

Quantum Gates & Circuits: Submodule 1

Quantum Computing using Qbits

Prof. Amlan Chakrabarti

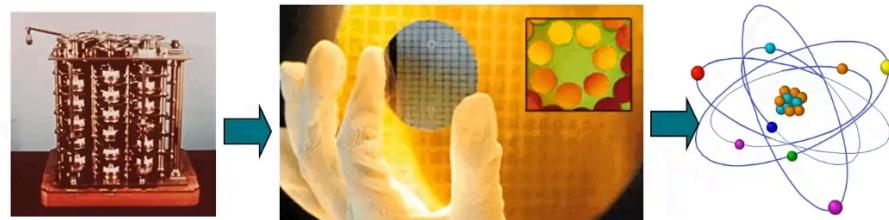
University of Calcutta

email: acakcs@caluniv.ac.in



इन्डियन इंस्टीट्यूट ऑफ एडवांस्ड कॉम्प्यूटिंग
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

Towards Quantum



Realizations are getting smaller (and faster) and reaching a point where “classical” physics is not longer a sufficient model for the laws of physics

2

इन्डियन इंस्टीट्यूट ऑफ एडवांस्ड कॉम्प्यूटिंग
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

What is Quantum Computing?

- The use of quantum mechanical principles to perform challenging computational tasks is called quantum computation.
- The quantum phenomenon like entanglement and superposition make it possible for low cost computation to happen.



इन्डियन इंस्टीट्यूट ऑफ एडवांस्ड कॉम्प्यूटिंग
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

5 December 2023: IBM Releases First-Ever 1,000-Qubit Quantum Chip

<https://www.scientificamerican.com/article/ibm-releases-first-ever-1-000-qubit-quantum-chip/>

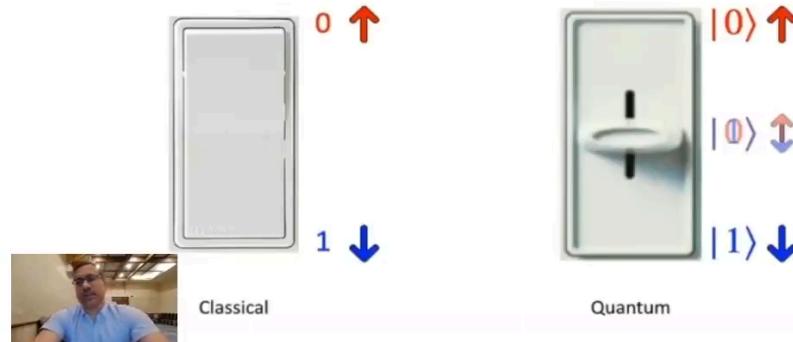


of Quantum Computing: Quantum Computing Qubits should double every 2 years!

 Centre for Development of Advanced Computing

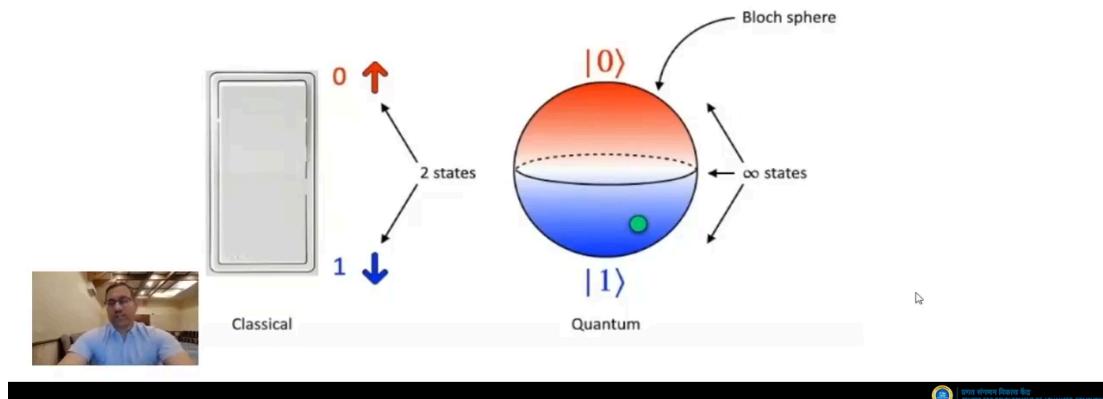
<https://www.scientificamerican.com/article/ibm-releases-first-ever-1-000-qubit-quantum-chip/#:~:text=IBM%20has%20unveiled%20the%20first,error%2Dresistant%20rather%20>

Classical bits vs Qubits



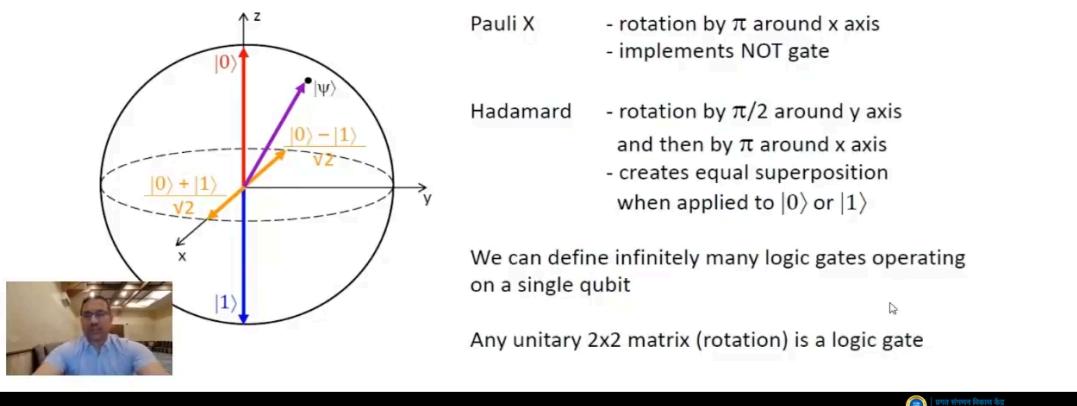
 Centre for Development of Advanced Computing

