CSE 392: Matrix and Tensor Algorithms for Data

Instructor: Shashanka Ubaru

University of Texas, Austin

Spring 2024

Lecture 25: Introduction to quantum computing I

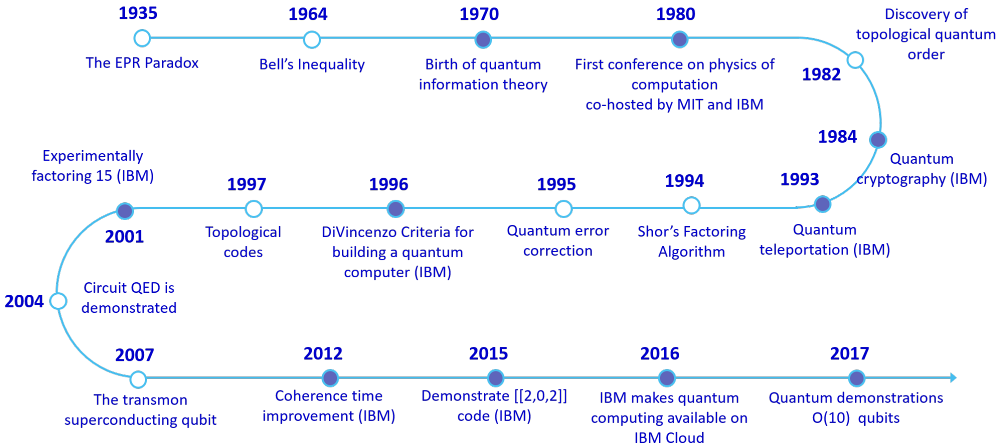
Outline

Quantum Computing Dialog

- "The **underlying physical laws** necessary for the mathematical theory of a **large part of physics** ... are **completely known**, and the **difficulty** is only that the exact application of these laws leads to **equations much too complicated** to be soluble. It therefore becomes desirable that **approximate** practical **methods** ... should be developed..." **[Dirac, 1929]**
- "I'm **not happy** with all the analysis that go with just **classical theory**, because **nature isn't classical**, dammit.
  And if you want to make a **simulation of nature**, you'd **better make it quantum mechanical**, and, by golly, it's **a wonderful problem** because it doesn't look so easy" **[Feynman 1982]**

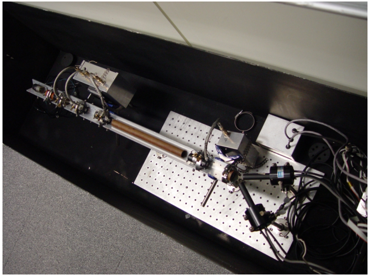
1981 Conference

History of Quantum Computing



Early History

- 1970 Quantum money (Stephen Wiesner). Unpublished until 1993
- 1981 Conference at MIT. Feynman reasoned that because quantum mechanics is hard to simulate, maybe a quantum computer would be good for simulating quantum mechanics
- 1982 No-cloning theorem (Wootters-Zurek)
- 1984 Quantum Crytography (Bennett-Brassard) "BB84"
- 1989 Quantum Key Distribution Device
- 1993 Teleportation (Bennett et. al.)
- 1994 Polynomial time factoring algorithm (Peter Shor)



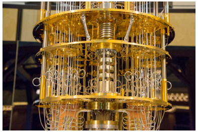
- 1995 Quantum Error-correcting codes (Calderbank-Shor)

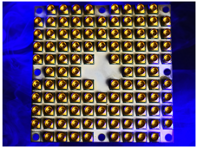
- 1996 Fault-tolerant quantum computation (Peter Shor)

- 1997 Fault-tolerant Quantum Computation with Constant Error (Aharonov-Ben Or)

Current Effort

- **Superconducting qubits**:
  - IBM: 133 qubits (Heron)
  - Google: 72 qubits (Bristlecone)
  - Rigetti 84 qubits (Ankaa-2)
  - DWave: 5760 "qubits" (quantum annealer)
- **Ion Traps**:
  - Quantinuum (32 qubits)
  - IonQ (32 qubits)
- **Photonics**:
  - USTC: 76 qubits (Jiuzhang)
  - Xanadu: 24 qubits (X24)
- Qubit count is not everything... equally and often more important is the computation **fidelity** and **connectivity**...





