1, -1\}$ **to produce the Ising model**
  - **Objective function → Hamiltonian (energy) and minimization determines the ground state energy**
  - **Evaluation of the Objective Function (Hamiltonian) is the Expectation Value** $\langle \psi | H | \psi \rangle$**…**
  - **…where** $|\psi\rangle$ **is the state of the Ising model**

Note: when applying constraints via slack variables, a suboptimal solution may give "impossible" results that don't satisfy the constraints

$$H = -\sum_{j,k} J_{jk} Z_j Z_k - \sum_j h_j Z_j$$

Hamiltonians are sums of tensor products of Z matrices

This is mostly just recasting an optimization problem into something that resonates with physicists

QUBO Application

- **Example…**
  - **min** $2-4x_0-2x_1-2x_2+4x_0x_1+4x_0x_2$
  - **subject to** $x_j \in \{0,1\}$
  - **Substitute** $x_j = (1-z_j)/2$
  - **min** $z_0(z_1+z_2)$
  - **subject to** $z_j \in \{1,-1\}$

Diagonal tensor product of Z gates

  - **Ising Hamiltonian** $H = \overset{z_0}{Z} \otimes \overset{z_1}{Z} \otimes \overset{z_2}{I} + \overset{z_0}{Z} \otimes \overset{z_1}{I} \otimes \overset{z_2}{Z}$
  - **There are three variables, therefore three qubits are needed**
  - **Expectation Values based on** $\langle \psi | H | \psi \rangle$

$$\langle 000 | H | 000 \rangle = 2$$
$$\langle 001 | H | 001 \rangle = 0$$
$$\langle 010 | H | 010 \rangle = 0$$
$$\boxed{\begin{gathered}\langle 011 | H | 011 \rangle = -2 \\ \langle 100 | H | 100 \rangle = -2\end{gathered}}$$
$$\langle 101 | H | 101 \rangle = 0$$
$$\langle 110 | H | 110 \rangle = 0$$
$$\langle 111 | H | 111 \rangle = 2$$

Orthogonality note:
$\langle x| Z_j |x\rangle = 1$ if the j^{th} bit of x is 0 and that $\langle x| Z_j |x\rangle = -1$ otherwise
$\langle x| Z_j Z_k |x\rangle = 1$ if the j^{th} and k^{th} bits of x are equal and $\langle x| Z_j Z_k |x\rangle = -1$ otherwise

$$\langle 011 | H | 011 \rangle = \langle 011 | Z_0Z_1 + Z_0Z_2 | 011 \rangle = \langle 011 | Z_0Z_1 | 011 \rangle + \langle 011 | Z_0Z_2 | 011 \rangle = -1-1 = -2$$

$$|011\rangle \rightarrow z_0 = 1, z_1 = -1, z_2 = -1$$
$$|100\rangle \rightarrow z_0 = -1, z_1 = 1, z_2 = 1$$

Adiabatic QC and Quantum Annealing

- Adiabatic quantum computing uses a quantum device called a quantum annealer
  - Think of simulated annealing, where the temperature is varied
  - A simple Hamiltonian adiabatically evolves to the desired complicated Hamiltonian
  - But don't add more energy than ΔE

- Quantum Annealing
  - Adiabatic evolution can take too long for the process to lead to a feasible/optimal solution
  - System evolves from its initial state to the Ising model's ground state
  - Physical quantum devices based on quantum annealing are simpler to construct
  - It's possible to scale the size of these quantum annealers up to hundreds or even thousands of qubits

There is no known computational advantage to quantum annealing
Also, scaling will be limited by the connectivity between qubits

Quantum Approximate Optimization Algorithm

- **Quantum Approximate Optimization Algorithm (QAOA)**
  - **For use with gate-based quantum circuit computers, as an alternative to quantum annealers**