Classical bits vs Qubits

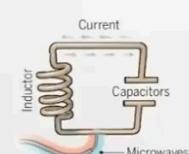


Computation-Transformation of the Memory State

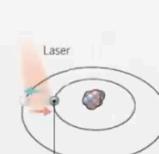
1-qubit logic gates: rotations around x, y and z axes



Qubit = A Quantum Bit



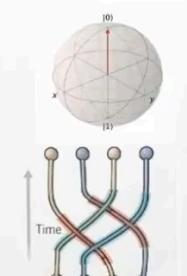
Superconducting loops
Google, IBM, Rigetti, DWave



Trapped ions
Honeywell, IonQ



Silicon quantum dots
Intel Corporation, HRL

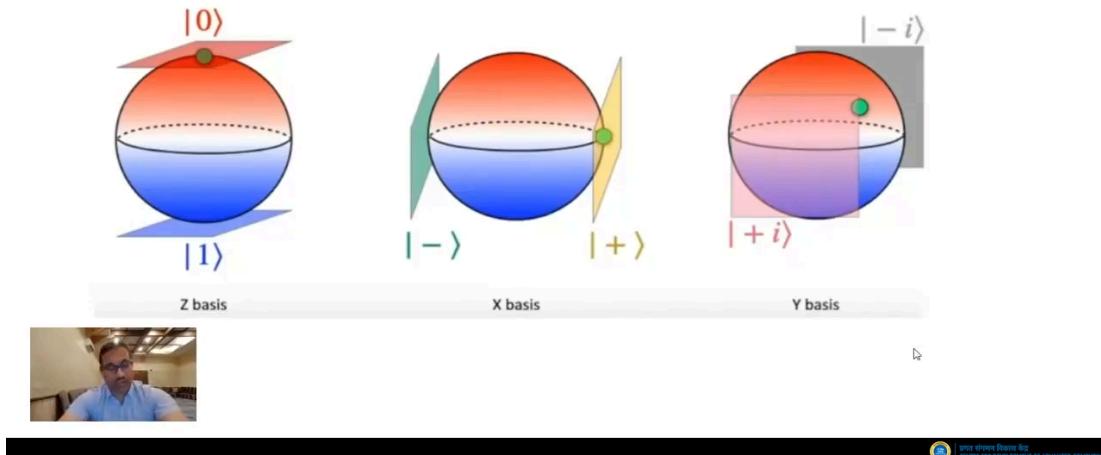


Topological qubits
Microsoft

DOI: 10.1126/science.354.6316.1090



Most Important Basis for Measurement



The Postulates of Quantum Mechanics

Postulate 1: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.

Postulate 2: The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2 , $U|\psi\rangle = |\psi'\rangle$.

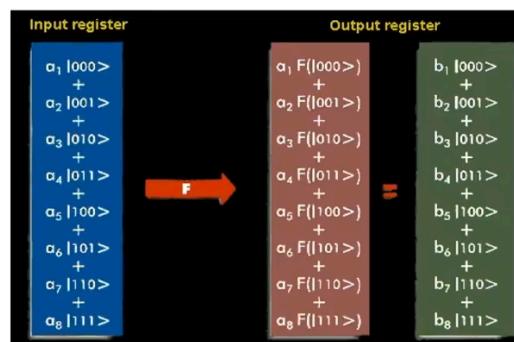
Postulate 3: Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$, and the state of the system after the measurement is $\frac{M_m|\psi\rangle}{\sqrt{p(m)}}$.

The measurement operators satisfy the *completeness equation*, $\sum_m M_m^\dagger M_m = I$.

 The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems 1 through n , and system number i , is prepared in the state $|\psi_i\rangle$, then the total system is $|\psi_1\rangle \oplus |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle$.



Why Is This Helpful?



- Multiple computations simultaneously
- Computing power is exponential



It's the Scaling

- The Quantum State Space becomes 2^n large in the number of qubits, this translates a huge energy advantage.
- The energy efficiency will scale exponentially with the increase in qubits



	CLASSICAL COMPUTING	QUANTUM COMPUTING
COMPUTING UNITS	Calculates with transistors, which can take two levels 0 and 1	
COMPUTING CAPACITY	Capability increased linearly (1:1) with number of transistors	
ERROR RATES & ENVIRONMENT	Low error rates. Can operate at room temperature	
SUITABILITY	Suitable for routine processing.	