Future Directions

- **Quantum Advantage** (or "Supremacy") - Demonstrate a special purpose application whose output cannot be simulated as fast using existing classical computers (50-100 qubits)

Future Directions

- **Quantum Advantage** (or "Supremacy") - Demonstrate a special purpose application whose output cannot be simulated as fast using existing classical computers (50-100 qubits)

MENU **nature**

Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, [...] John M. Martinis

Nature **574**, 505–510(2019) | Cite this article

Abstract

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor[1]. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits[2,3,4,5,6,7] to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 2^{53} (about 10^{16}). Measurements from repeated experiments sample the resulting probability distribution, which we verify using classical simulations. Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy[8,9,10,11,12,13,14] for this specific computational task, heralding a much-anticipated computing paradigm.

Future Directions

- **Quantum Advantage** (or "Supremacy") - Demonstrate a special purpose application whose output cannot be simulated as fast using existing classical computers (50-100 qubits)

MENU ∨ **nature**

Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, [...] John M. Martinis

Nature **574**, 505–510(2019) | Cite this article

661k Accesses | **26** Citations | **6016** Altmetric | Metrics

Abstract

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor[1]. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits[2,3,4,5,6,7] to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 2^{53} (about 10^{16}). Measurements from repeated experiments sample the resulting probability distribution, which we verify using classical simulations. Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy[8,9,10,11,12,13,14] for this specific computational task, heralding a much-anticipated computing paradigm.

Science | Contents | News | Careers | Journals

SHARE

Google researchers in Santa Barbara, California, say their advance may lead to near-term applications of quantum computers. ISTOCK.COM/JHVEPHOTO

IBM casts doubt on Google's claims of quantum supremacy

By Adrian Cho | Oct. 23, 2019 , 5:40 AM

Future Directions

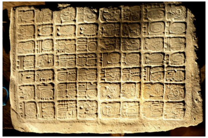
- **Quantum Advantage** (or "Supremacy") - Demonstrate a special purpose application whose output cannot be simulated as fast using existing classical computers (around 100 qubits)
- **Approximate quantum computer** - Demonstrate a useful application (quantum chemistry, optimization, ...) with a quantum device which does not need full fault tolerance (1K-5K qubits)
- **Universal fault-tolerant** quantum computer - Run useful quantum algorithms with exponential speed up over their classical counterparts (requires error correction) (1M-5M qubits)
- **Large-scale**, fault tolerant (**logical**) quantum system
- **Topological qubits**
- Find **useful** algorithms of notable **quantum advantage**

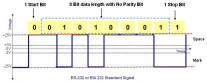
Classical Bits

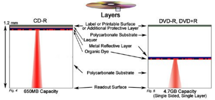
- A **bit** is a **fundamental unit of information** used in classical computation and digital communication
- A classical bit can hold the **binary** value of either 0 **or** 1, yet **not** a combination of the two
- In information theory, one **bit** is typically defined as the **information entropy** of a **binary random variable** that is 0 or 1 with **equal probability** (sometimes called a **Shannon**, but you'll never see that...)
- The state of each **classical bit**, can be set **independently** of the state of other classical bits
- The state of a register of q classical bits, can be represented by a **binary string** in $\{0, 1\}^q$
- This is a q-**dimensional space**
- The dimension of the **state-space** grows **linearly** with the number of bits

Classical Bits

- Physical representation of the abstract notion of a **bit** entity, can be by:
  - Stone tablet
  - Holes in a punch card
  - Varying levels of voltage or current
  - Magnetic field
  - Reflective vs. non-reflective spots on an optical disk
  - etc.