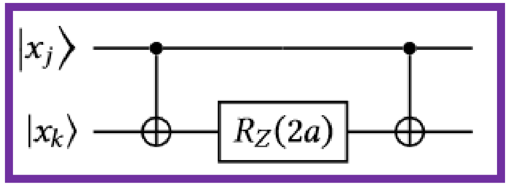
$$H_0 = \otimes_{i=0}^{n-1} \left| + \right\rangle = -\sum_{j=0}^{n-1} X_j \qquad H_1 = -\sum_{j,k} J_{jk} Z_j Z_k - \sum_j h_j Z_j$$

  - **…such that**

$$\exp(i\beta_k H_0) = \exp(i\beta_k \sum_{j=1}^{n-1} X_j) = \boxed{\prod_{j=0}^{n-1} \exp(-i\beta_k X_j)} \qquad \boxed{R_X(2\beta)}$$

$$\exp(i\gamma_l H_1) = \exp(i\gamma_l \sum_{j,k} J_{jk} Z_j Z_k + \sum_j h_j Z_j) = \boxed{\prod_{j,k} \exp(-i\gamma_l J_{jk} Z_j Z_k)} \boxed{\prod_j \exp(-i\gamma_l h_j Z_j)} \qquad \boxed{R_Z(2\gamma)}$$

  - **Let** $a = \gamma_l J_{jk}$
  - **If** $\left| x \right\rangle$ **is a computational basis state in which j and k have the same value, then** $\exp(-iaZ_j Z_k)\left| x \right\rangle = \exp(-ia)\left| x \right\rangle$
  - **If j and k have different values, then** $\exp(-iaZ_j Z_k)\left| x \right\rangle = \exp(ia)\left| x \right\rangle$



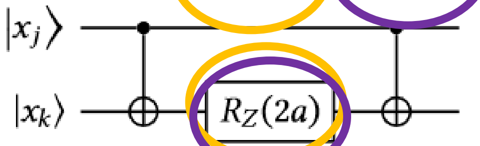
Quantum Approximate Optimization Algorithm

- **Quantum Approximate Optimization Algorithm (QAOA)**
  - **Example: Let** $H = 3Z_0Z_2 - Z_1Z_2 + 2Z_0$

$$H_0 = \otimes_{i=0}^{n-1} |+\rangle = -\sum_{j=0}^{n-1} X_j \qquad H_1 = -\sum_{j,k} J_{jk} Z_j Z_k - \sum_j h_j Z_j$$

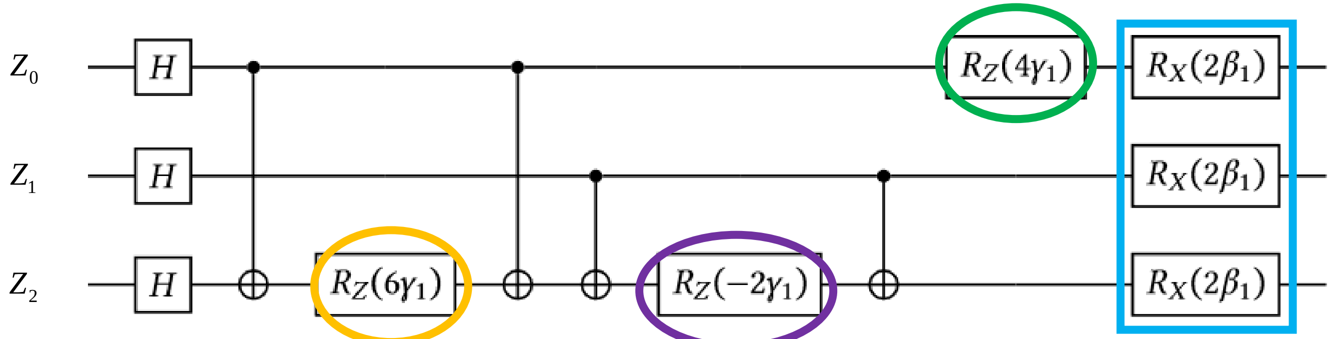
$$\boxed{H_0 = -X_0 - X_1 - X_2} \qquad H_1 = -(-3Z_0Z_2 + Z_1Z_2) - (-2Z_0)$$

