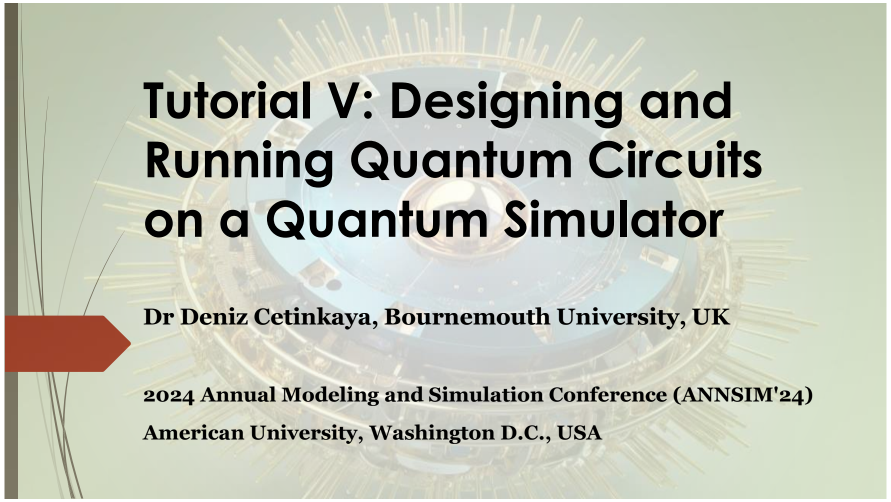
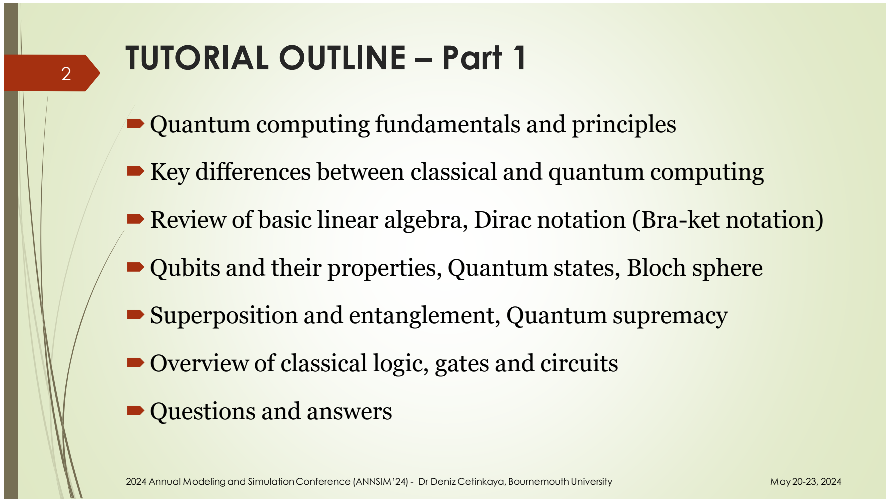


Tutorial V: Designing and Running Quantum Circuits on a Quantum Simulator

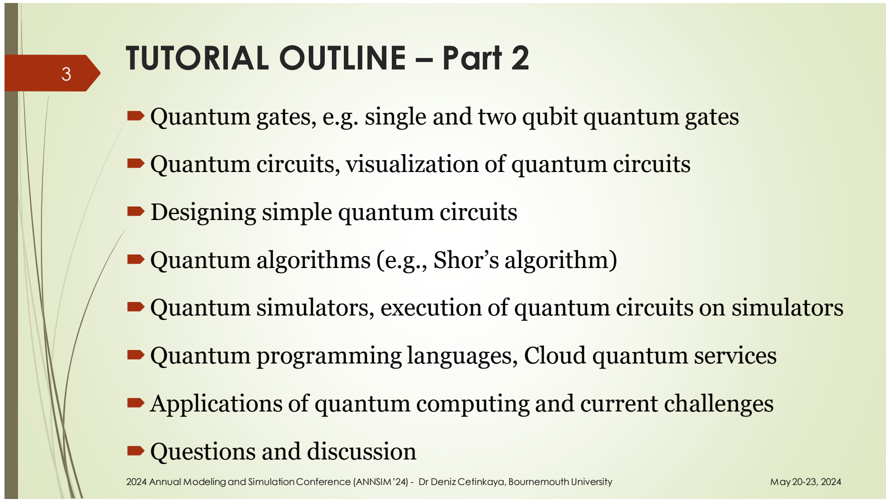
Dr Deniz Cetinkaya, Bournemouth University, UK