Single Quantum Bit - Definition

- **Definition: Computational Basis States** : A qubit has **two** special states, which in Dirac's **ket notation** are denoted by $|0\rangle$ and $|1\rangle$
- **Definition : Single Qubit Quantum State**: The state of a single **quantum bit** (aka **qubit**) can be represented as a **unitary vector** in a **2-dimensional complex** vector space, $\mathbb{C}^2$

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

  where
  - $\alpha, \beta \in \mathbb{C}$
  - $|\alpha|^2 + |\beta|^2 = 1$
  - $|0\rangle$ and $|1\rangle$ represent the basis states in $\mathbb{C}^2$ (They correspond to the classical states)
- Consider the standard unitary basis for $\mathbb{C}^2$, we can denote $|0\rangle$ by $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle$ by $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Quantum Bits - Physical Representation

- Various propositions for a **physical substrate** to represent the **abstract** notion of a **qubit**

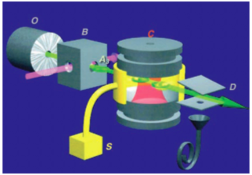
Classical

Relay

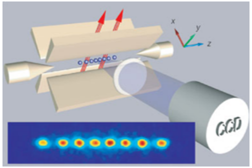
Vacuum tube

Transistor

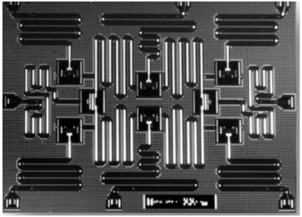
Quantum



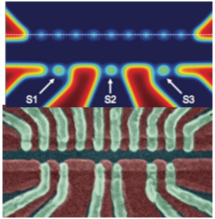
Rydberg atoms (Haroche)



Ion traps (Blatt & Wineland)



Superconducting resonators (IBM)



Quantum dots (Petta)

Quantum Bits - Tensor Product Space (Recall)

- **Definition: Tensor Product Space**: Let V and W be **vector spaces** over the field F
- Let $\{v_1, ..., v_m\} \in V$ and $\{w_1, ..., w_n\} \in W$ be **bases** of the respective spaces
- The tensor product $V \otimes W$ induces a **tensor product space** over the field F, equipped with the bi-linear operation $\otimes : V \times Q \to V \otimes W$
- The vectors $v_i \otimes w_j, \forall i = 1, ..., m, \forall j = 1, ..., n$ forms a **basis** for the **vector space** $V \otimes W$
- Considering the standard bases for the vector spaces V and W, the tensor product space becomes the **Kronecker product**

Tensor Product Properties

- **Tensor Product Properties**: Let A, $B \in \mathbb{C}^{m\times m}$ and $C, D \in \mathbb{C}^{n\times n}$ be linear transformations on V and W respectively, $v, u \in \mathbb{C}^m$, $w, x \in \mathbb{C}^n$ and $a, b \in \mathbb{C}$. The tensor product satisfies the following properties:
  - $(A \otimes C)(B \otimes D) = AB \otimes CD$
  - $(A \otimes C)(u \otimes w) = Au \otimes Cw$
  - $(u + v) \otimes w = u \otimes w + v \otimes w$
  - $u \otimes (x + w) = u \otimes w + u \otimes x$
  - $(A \otimes C)^* = A^* \otimes C^*$

Hilbert Space

- **Definition: Hilbert Space**:
  - A **Hilbert space** is a **vector space** $\mathbb{H}$ with an **inner product** $\langle x, y \rangle = x^* y$ such that the norm defined by
  $$|x| = \sqrt{\langle x, x \rangle}$$
  turns $\mathbb{H}$ into a complete metric space
  - For a **complex inner product space**, the inner product $\langle x, y \rangle$ associates a **complex number** to each pair of elements x, y of $\mathbb{H}$ while satisfying the following properties:
    - The inner product of a pair of elements is equal to the **complex conjugate** of the inner product of the **swapped elements**:
    $$\langle y, x \rangle = \overline{\langle x, y \rangle}$$
    - The inner product is **linear** in its arguments. For all complex numbers $a \in \mathbb{C}$ and $b \in \mathbb{C}$,
    $$\langle a x_1 + b x_2, y \rangle = a \langle x_1, y \rangle + b \langle x_2, y \rangle$$
    - The inner product of an element with itself is **positive definite**:
    $$\langle x, x \rangle \geq 0$$
    where the case of equality holds precisely when $x = 0$