$$\boxed{R_X(2\beta) \quad R_X(2\beta) \quad R_X(2\beta)}$$



$$R_Z(2\gamma)$$

  - **The quantum circuit implementation (for p=1) is**



There is no known computational advantage to QAOA

  - **As seen with QUBO, $\langle x|Z_j|x\rangle = 1$ if the jth bit of x is 0 and that $\langle x|Z_j|x\rangle = -1$ otherwise**
  - **$\langle x|Z_jZ_k|x\rangle = 1$ if the jth and kth bits of x are equal and $\langle x|Z_jZ_k|x\rangle = -1$ otherwise**

$$\langle 101|H|101\rangle = \langle 101|3Z_0Z_2 - Z_1Z_2 + 2Z_0|101\rangle = 3\langle 101|Z_0Z_2|101\rangle - \langle 101|Z_1Z_2|101\rangle + 2\langle 101|Z_0|101\rangle = 3+1-2 = 2$$

Variational Quantum Eigensolver

- Measurements in quantum mechanics are represented by Hermitian operators (observables), e.g., Z matrix
- The expectation value of any Hermitian operator (observable) A is given by
  $$\langle A \rangle_{\psi} = \sum_{j,k} \left| \langle \lambda_j^k | \psi \rangle \right|^2 \lambda_j = \langle \psi | A | \psi \rangle$$
- An observable can be expressed as a linear combination of tensor products of Pauli matrices, I, X, Y, Z
  - Example $A = \frac{1}{2} Z \otimes I \otimes X - 3 I \otimes Y \otimes Y + 2 Z \otimes X \otimes Z$
    $$\langle \psi | A | \psi \rangle = \tfrac{1}{2} \langle \psi | Z \otimes I \otimes X | \psi \rangle - 3 \langle \psi | I \otimes Y \otimes Y | \psi \rangle + 2 \langle \psi | Z \otimes X \otimes Z | \psi \rangle$$
    - The eigenvectors of Z are $|0\rangle$ with eigenvalue 1 and $|1\rangle$ with eigenvalue −1
    - The eigenvectors of X are $|+\rangle$ with eigenvalue 1 and $|-\rangle$ with eigenvalue −1
    - The eigenvectors of Y are $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ with eigenvalue 1 and $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ with eigenvalue −1
    - Any (non-null) state is an eigenvector of I with eigenvalue 1

ZIX	Eigenvalue
|0>|0>|+>	1
|0>|0>|->	-1
|0>|1>|+>	-1
|0>|1>|->	1
|1>|0>|+>	-1
|1>|0>|->	1
|1>|1>|+>	1
|1>|1>|->	-1

IYY	Eigenvalue
|0>|i>|i>	1
|0>|i>|-i>	-1
|0>|-i>|i>	-1
|0>|-i>|-i>	1
|1>|i>|i>	-1
|1>|i>|-i>	1
|1>|-i>|i>	1
|1>|-i>|-i>	-1

ZXZ	Eigenvalue
|0>|+>|0>	1
|0>|+>|1>	-1
|0>|->|0>	-1
|0>|->|1>	1
|1>|+>|0>	-1
|1>|+>|1>	1
|1>|->|0>	1
|1>|->|1>	-1

Variational Quantum Eigensolver

- Example (continued)
  - Recall $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$ such that $|0\rangle = H|+\rangle$ and $|1\rangle = H|-\rangle$
  - Also, $SH|0\rangle = |i\rangle$ and $SH|1\rangle = |-i\rangle$ such that $|0\rangle = (SH)^\dagger |i\rangle$ and $|1\rangle = (SH)^\dagger |-i\rangle$
  - Therefore…
  - H takes the eigenvectors of X to the standard/computational basis
  - SH takes the eigenvectors of Y to the standard/computational basis
  - I takes the eigenvectors of Z to the standard/computational basis