2024 Annual Modeling and Simulation Conference (ANNSIM'24)
American University, Washington D.C., USA



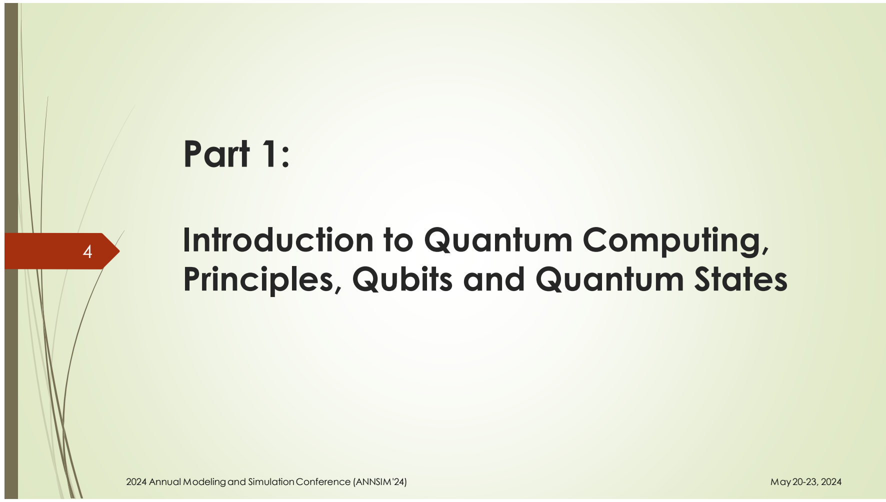
TUTORIAL OUTLINE – Part 1

- Quantum computing fundamentals and principles
- Key differences between classical and quantum computing
- Review of basic linear algebra, Dirac notation (Bra-ket notation)
- Qubits and their properties, Quantum states, Bloch sphere
- Superposition and entanglement, Quantum supremacy
- Overview of classical logic, gates and circuits
- Questions and answers



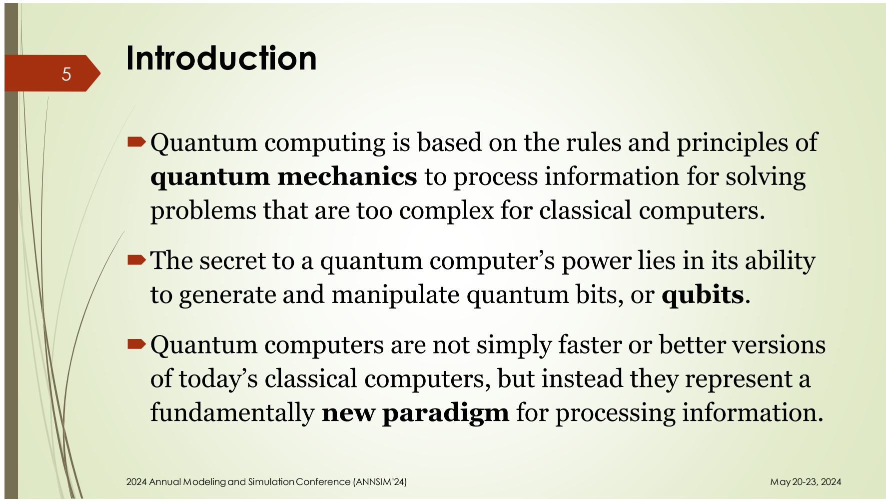
TUTORIAL OUTLINE – Part 2

- Quantum gates, e.g. single and two qubit quantum gates
- Quantum circuits, visualization of quantum circuits
- Designing simple quantum circuits
- Quantum algorithms (e.g., Shor's algorithm)
- Quantum simulators, execution of quantum circuits on simulators
- Quantum programming languages, Cloud quantum services
- Applications of quantum computing and current challenges
- Questions and discussion