State Representation

- **Definition: Bra-Ket Notation**:
  - Given a Hilbert space $\mathbb{H}$, a quantity $\psi \in \mathbb{H}$ enclosed in a **ket**, denoted $|\psi\rangle$, is a vector and can be thought of as a column vector
  - A quantity $\phi \in \mathbb{H}^*$ enclosed in a **bra**, denoted $\langle\phi|$, is a vector in the **dual space**, and can be thought of as a row vector that is the **conjugate transpose** of $\phi \in \mathbb{H}$
  - An **inner product** of $\langle\phi|$ and $|\psi\rangle$ in the Hilbert space $\mathbb{H}$ is denoted by $\langle\phi|\psi\rangle$
- **Notation: Standard Basis**: The standard basis for $\mathbb{C}^2$, which is a Hilbert space, is denoted by $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Bra-Ket Representation

- The bra-ket notion of a state $\alpha|0\rangle + \beta|1\rangle$ is equivalent to the previously defined representation $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, where α and β are the **amplitudes** of the $|0\rangle$ and $|1\rangle$ states respectively
- Basis vectors are **orthogonal**:

$$\langle 0|1\rangle = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0$$

- The state can be denoted as

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

- Bras and kets are essentially vectors (in dual spaces), and as such they obey the **usual rules** for vectors in vector spaces:

$$\gamma(\alpha|0\rangle + \beta|1\rangle) = \gamma\alpha|0\rangle + \gamma\beta|1\rangle \iff \gamma \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \gamma\alpha \\ \gamma\beta \end{bmatrix}$$

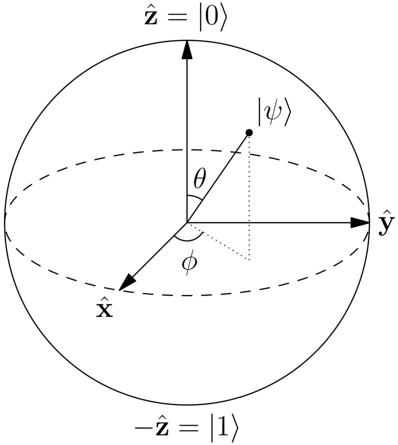
$$(\alpha_1|0\rangle+\beta_1|1\rangle)+(\alpha_2|0\rangle+\beta_2|1\rangle) = (\alpha_1+\alpha_2)|0\rangle+(\beta_1+\beta_2)|1\rangle) \iff \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}+\begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} = \begin{bmatrix} \alpha_1+\alpha_2 \\ \beta_1+\beta_2 \end{bmatrix}$$

Bloch Sphere Representation

- State space of a **single** qubit can be represented **geometrically** using the **Bloch sphere** representation
- Most general **pure** state

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

- The Bloch sphere is a **unit 2-sphere**, with **antipodal points** corresponding to a pair of **mutually orthogonal** state vectors
- **North** and **south** poles are typically chosen to correspond to the standard basis vectors $|0\rangle$ and $|1\rangle$
- **Points** on the **surface** of the sphere correspond to the **pure states** of the system, whereas **interior points** correspond to the **mixed states** (aka **density matrices**)
- **Unitary** operations correspond to **rotations** on the Bloch sphere



Multiple Qubit State

- The state of q qubits is a **unit vector** in $(\mathbb{C}^2)^{\otimes q} = \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \cdots \otimes \mathbb{C}^2}_{q \text{ times}}$
- Given the **standard basis** for each $\mathbb{C}^2$, a basis for $(\mathbb{C}^2)^{\otimes q}$ is given by:

$$
\begin{aligned}
|0\rangle &= \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{q \text{ times}} = |0B_q\rangle = |\underbrace{000\ldots0}_{q-\text{terms}}\rangle \\
|1\rangle &= \underbrace{|0\rangle \otimes \cdots \otimes |1\rangle}_{q \text{ times}} = |1B_q\rangle = |\underbrace{000\ldots1}_{q-\text{terms}}\rangle \\
&\vdots \\
|2^q - 1\rangle &= \underbrace{|1\rangle \otimes \cdots \otimes |1\rangle}_{q \text{ times}} = |(2^q - 1)B_q\rangle = |\underbrace{111\ldots1}_{q-\text{terms}}\rangle
\end{aligned}
$$