Centre for Development of Advanced Computing

Quantum Algorithms



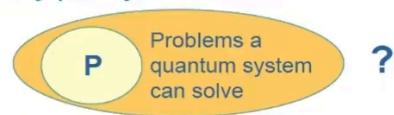
Richard Feynman



David Deutsch



- Feynman (1982): there may be quantum systems that cannot be simulated efficiently on a “classical” computer
- Deutsch (1985): proposed that machines using quantum processes might be able to perform computations that “classical” computers can only perform very poorly



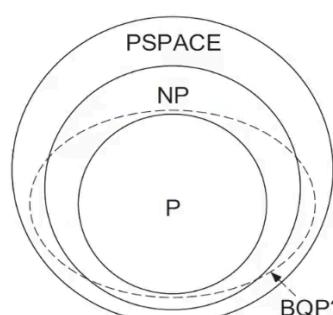
- Concept of *quantum computer* emerged as a universal device to execute such quantum algorithms

BQP (Bounded-Error Quantum Polynomial-Time): Class of problems solvable efficiently by a quantum computer

12

Centre for Development of Advanced Computing

The Power of Quantum Computation



P = solved in polynomial time
NP = verified in polynomial time
PSPACE = solved in polynomial space

BQP?

BQP (bounded error quantum polynomial time) is the class of decision problems solvable by a quantum computer in polynomial time, with an error probability of at most 1/3 for all instances.



Centre for Development of Advanced Computing

Quantum Computing Can Perform Better

Quantum Computing: Thrust Areas

- Quantum Technology
 - Quantum Algorithms
 - Quantum Modelling and Simulation
 - Quantum Communication and Cryptography



15



Quantum Gates & Circuits: Submodule 1

Basic Quantum Gates

Prof. Amlan Chakrabarti
University of Calcutta
email: acakcs@caluniv.ac.in



- **Qubit vs. Bit:**

Bit (Classical) degree of freedom that can take only two possible values.

- **Qubit**

- Quantum observable whose spectrum contains two values {0,1}.
- Minimal quantum physical system.
- The boolean observable of a qubit system is called a sharp observable, as it can have only values 0 and 1.
- A qubit can have another observable which has an equal probability of 1 and 0, individual probabilities summed will result to unity.
- **Qubit in reality:**
 - Electron spin (up or down)
 - Photon polarization (horizontal/vertical)
 - Spin of atomic nucleus
 - Current in a super conducting loop
 - Presence/absence of a particle



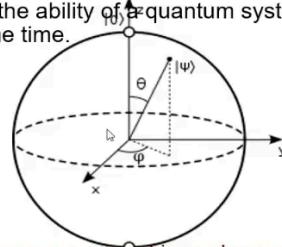
18

 IIT Madras Centre for Development of Advanced Computing

Quantum Phenomenon: Superposition and Entanglement

- **Superposition**

- Superposition is the ability of a quantum system to be in multiple states at the same time.



19

 IIT Madras Centre for Development of Advanced Computing

Computation with Qubits

How does the use of qubits affect computation?

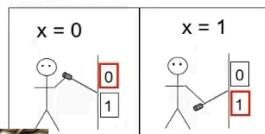
Classical Computation

Data unit: bit

 = '1'  = '0'

Valid states:

$x = '0'$ or $'1'$



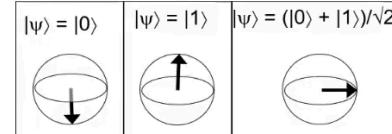
Quantum Computation

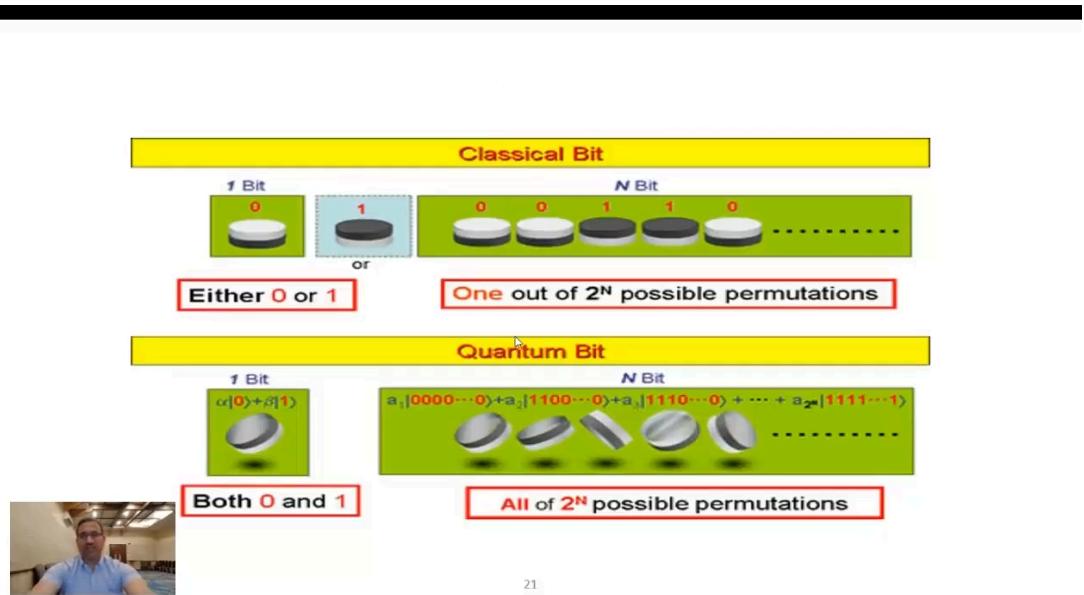
Data unit: qubit

 = $|1\rangle$  = $|0\rangle$

Valid states:

$|\psi\rangle = c_1|0\rangle + c_2|1\rangle$





21

Centre for Development of Advanced Computing

Entanglement

- An n-qubit system can exist in any superposition of the 2^n basis states

$$c_0|00 \dots 00\rangle + c_1|00 \dots 01\rangle + \dots + c_{2^n-1}|11 \dots 11\rangle, \quad \sum_{i=0}^{2^n-1} |c_i|^2 = 1$$

- If such a state can be represented as a tensor product of individual qubit states then the qubit states are **not entangled**. For example:

$$\left(\underbrace{\frac{1}{\sqrt{8}}|00\rangle + \frac{\sqrt{3}}{\sqrt{8}}|01\rangle + \frac{1}{\sqrt{8}}|10\rangle + \frac{\sqrt{3}}{\sqrt{8}}|11\rangle}_{2^n \text{ probability amplitudes}} \right) = \left(\underbrace{\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle}_{2n \text{ probability amplitudes}} \right) \otimes \left(\underbrace{\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle}_{2n \text{ probability amplitudes}} \right)$$

$$\left(a|0\rangle + b|1\rangle \right) + \left(c|0\rangle + \frac{1}{\sqrt{2}}|11\rangle \right) \neq (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$

Centre for Development of Advanced Computing

Quantum Logic Networks

- Invented by Deutsch (1989)
 - Analogous to classical Boolean logic networks
 - Generalization of Fredkin-Toffoli reversible logic circuits
- System is divided into individual bits, or *qubits*
 - 2 orthogonal states of each qubit are designated as the *computational basis states*, "0" and "1"
- Quantum logic gates:
 - Local unitary transforms that operate on only a few state bits at a time
- Computation via predetermined sequence of gate applications to selected bits



23

Centre for Development of Advanced Computing

Quantum Gates: NOT

- All classical input-consuming reversible gates can be represented as unitary transformations!

- *E.g., input-consuming NOT gate (inverter)*



in	out
0	1
1	0

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{matrix} 0 \\ 1 \end{matrix} \quad N \equiv \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \begin{matrix} 0 \\ 1 \end{matrix} \quad N|0\rangle = |1\rangle$$

$$|1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{matrix} 0 \\ 1 \end{matrix} \quad N|1\rangle = |0\rangle$$



24

The Hadamard Transform

- Used frequently in quantum logic networks for generating Superpositions

$$H \equiv \begin{bmatrix} 0 & 1 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 1 & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{matrix} 0 \\ 1 \end{matrix} \quad H^2 = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$



25

One Qbit Logic Gates

$$X (\text{NOT}) \quad Y \quad Z \quad S$$

$$\begin{matrix} 0 & 1 \\ 0 & 1 \end{matrix} \quad \begin{matrix} 0 & 1 \\ 0 & -i \end{matrix} \quad \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \quad \begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}$$

$$\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \quad \begin{matrix} 1 & 0 \\ i & 0 \end{matrix} \quad \begin{matrix} 1 & 0 \\ 0 & -1 \end{matrix} \quad \begin{matrix} 1 & 0 \\ 0 & i \end{matrix}$$

$$T \quad \text{Hadamard (H)} \quad \text{Sqrt NOT}$$

$$\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \quad \begin{matrix} 0 & 1 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{matrix} \quad \begin{matrix} 0 & 1 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{matrix}$$

$$\begin{matrix} 0 & 1 \\ 0 & e^{i\pi/4} \end{matrix} \quad \begin{matrix} 1 & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{matrix} \quad \begin{matrix} 1 & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{matrix}$$



Identity transformation, Pauli matrices, Hadamard

$$\delta_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

$$\delta_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$|\varphi\rangle = \alpha_1|0\rangle + \alpha_0|1\rangle$$

$$\delta_2 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$|\varphi\rangle = -i\alpha_1|0\rangle + i\alpha_0|1\rangle$$

$$\delta_3 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$|\varphi\rangle = \alpha_0|0\rangle - \alpha_1|1\rangle$$



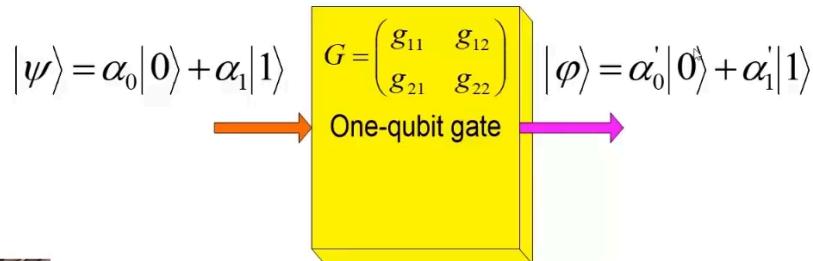
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$|\varphi\rangle = \alpha_0 \frac{|0\rangle + |1\rangle}{\sqrt{2}} + \alpha_1 \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

27

One qubit gates

- Transform an input qubit into an output qubit
- Characterized by a 2×2 matrix with complex coefficients

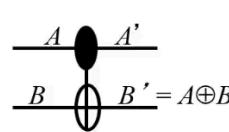


$$|\varphi\rangle = G|\psi\rangle \quad \begin{pmatrix} \alpha'_0 \\ \alpha'_1 \end{pmatrix} = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

28

Controlled-NOT

- A.k.a. CNOT (or input-consuming XOR)



$$\begin{array}{cc|cc} A & B & A' & B' \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{array}$$

00 01 10 11

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

Example:

$$X|\mathbf{10}\rangle = |\mathbf{11}\rangle$$



In a CNOT (Controlled-NOT) gate in quantum computing, measuring one qubit can indeed provide information about the other qubit, depending on the state of the measured qubit and the entanglement between the qubits.