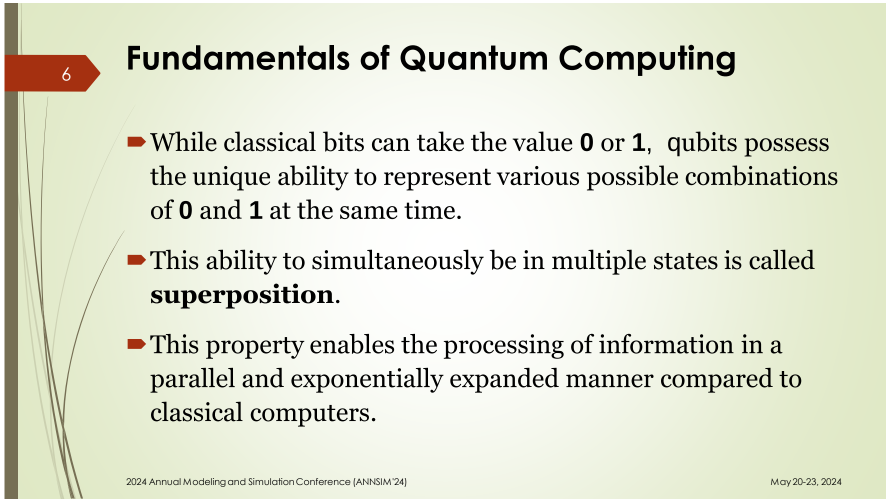
Part 1:

Introduction to Quantum Computing, Principles, Qubits and Quantum States



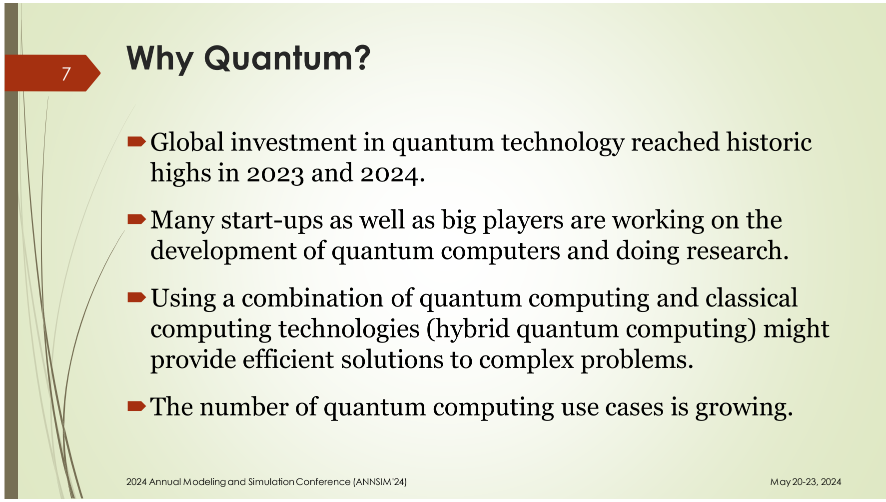
Introduction

- Quantum computing is based on the rules and principles of **quantum mechanics** to process information for solving problems that are too complex for classical computers.
- The secret to a quantum computer's power lies in its ability to generate and manipulate quantum bits, or **qubits**.
- Quantum computers are not simply faster or better versions of today's classical computers, but instead they represent a fundamentally **new paradigm** for processing information.



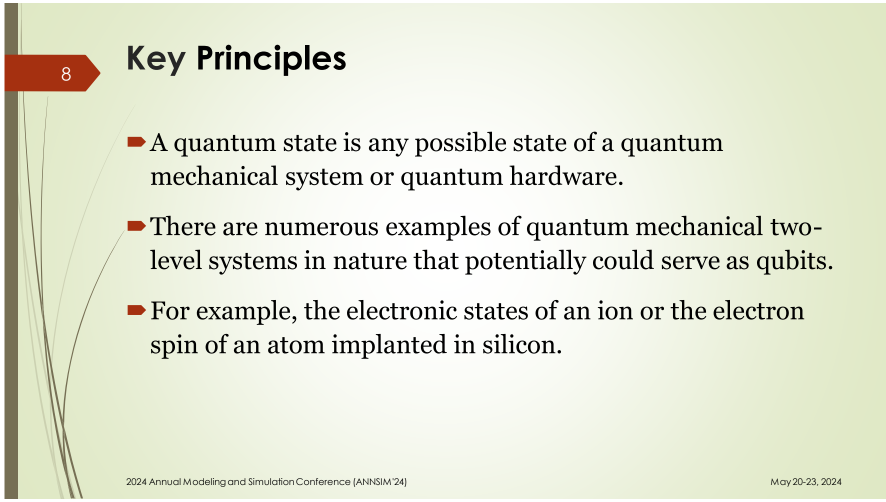
Fundamentals of Quantum Computing

- While classical bits can take the value **0** or **1**, qubits possess the unique ability to represent various possible combinations of **0** and **1** at the same time.
- This ability to simultaneously be in multiple states is called **superposition**.
- This property enables the processing of information in a parallel and exponentially expanded manner compared to classical computers.