- The **state of** q **qubits** can be represented as: $|\psi\rangle = \sum_{j=0}^{2^q-1} \alpha_j |j\rangle$, with $\alpha_j \in \mathbb{C}$ and $\sum_{j=0}^{2^q-1} |\alpha_j|^2 = 1$

Postulates: State Space

- Quantum states are vectors in a **Hilbert** space, a complex vector space:

$$|\psi\rangle = \begin{bmatrix} z_1 \\ . \\ . \\ . \\ z_n \end{bmatrix}$$

- The z_i are complex numbers, called **amplitudes**
- The inner product on the vector space is defined as

$$\langle\psi'|\psi\rangle = \begin{bmatrix} z_1'^* & . & . & . & z_n'^* \end{bmatrix} \begin{bmatrix} z_1 \\ . \\ . \\ . \\ z_n \end{bmatrix} = \sum_{i=1}^{n} z_i'^* z_i$$

- States are usually normalized $\langle\psi|\psi\rangle = 1$
- Systems are combined by the **tensor product** on their Hilbert spaces: $|\Psi\rangle_{12} = |\psi\rangle_1 \otimes |\psi\rangle_2$.

Postulates: Unitarity

- Evolution is Unitary: $|\psi\rangle \to |\psi'\rangle = U|\psi\rangle$.
- U is a unitary matrix $U^\dagger U = I$ (the identity matrix).
- Therefore U is its own **inverse** $U^{-1} = U$.
- Rows and columns of U are orthonormal.

Basis States and Superposition

- **Definition: Standard Basis State**: q qubits are in a **basis state** if their state $|\psi\rangle = \sum_{j=0}^{2^q-1} \alpha_j |j\rangle$ is such that **exists** an index k for which $\alpha_k = 1$ while $\alpha_j = 0, \forall j \neq k$
- Otherwise, the qubits are in a **superposition** state

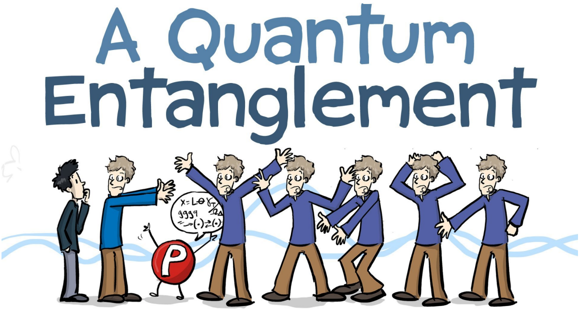
  Proposition: Basis State of Multiple Qubits: q qubits are in a **(standard) basis state if and only if** each of the individual qubits is in a **basis state**
- There is **no classical equivalent** to superposition as q classical bits are **always** in a basis state, i.e., the q bits will always correspond exactly to one of the 2^q binary strings representing the numbers $0, \ldots, 2^q - 1$
- **Superposition** is one of the unique key features of quantum computers

Product States and Entanglement - Definition

- **Definition** : A quantum state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes q}$ is a **product state** if there **exist** q single-qubit quantum states $|\psi_i\rangle \in (\mathbb{C}^2)$, $i = 1, \ldots, q$ such that

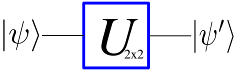
$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_q\rangle$$

- **Otherwise**, it is an **entangled** state



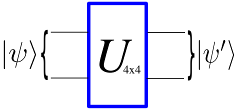
Outline of Quantum Computation

- Single qubit gates



$$|\psi'\rangle = U|\psi_{2\times 2}\rangle$$

- Multiple qubit gates



$$|\psi'\rangle = U|\psi_{4\times 4}\rangle$$

- **Universality** : **Any unitary operation** (on any number of qubits) can be decomposed in terms of arbitrary one- and two-qubit gates

Quantum Logic Gate

- **Logical gates** are the **fundamental building blocks** of **computation** and **information** processing tasks
- Similarly to **classical logical gate**, a **quantum** logic gate is a mean to **manipulate** the state of a qubit or a set of qubits
- Examples of classical gates:
  - NOT - the only single bit gate (unless identity counts...)
  - AND
  - OR
  - XOR
  - NAND
- Quantum **gate set** is more **elaborate**, and subject to several conditions