Explanation:

1. Entanglement in CNOT Gate:

In a CNOT gate, two qubits are involved: a control qubit (usually denoted as q_{control}) and a target qubit (usually denoted as q_{target}).

If the control qubit is in the state $|1\rangle$, it flips the state of the target qubit. If the control qubit is in the state $|0\rangle$, the target qubit remains unchanged.

2. Measurement and Entanglement:

When two qubits are entangled, measuring one qubit can instantaneously affect the state of the other qubit.

If we measure the control qubit, and it collapses to $|0\rangle$ or $|1\rangle$, we instantly know the state of the target qubit, as it will be flipped or remain the same, respectively.

3. Example:

Let's say we have a CNOT gate with qubit q_{control} as the control qubit and q_{target} as the target qubit.

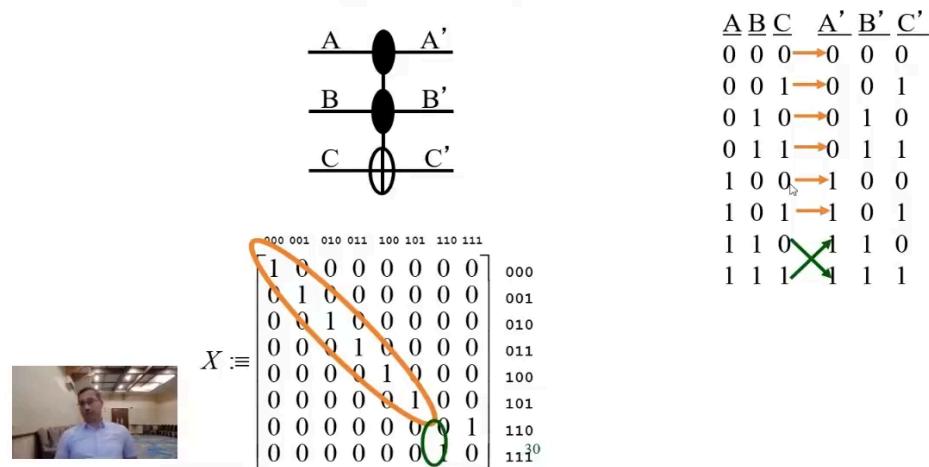
If q_{control} is in the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and q_{target} is in the state $|0\rangle$ before measurement.

If we measure q_{control} and it collapses to $|0\rangle$, then q_{target} remains $|0\rangle$. If it collapses to $|1\rangle$, then q_{target} flips to $|1\rangle$.

Conclusion:

In summary, measuring one qubit in a CNOT gate can provide information about the state of the other qubit due to their entanglement. This property is fundamental in quantum computing and can be used for various quantum information processing tasks, including quantum teleportation and quantum error correction.

Toffoli Gate (CCNOT)



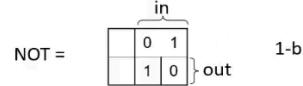
Computation with Qubits

How does the use of qubits affect computation?

Classical Computation

Operations: logical

Valid operations:



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

Quantum Computation

Operations: unitary

Valid operations:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\sigma_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \quad H_d = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

2-qubit

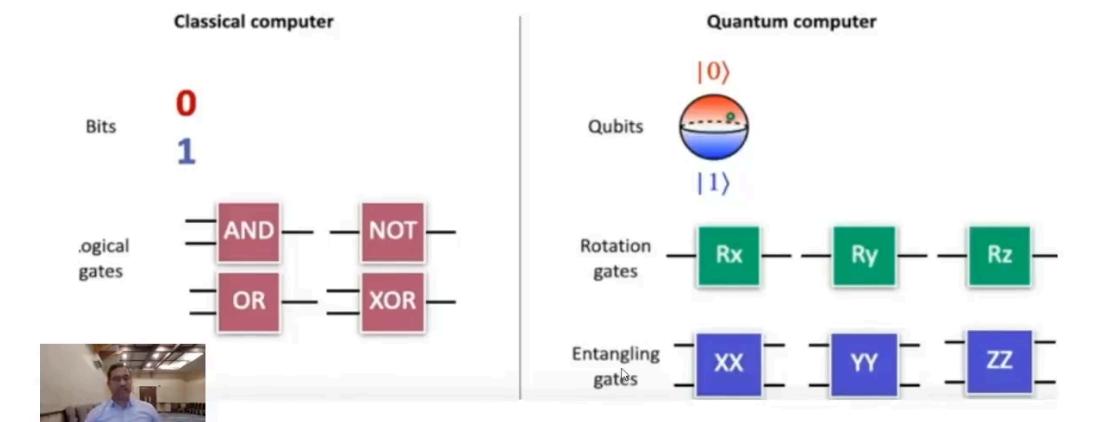
CNOT = $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