Why Quantum?

- Global investment in quantum technology reached historic highs in 2023 and 2024.
- Many start-ups as well as big players are working on the development of quantum computers and doing research.
- Using a combination of quantum computing and classical computing technologies (hybrid quantum computing) might provide efficient solutions to complex problems.
- The number of quantum computing use cases is growing.



Key Principles

- A quantum state is any possible state of a quantum mechanical system or quantum hardware.
- There are numerous examples of quantum mechanical two-level systems in nature that potentially could serve as qubits.
- For example, the electronic states of an ion or the electron spin of an atom implanted in silicon.

Quantum Computers

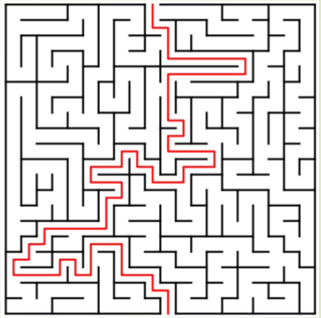
- There are many companies such as IBM, Microsoft, Google, Amazon, D-Wave, Rigetti Computing, IonQ, Quantiuum, Xanadu, etc. which are developing quantum computers and technologies.
- Quantum computers are built using various hardware technologies whereas the main types are superconducting circuits, photonic networks, trapped ions, quantum dots, etc.
- Superconducting and trapped ions are the commonly used ones.

Note that …

- A quantum computer is not just a more powerful kind of computer.
- It is a different kind of computer based on a completely different technology.
- Quantum supremacy is the goal for a quantum computer that could perform calculations that are not possible with classical computers.

Thinking in Quantum World

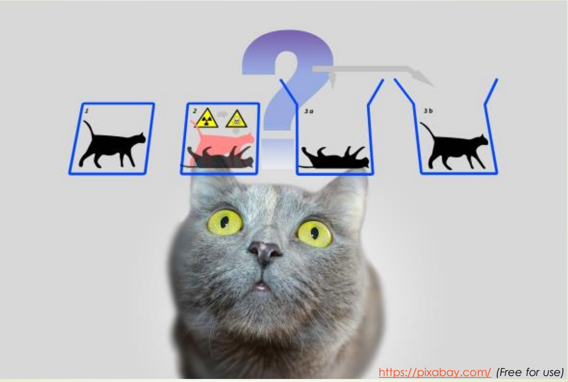
- Consider the problem of finding the correct path in a maze.
- A typical solution with classical computers would be trying every possible path one by one and optimising the number of trials in the best case.
- The main point in quantum thinking is to understand that we can try every possible path at the same time.



Classical vs. Quantum Computing

Feature	Quantum	Classical
Theory	Quantum mechanics	Classical physics
Technology	Superconducting loops, trapped ions, quantum dots, etc.	Transistors
Information storage	Qubits	Bits
Computation	Probabilistic	Deterministic
Operations	Linear algebra operations	Boolean algebra operations
System state	Continuous possible states in superposition	Discrete number of possible states
Error rate	High	Low
Environment	Ultra cold	Room temperature
Applications	Complex problems, optimisation, simulation	General purpose
Computing power	Exponential growth	Linear growth
Processing	QPU	CPU

Schrödinger's cat



https://pixabay.com/ (Free for use)

Overview of Basic Linear Algebra

- Linear algebra is the study of lines and planes, vector spaces, matrices and mappings that are required for linear transforms.
- A vector has a magnitude and direction.
- Matrix is an arrangement of numbers into rows and columns.

$$M = \begin{bmatrix} 5 & 3 & 7 \\ 6 & 4 & 8 \end{bmatrix}$$

Matrix Multiplication

- If A is an m×n matrix and B is an n×p matrix, the matrix product C=AB is defined to be the m×p matrix.
- e.g.:

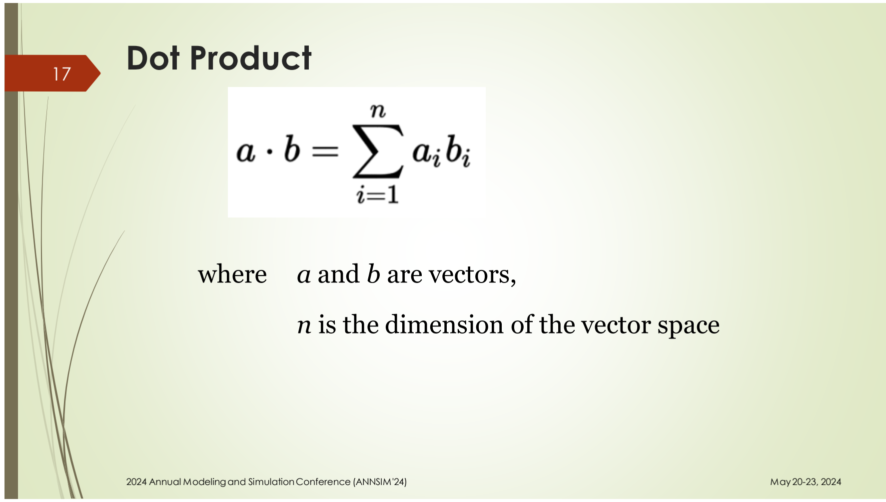
$$A = \begin{bmatrix} 5 & 3 & 7 \\ 6 & 4 & 8 \end{bmatrix} \qquad B = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$$

$$C = \begin{bmatrix} 5*1+3*2+7*3 \\ 6*1+4*2+8*3 \end{bmatrix} = \begin{bmatrix} 32 \\ 38 \end{bmatrix}$$

Matrix Transpose

- The transpose of a matrix A is the flipped version of the original matrix by interchanging the rows and columns.
- e.g.:

$$A = \begin{bmatrix} 5 & 3 & 7 \\ 6 & 4 & 8 \end{bmatrix} \qquad A^T = \begin{bmatrix} 5 & 6 \\ 3 & 4 \\ 7 & 8 \end{bmatrix}$$

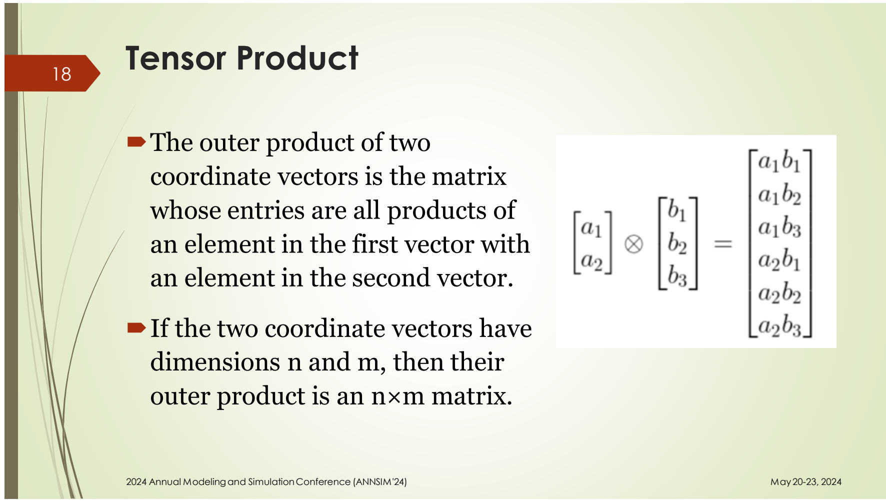


Dot Product

$$a \cdot b = \sum_{i=1}^{n} a_i b_i$$

where a and b are vectors,

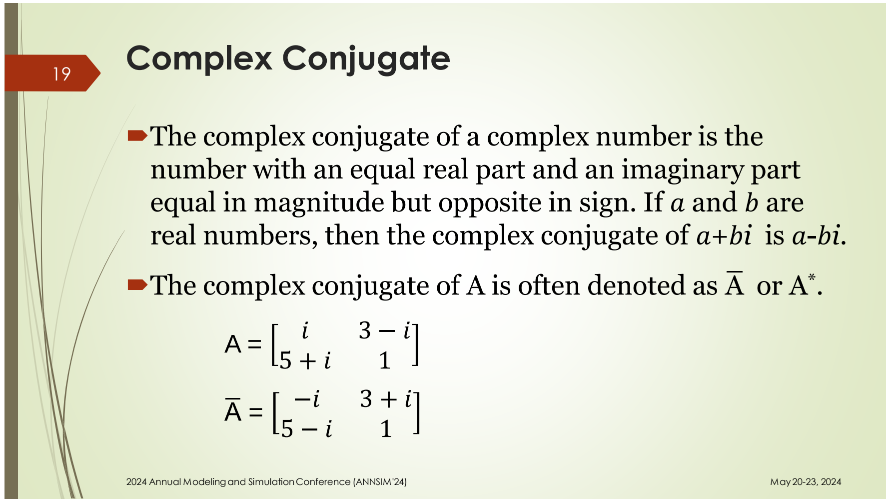
n is the dimension of the vector space



Tensor Product

- The outer product of two coordinate vectors is the matrix whose entries are all products of an element in the first vector with an element in the second vector.
- If the two coordinate vectors have dimensions n and m, then their outer product is an n×m matrix.