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

$$Z \otimes I \otimes X \rightarrow I \otimes I \otimes H \qquad I \otimes Y \otimes Y \rightarrow I \otimes (SH)^\dagger \otimes (SH)^\dagger \qquad Z \otimes X \otimes Z \rightarrow I \otimes H \otimes I$$

$$\langle \psi | A | \psi \rangle = \tfrac{1}{2}\langle \psi | Z \otimes I \otimes X | \psi \rangle - 3\langle \psi | I \otimes Y \otimes Y | \psi \rangle + 2\langle \psi | Z \otimes X \otimes Z | \psi \rangle$$

$$\langle \psi | A | \psi \rangle = \tfrac{1}{2}\langle \psi | I \otimes I \otimes H | \psi \rangle - 3\left\langle \psi | I \otimes (SH)^\dagger \otimes (SH)^\dagger | \psi \right\rangle + 2\langle \psi | I \otimes H \otimes I | \psi \rangle$$

  - Bottom line: For any Hermitian operator A, there is always a unitary transformation that takes any basis of eigenvectors of A to the computational basis, and vice versa

➢ Note: Everything we have done, so far, is to find the ground state (minimum) of the Hamiltonian

➢ However, the Hamiltonian may be augmented to find excited states with Physical Chemistry applications

There is no known computational advantage to VQE

Grover's Algorithm

- Grover's algorithm is $O(\sqrt{n})$

Hacking a 13-character (alpha only) password

- $26^{13} = 2.5 \times 10^{18}$ combinations
- At one guess/nanosecond, that's 2.5×10^{9} sec (~80 years)
- Grover solves it in $\sqrt{n} = \sqrt{2.5 \times 10^{9}} = 50{,}000$ sec
- <u>If</u> QC advances like today's Intel chips, i.e., at 50,000X…
- …then the password will be hacked in 1 sec

- Caveats:
  - It provides only a quadratic speedup
  - You need to know the number of solutions (or be patient in guessing)
  - It can be adapted to optimization via a binary search of cost function values
  - Classical algorithms, such as Schoening's algorithm, offer a better speedup for satisfiability problems
  - A quantum version <u>may</u> offer further enhancement

Quantum Machine Learning

Quantum Machine Learning

Application: Quantum Neural Networks

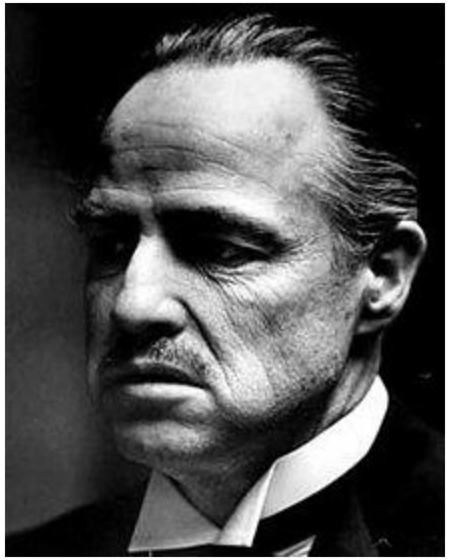
Many machine learning problems can be reduced to the minimization of a loss function through some optimization algorithm on a suitable model

Quantum Machine Learning (QML)

- Quantum Machine Learning
  - Use a quantum computer in some part a model that you wish to train
  - Use data generated by some quantum process
  - Use a quantum computer to process quantum-generated data

- Four families of QML
  - CQ – classical data training a quantum algorithm
  - QQ – quantum technologies still immature

	Classical Algorithm	**Quantum Algorithm**
Classical Data	CC	**CQ**
Quantum Data	QC	QQ



- Quantum algorithms
  - Quantum model and quantum optimization (hardware not currently ready)
  - Quantum model and classical optimization (available on NISQ devices)

- Models
  - Quantum Support Vector Machines (SVM): quantum computers mapping data to quantum states
  - Quantum Neural Networks: a full quantum model running on a quantum computer