More than one qubit

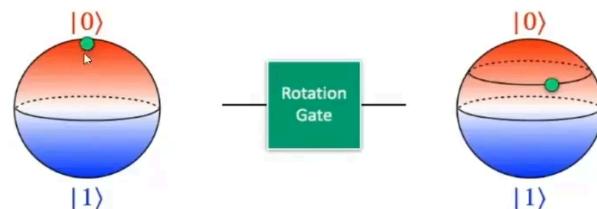
	Single qubit	Two qubits
Hilbert space	$ \psi\rangle = \begin{pmatrix} 0\rangle \\ 1\rangle \end{pmatrix}$	$\mathcal{H}_2^{\otimes 2} = \mathcal{H}_2 \otimes \mathcal{H}_2 = \begin{pmatrix} 00\rangle \\ 01\rangle \\ 10\rangle \\ 11\rangle \end{pmatrix} = \begin{pmatrix} 0\rangle \\ 1\rangle \\ 0\rangle \\ 1\rangle \end{pmatrix} \begin{pmatrix} 0\rangle \\ 1\rangle \\ 0\rangle \\ 1\rangle \end{pmatrix}$
Arbitrary state	$ \psi\rangle = c_1 0\rangle + c_2 1\rangle = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$	$ \Psi\rangle = c_1 00\rangle + c_2 01\rangle + c_3 10\rangle + c_4 11\rangle = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix}$
Operator	$U \psi\rangle = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$	$U \Psi\rangle = \begin{pmatrix} U_{11} & U_{12} & U_{13} & U_{14} \\ U_{21} & U_{22} & U_{23} & U_{24} \\ U_{31} & U_{32} & U_{33} & U_{34} \\ U_{41} & U_{42} & U_{43} & U_{44} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix}$



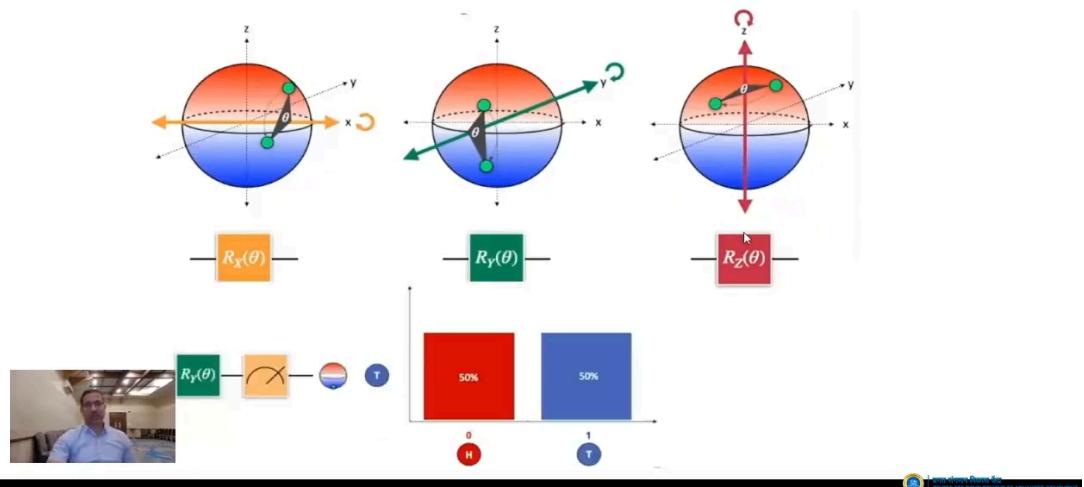
Bits, Qubits and Gates



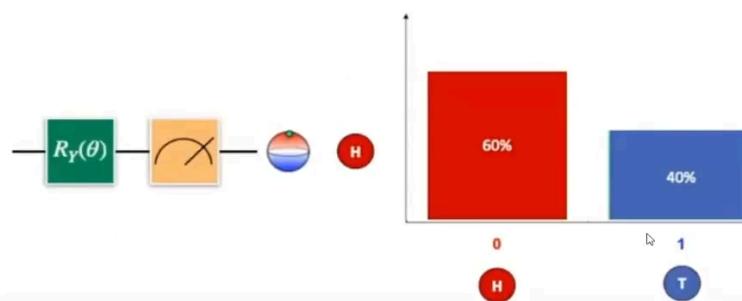
Rotation Gates: Qubit Transformations



Rotation Gates: Qubit Transformations



Rotation with Bias



Physical Machine Descriptions (PMDs)

- Technology for a given quantum implementation
- Quantum gate implementation is achieved by means of supported quantum operations
- Variability among the PMDs
 - primitive quantum operations
 - related cost
- Commonly known PMDs
 - Quantum dot (QD)
 - Superconducting (SC)
 - Ion trap (IT)
 - Neutral atom (NA)
 - Linear photonics (LP)
 - Nonlinear photonics (NP)



Minimal Set of 1-qubit gates

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = P\left(\frac{\pi}{2}\right)R_x(\pi) = iR_x(\pi)$$

$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = P\left(\frac{\pi}{2}\right)R_y(\pi) = iR_y(\pi)$$

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = P\left(\frac{\pi}{2}\right)R_z(\pi) = iR_z(\pi)$$

- Any two of $\{R_x, R_y, R_z\}$ can be converted into the third one

$$R_x(\theta) = R_z\left(-\frac{\pi}{2}\right) \cdot R_y(\theta) \cdot R_z\left(\frac{\pi}{2}\right)$$



- Quantum Logic Circuits**

- Circuit behavior is governed explicitly by quantum mechanics
- Signal states are vectors interpreted as a superposition of binary “qubit” vectors with complex-number coefficients

$$|\Psi\rangle = \sum_{i=0}^{2^n-1} c_i |i_{n-1}i_{n-2}\dots i_0\rangle$$

- Operations are defined by linear algebra over Hilbert Space and can be represented by unitary matrices with complex elements
- Severe restrictions exist on copying and measuring signals
- Many universal gate sets exist but the best types are not obvious