$$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \otimes \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} a_1 b_1 \\ a_1 b_2 \\ a_1 b_3 \\ a_2 b_1 \\ a_2 b_2 \\ a_2 b_3 \end{bmatrix}$$

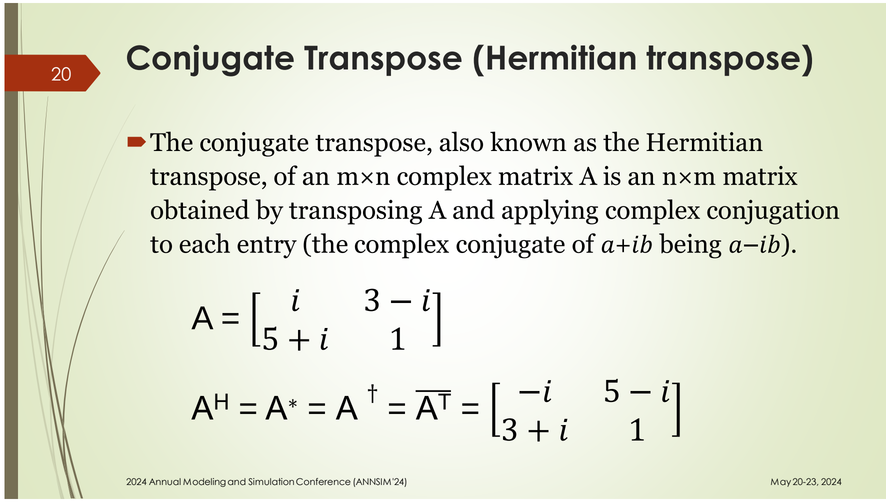


Complex Conjugate

- The complex conjugate of a complex number is the number with an equal real part and an imaginary part equal in magnitude but opposite in sign. If a and b are real numbers, then the complex conjugate of $a+bi$ is $a-bi$.
- The complex conjugate of A is often denoted as $\bar{A}$ or A^*.

$$A = \begin{bmatrix} i & 3-i \\ 5+i & 1 \end{bmatrix}$$

$$\bar{A} = \begin{bmatrix} -i & 3+i \\ 5-i & 1 \end{bmatrix}$$

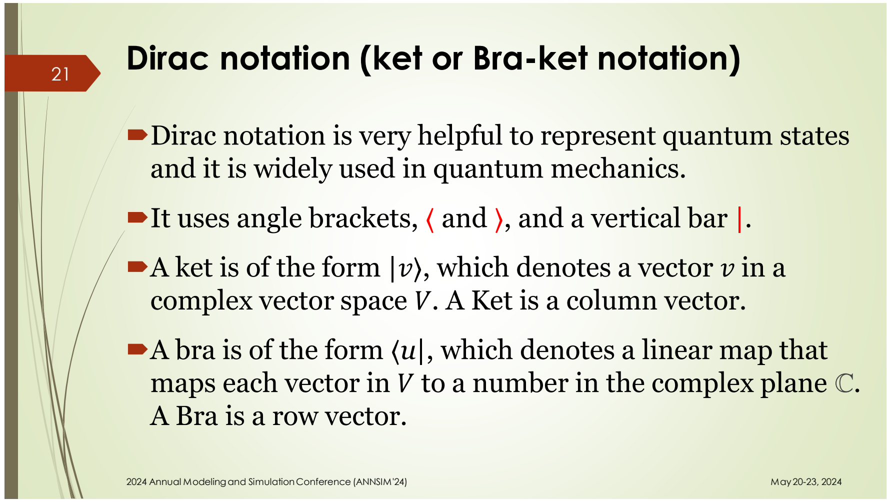


Conjugate Transpose (Hermitian transpose)

- The conjugate transpose, also known as the Hermitian transpose, of an m×n complex matrix A is an n×m matrix obtained by transposing A and applying complex conjugation to each entry (the complex conjugate of $a+ib$ being $a-ib$).