Quantum Neural Networks

- CQ – Classical data training a quantum algorithm
  - Classical computing for the preparation of circuits and the statistical analysis of measurements
  - Quantum neural networks are “purely quantum” models

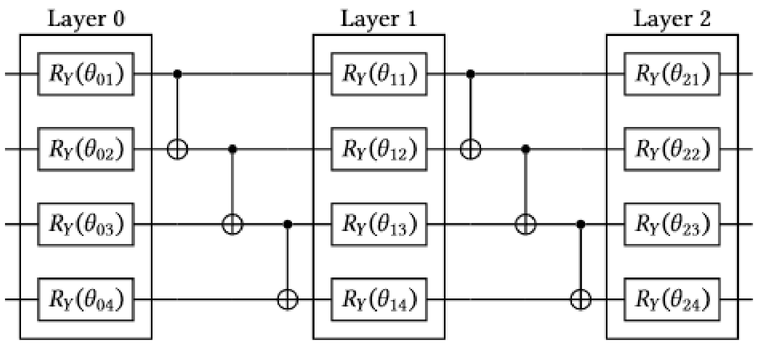
- Data input: Input nodes
  - Classical inputs mapped to quantum states through a feature map

- Data processing: Network
  - Architecture is a variational circuit dependent on optimizable parameters

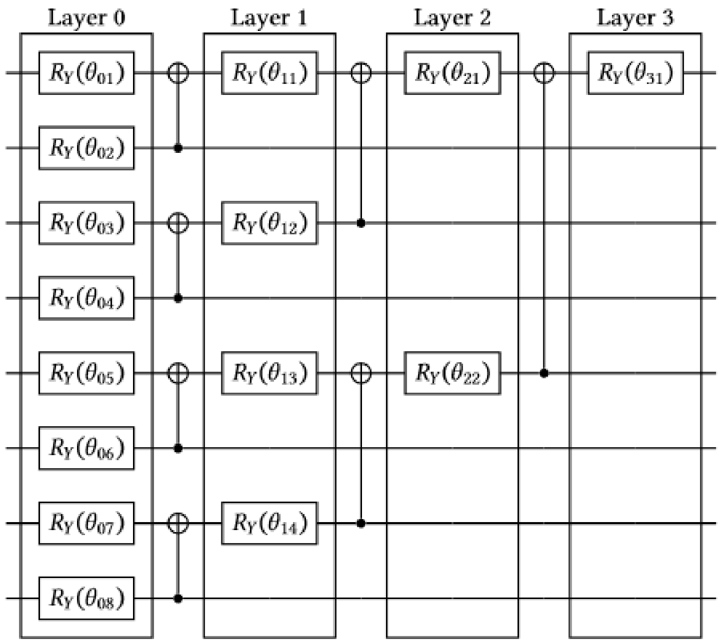
- Data output: Output nodes
  - Output is the result of a measurement operation on the final state

Quantum Neural Networks

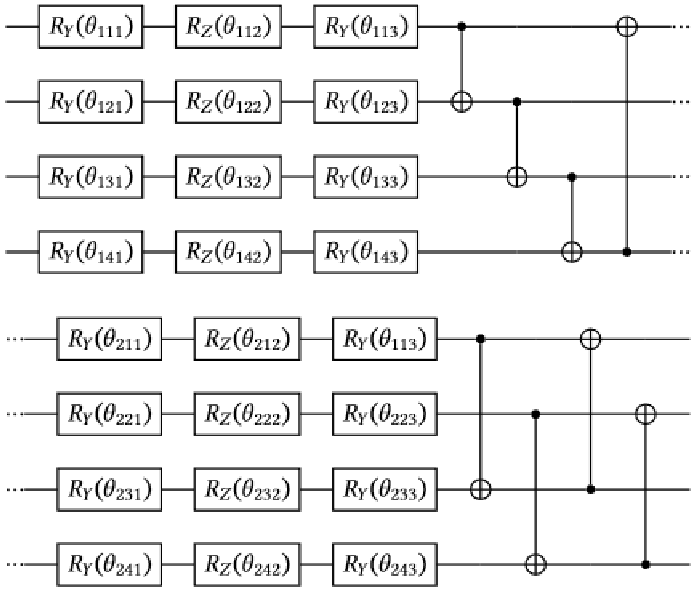
- Variational forms



Two-local Variational Form



Tree Tensor Variational Form



Strongly Entangling Layers

These variational circuits have the same "black box" explainability challenges as classical neural nets