Quantum Circuit Characteristics

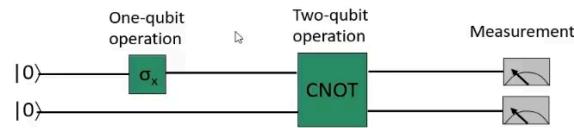
- Unitary Operations**

- Gates and circuits must be reversible (information-lossless)
 - Number of output signal lines = Number of input signal lines
 - The circuit function must be a bijection, implying that output vectors are a permutation of the input vectors
- Classical logic behavior can be represented by permutation matrices
- Non-classical logic behavior can be represented including state sign (phase) and entanglement



Quantum Circuit Model

Example Circuit



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

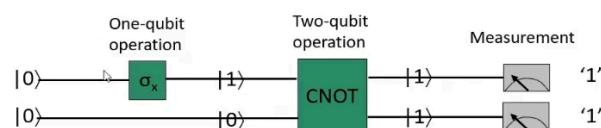
$$\sigma_x \otimes I = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



Centre for Development of Advanced Computing

Quantum Circuit Model

Example Circuit



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

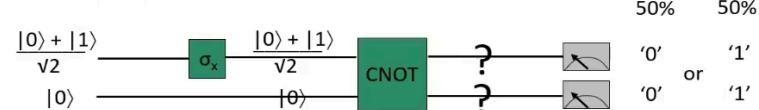
$$\sigma_x \otimes I = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



Centre for Development of Advanced Computing

Quantum Circuit Model

Example Circuit



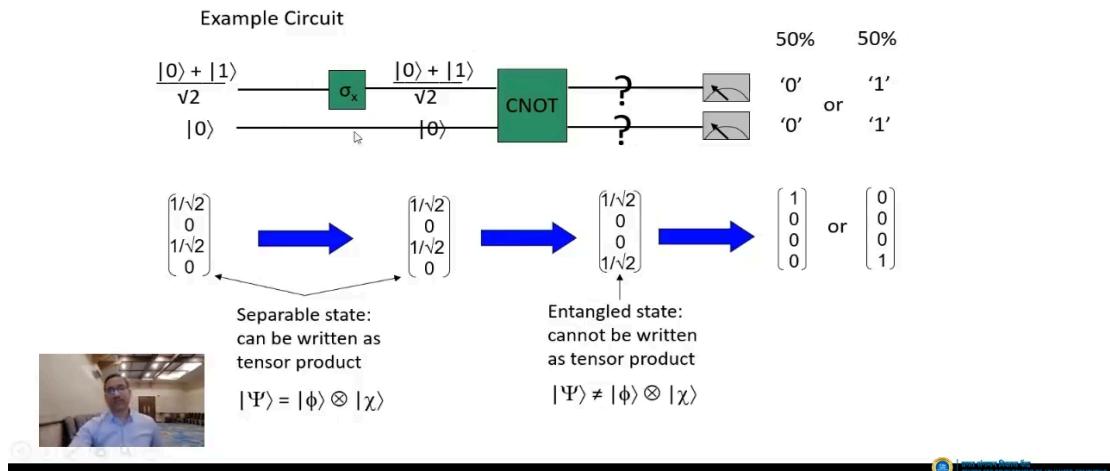
$$\begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 1/\sqrt{2} \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 1/\sqrt{2} \\ 0 \end{bmatrix} \quad \begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{bmatrix} \quad \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$



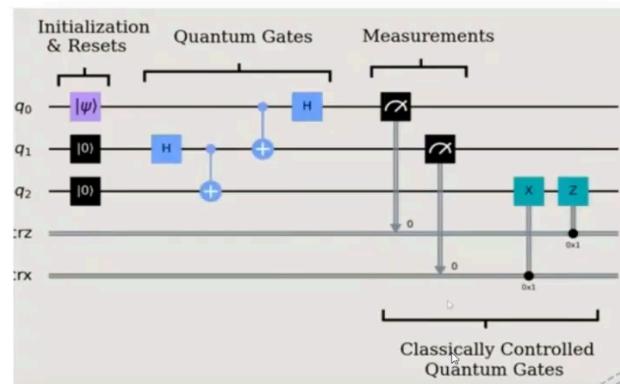
Centre for Development of Advanced Computing

Quantum Circuit Model



Quantum Computing Group

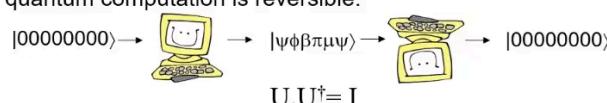
Quantum Circuits



Some Interesting Consequences

Reversibility

Since quantum mechanics is reversible (dynamics are unitary), quantum computation is reversible.