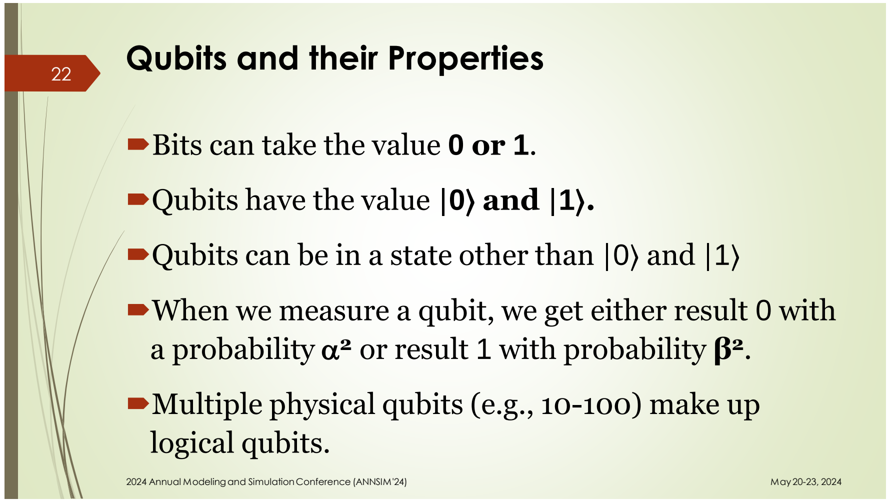
$$A = \begin{bmatrix} i & 3-i \\ 5+i & 1 \end{bmatrix}$$

$$A^H = A^* = A^{\dagger} = \overline{A^T} = \begin{bmatrix} -i & 5-i \\ 3+i & 1 \end{bmatrix}$$



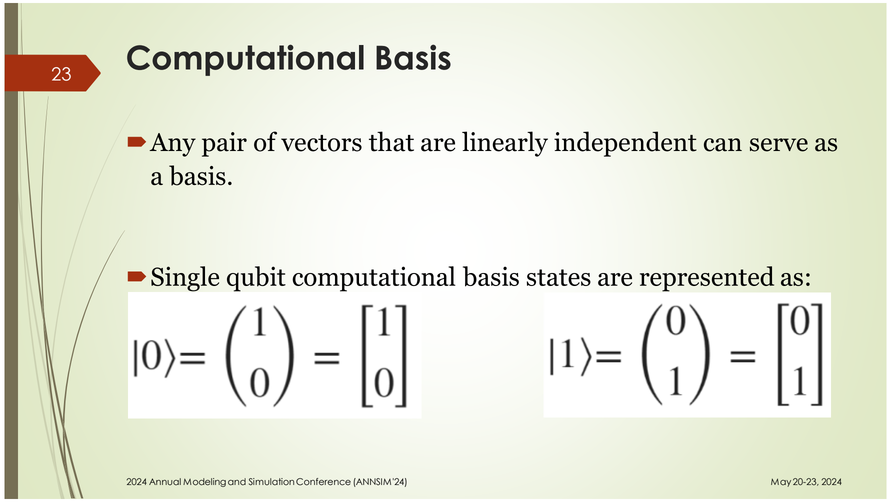
Dirac notation (ket or Bra-ket notation)

- Dirac notation is very helpful to represent quantum states and it is widely used in quantum mechanics.
- It uses angle brackets, $\langle$ and $\rangle$, and a vertical bar $|$.
- A ket is of the form $|v\rangle$, which denotes a vector v in a complex vector space V. A Ket is a column vector.
- A bra is of the form $\langle u|$, which denotes a linear map that maps each vector in V to a number in the complex plane $\mathbb{C}$. A Bra is a row vector.