Quantum Logical Gates - Properties

- **Definition: Gate** : **Any operation** applied by a quantum computer with q qubits, also called a gate, is a **unitary** matrix in $\mathbb{C}^{2^q \times 2^q}$
- **Definition: Unitary operation** : A matrix U is **unitary** if

$$U^\dagger U = UU^\dagger = I$$

- **Property: Norm Preserving** : Unitary matrices are **norm-preserving**: given a unitary matrix U and a vector $|\psi\rangle$

$$\|U|\psi\rangle\| = \||\psi\rangle\|$$

- **State Evolution**: For a q-qubit system, the quantum **state** is a **unit vector** $|\psi\rangle \in \mathbb{C}^{2^q}$, a quantum **operation** is a **unitary matrix** $U \in \mathbb{C}^{2^q \times 2^q}$, and the **application** of U onto the **state** $|\psi\rangle$ is the **unit vector** $U|\psi\rangle \in \mathbb{C}^{2^q}$

Quantum Logical Gates - Properties

- These definitions entail the following central **properties**
  - **Linearity** : Quantum operations are **linear**
  - **Reversibility** : Quantum operations are **reversible**
- **Reversibility** : The **classical model of computation** is typically **not reversible**, as memory can be erased, yet, [Bennett, 1973] shows that computations can be **made reversible** by means of (a reasonable amount of) **extra space**
- **Turing Completeness** : While these properties may initially seem to be extremely **restrictive**, [Deutsch, 1985] shows that a **universal quantum computer** is **Turing-complete**, implying that it can **simulate any Turing-computable function**, given sufficient **time** and **memory**

The Pauli Matrices

- **Pauli Matrices** : 2×2 matrices commonly used in quantum computation (more on that in the Quantum Computation lecture)

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- The Pauli matrices form a **basis** for $\mathbb{C}^{2\times 2}$, they are Hermitian, and they satisfy the **relationship** $XYZ = iI$
- The identity operator I is sometimes omitted from the list

Single Qubit Gates - Pauli

- **Pauli Gates** : Perform π radians rotations about a principal axis upon a single qubit

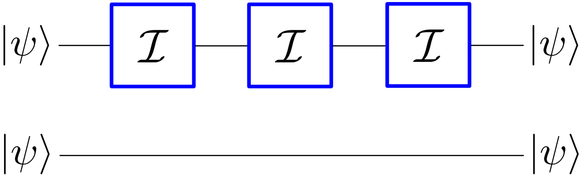
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- X and Y gates perform quantum equivalent to the classical **NOT** gate
  - X gate maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$ (**bit-flip**)
  - Z gate **flips** the **phase**, leaves $|0\rangle$ unchanged, and maps $|1\rangle$ to $-|1\rangle$
  - Y gate performs both a **bit-flip** and a **phase-flip**
- The **identity** operator I, performs an **idle** operation on a single qubit

Single Qubit Gates - Quantum Wire

- **Quantum Wire** : Trivially maintains the state of a system



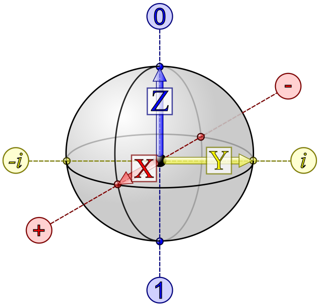
- Equivalent to application of **identity** gates **sequentially**
- In practice, **non-trivial** at all in actual quantum systems

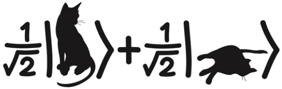
Single Qubit Gates - Hadamard Gate

- **Hadamard Gate** : Rotates by π radians about the $X + Z$ axis (which is equivalent to π about X followed by $\frac{\pi}{2}$ over the Y-axis)
- Exchanges the Z and X axes
- Maps classical states to equal-weighted **superposition** states and vice versa
  - $|0\rangle \rightarrow |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ $\qquad |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \rightarrow |0\rangle$
  - $|1\rangle \rightarrow |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ $\qquad |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \rightarrow |1\rangle$
- Represented by