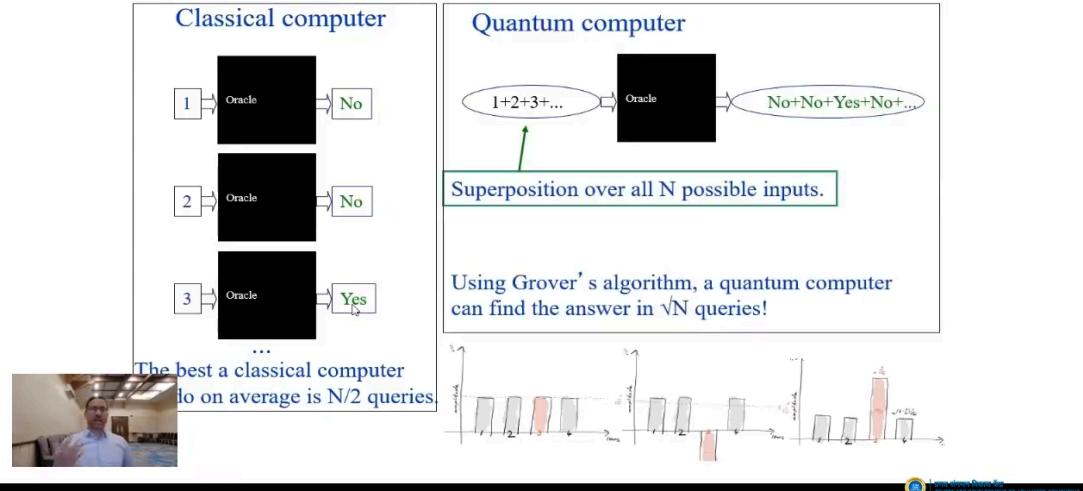


No cloning theorem

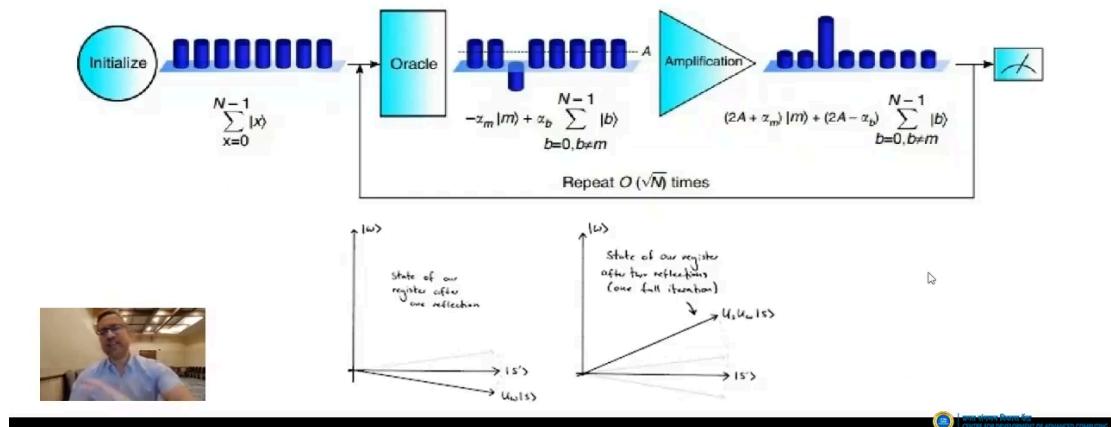
It is impossible to exactly copy an unknown quantum state



Grover's Search Algorithm

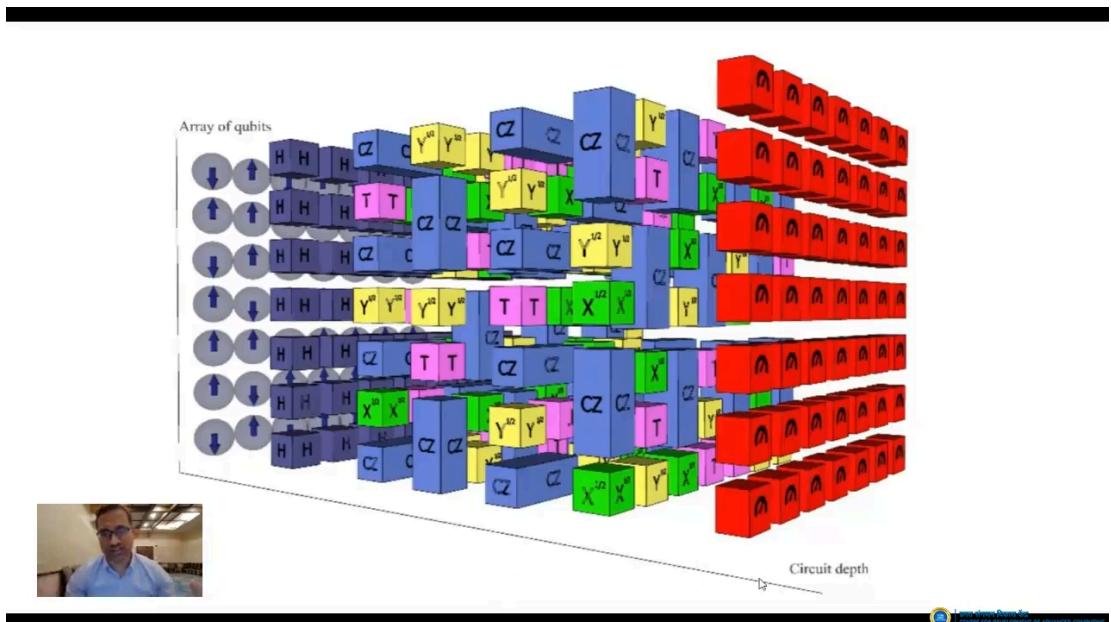


- Grover's Search Algorithm



Qiskit Textbook (Algorithms) -
<https://github.com/Qiskit/textbook/tree/main/notebooks/ch-algorithms>

Large scale Quantum Circuit



Transpilation - <https://docs.quantum.ibm.com/api/qiskit/transpiler>

Transpilation