Quantum Neural Networks

- **Measurements (classification problems)**
  - The M operator associates the eigenvalues 1 and 0 to the qubit's value being 0 and 1
  - The Z operator associates the eigenvalues 1 and −1 to the qubit's value being 0 and 1

$$M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- **Training/Optimization (Adam algorithm)**
  - Numerical approximation
  - Automatic differentiation
  - Parameter shift rule

- **Tips**
  - Feature map → variational form → measurement operation
  - Variational form: too many optimizable parameters → overfitting, too few → underfitting
  - Small learning rate → accurate/slower, higher batch size → effective optimization/slower
  - Normalize the data and consider dimensionality reduction techniques

QML provides a larger state space with the potential benefit of requiring less data

Closing

Recap

Learning Objectives

More Information

References

Learning Objectives

- *Identify* the three aspects of quantum information science
- *Describe* the difference between a quantum bit (qubit) and a classical (0/1) bit
- *Explain* how superposition facilitates quantum cryptography and makes quantum computing relevant today
- *Explain* how entanglement facilitates quantum teleportation and makes quantum computing relevant today
- *Tell* the truths about quantum computing myths
- *Identify* different computational models for quantum optimization and their applications
- *Describe* the four families of quantum machine learning and variations of quantum neural networks

For More Information on…

- …the algorithms
  - Linear algebra (almost any college text will suffice)

- …the science underlying quantum computing
  - Quantum mechanics (Griffiths' Intro to QM, Weinberg's Lectures on QM)

- …the engineering challenges
  - Noise and decoherence, error detection, and error correction (Mike & Ike)

- …practicing quantum computing code
  - Qiskit, Penny Lane, and D-Wave documentation pages
  - OpenQASM, Q#, Cirq, Bracket
  - Qirk (web-based simulator)
  - Virtual Quantum Optics Lab (quantum objects experiments) vqol.org

Quantum Computing References

- **Textbooks**
  - Quantum Computation and Quantum Information (Michael Nielsen & Isaac Chuang aka “Mike & Ike”)
  - Quantum Computing: An Applied Approach (Hidary), complementary to Mike & Ike
  - Quantum Computer Science (Mermin)
  - Quantum Computing Algorithms (Burd)
  - A Practical Guide to Quantum Machine Learning and Quantum Optimization (Combarro & Gonzalez-Castillo)
  - Programming Quantum Computers (Johnston, Harrigan, Gimeno-Segovina)
  - E-book https://www.thomaswong.net (Thomas Wong)

- **Udemy**
  - Quantum Computing Made Simple
  - QC101 Quantum Computing and Intro to Quantum Machine Learning
  - QC201 Advanced Math for Quantum Computing

Acknowledgements

Roy Scrudder
Program Manager
Modeling and Simulation Engineering
Applied Research Laboratories
The University of Texas at Austin

Brian La Cour, Ph.D.
Senior Research Scientist
Center for Quantum Research
Applied Research Laboratories
The University of Texas at Austin

Q&A

- Where are the quantum computers? Can I order one from Dell or pick one up at Best Buy?
  - Research institutions, NSA, etc.
- What do the experts think? Progress, roadblocks, etc.
  - 10, 20, 50 years? Nobody knows at this time. An over-night breakthrough may occur.
- What are the implications for managers?
  - Workforce development
  - Quantum education
  - Quantum programming jobs

- My question to you…
  - This material has been essentially at the "101" level
  - Would you like another tutorial at the "201" level?
  - Would you like an I/ITSEC Workshop with hands-on quantum computing?
- Your questions…?