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

- Self-inverse

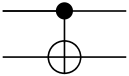




Multi Qubit Gates

- **Definition : Quantum Register** : A set of qubits grouped together
- **Controlled gates** act on 2 or more qubits, where one or more qubits act as a control for some operation
- **Controlled NOT gate** (or **CNOT**) acts on 2 qubits, and performs the NOT operation on the target qubit only when the control qubit is $|1\rangle$, and otherwise leaves it unchanged (essentially a reversible **XOR**)

$$\text{CNOT} =$$



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

- **Controlled Phase** (CPhase)
  - Same idea but target qubit is flipped around the Z axis (instead of X)
  - Equivalent to $CNOT$ up to single-qubit gates

Quantum Computation Model

- **Circuit** : The **input** to the quantum computer is a **circuit**, comprising the **instructions** as well as the **data** (unless QRAM is assumed)
- On a high level a quantum computer performs 3 tasks:
  - **State Preparation** : The state of the quantum computer is contained in a quantum register, which is initialized in a predefined way
  - **State Evolution** : The state **evolves** according to operations specified in advance according to an algorithm
  - **Quantum Measurement** : At the end of the computation, some information on the state of the quantum register is obtained by means of a special operation, called a **measurement**

Quantum Computation Model

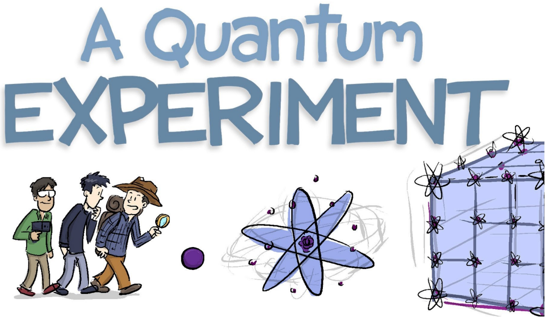
- By convention, the **initial quantum state** of the quantum computing device is $|0\rangle$
- The **input** to a quantum computing device is a **circuit**, or a set of circuits, which are then **combined** in an **algorithm**: the algorithm may be **self-contained** in the **quantum computer,** or it may involve an external, **classical computing**

Quantum Measurement

- Can we **determine** the state of a quantum system by **measurement** ?

Quantum Measurement

- Can we **determine** the state of a quantum system by **measurement** ?
- **No**, in a classical computer we can simply read the state of the bits, whereas in a quantum computer we do **not** have **direct**, **unrestricted access** to the quantum **state**
- **Partial information** regarding the quantum **state** can be gathered through a **measurement gate**



Quantum Measurement: Quantum Drill Sergeant

- Given a quantum system (e.g. a qubit) in an unknown state $|\psi\rangle = \alpha|e_1\rangle + \beta|e_2\rangle$, can we **determine** the quantum **state ?**

Quantum Measurement: Quantum Drill Sergeant

- Given a quantum system (e.g. a qubit) in an unknown state $|\psi\rangle = \alpha|e_1\rangle + \beta|e_2\rangle$, can we **determine** the quantum **state ?**
- **No!** quantum states are **not directly observable - fundamental limitation** of QM

Quantum Measurement: Quantum Drill Sergeant

- Given a quantum system (e.g. a qubit) in an unknown state $|\psi\rangle = \alpha|e_1\rangle + \beta|e_2\rangle$, can we **determine** the quantum **state ?**
- **No!** quantum states are **not directly observable - fundamental limitation** of QM

- The drill sergeant asks "Private $|\psi\rangle$, **are you** $|e_1\rangle$ or $|e_2\rangle$? "

Quantum Measurement: Quantum Drill Sergeant

- Given a quantum system (e.g. a qubit) in an unknown state $|\psi\rangle = \alpha|e_1\rangle + \beta|e_2\rangle$, can we **determine** the quantum **state ?**
- **No!** quantum states are **not directly observable - fundamental limitation** of QM

- The drill sergeant asks "Private $|\psi\rangle$, **are you** $|e_1\rangle$ or $|e_2\rangle$? "
- The poor private responds "I **don't know**, I'm a little **bit of both**"

Quantum Measurement: Quantum Drill Sergeant

- Given a quantum system (e.g. a qubit) in an unknown state $|\psi\rangle = \alpha|e_1\rangle + \beta|e_2\rangle$, can we **determine** the quantum **state ?**
- **No!** quantum states are **not directly observable - fundamental limitation** of QM

- The drill sergeant asks "Private $|\psi\rangle$, **are you** $|e_1\rangle$ or $|e_2\rangle$? "
- The poor private responds "I **don't know**, I'm a little **bit of both**"
- "I asked you a question **private**!"
- The terrified private conducts a quick **experiment**, and says "I'm $|e_1\rangle$ sir!"
- Thereafter, he remain $|e_1\rangle$...
- Measurement **collapses** the state to a **classical** state, and the amplitudes are gone

Complete Quantum Measurement

- **Attempt** to articulate the **Quantum Measurement** postulate : A quantum measurement is described by an **orthonormal basis** $|e_j\rangle$ for the state space
- If the **initial state** of the system is $|\psi\rangle$ then we get **outcome** j with probability

$$\Pr(j) = |\underbrace{\langle e_j|\psi\rangle}_{\text{amplitude}}|^2$$

- The **posterior state** is $|e_j\rangle$
- If we **expand** $|\psi\rangle = \sum_i \alpha_i |e_i\rangle$, the **amplitude** α_j can be found by the inner product

$$\langle e_j|\psi\rangle = \langle e_j| \sum_i \alpha_i |e_i\rangle = \delta_{ij}\alpha_i = \alpha_j$$

- **Problem** : **Not general** enough to describe **partial measurement**

(Partial) Measurement

- **Quantum Measurement** : A **quantum measurement** is described by a **spanning set** of **orthogonal subspaces** V_j with corresponding **projectors** Π_j (i.e. $\Pi_j \Pi_k = 0$ when $j \neq k$)
- If the initial state of the system is $|\psi\rangle$ then we get outcome j with probability

$$\Pr(j) = \langle \psi | \Pi_j^\dagger \Pi_j | \psi \rangle$$

- The posterior state is $\frac{\Pi_j |\psi\rangle}{\sqrt{\Pr(j)}}$
- The measurement operators satisfy the **completeness equation**

$$\sum_j \Pi_j^\dagger \Pi_j = I$$

- The projectors to measure a single qubit k out of a register are

$$|0\rangle\langle 0|_k \otimes I_{\bar{k}} \qquad \text{and} \qquad |1\rangle\langle 1|_k \otimes I_{\bar{k}}$$

Quantum Measurement - Principle of Uncertainty

- **Principle of Uncertainty** : Measurement **disturbs** the qubit. Following the measurement the measured qubit becomes **classical** and the original state is **no** longer **recoverable**
- The state of the quantum system after a measurement **collapses** to a **linear combination** of only those basis states that are **consistent** with the **outcome** of the measurement
- From an **information theory** standpoint, it implies that only **finite** amount of **classical information** is **storagable** in a qubit

Single Qubit Measurement

- **Single Qubit Measurement** : Given a q-qubit quantum state $|\psi\rangle = \sum_{j=0}^{2^q-1} \alpha_j |j\rangle$, a measurement gate on qubit k outputs 0 with probability $\sum_{j:(jB_q)_k=0} |\alpha_j|^2$ and 1 with probability $\sum_{j:(jB_q)_k=1} |\alpha_j|^2$
- That is summation over all j's such that the binary representation of j is 0 or 1 respectively
- Let $x \in \{0, 1\}$ be the measured value. Following the measurement, the quantum state becomes

$$\sum_{j:(jB_q)_k=x} \frac{\alpha_j}{\sqrt{\sum_{j:(jB_q)_k=x} |\alpha_j|^2}} |j\rangle$$

- **Multiple Qubit Measurement** : Given a q-qubit quantum state $|\psi\rangle = \sum_{j=0}^{2^q-1} \alpha_j |j\rangle$, measurement of the q qubits yields jB_q with probability $|\alpha_j|^2$, for $j = 0, \ldots, 2^q - 1$

Questions