Qubits and their Properties

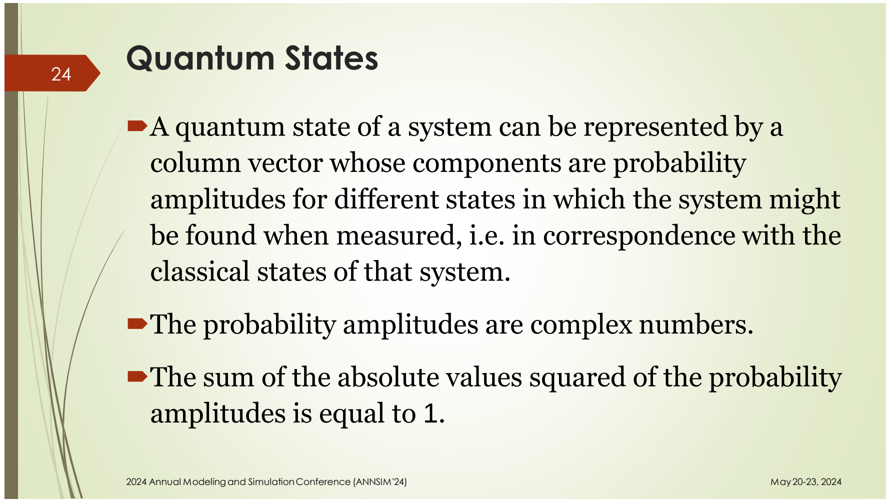
- Bits can take the value **0 or 1**.
- Qubits have the value **$|0\rangle$ and $|1\rangle$.**
- Qubits can be in a state other than $|0\rangle$ and $|1\rangle$
- When we measure a qubit, we get either result 0 with a probability α^2 or result 1 with probability β^2.
- Multiple physical qubits (e.g., 10-100) make up logical qubits.



Computational Basis

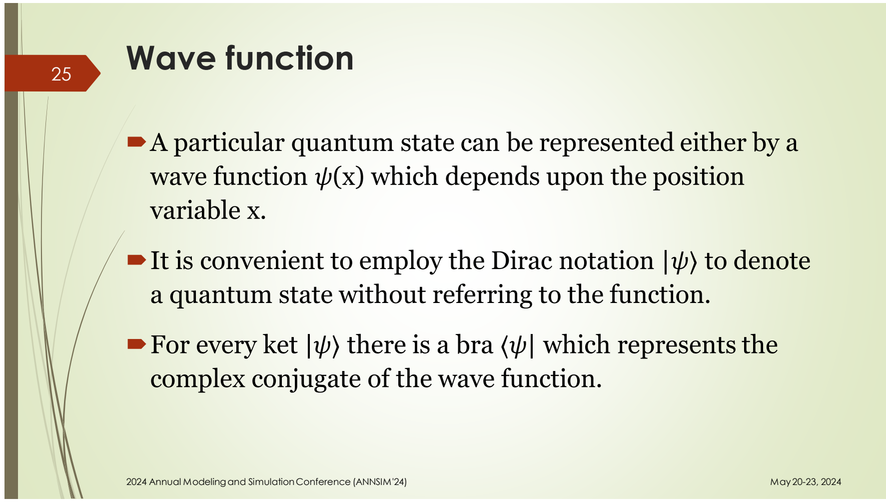
- Any pair of vectors that are linearly independent can serve as a basis.
- Single qubit computational basis states are represented as:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$



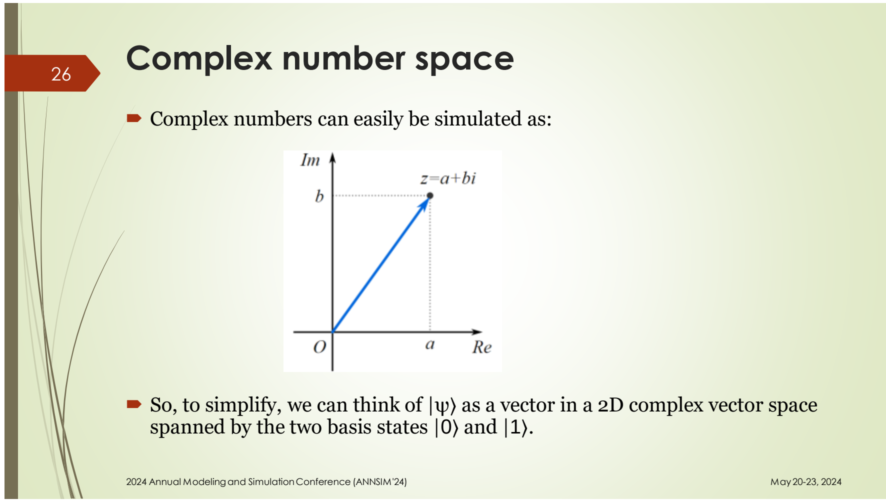
Quantum States

- A quantum state of a system can be represented by a column vector whose components are probability amplitudes for different states in which the system might be found when measured, i.e. in correspondence with the classical states of that system.
- The probability amplitudes are complex numbers.
- The sum of the absolute values squared of the probability amplitudes is equal to 1.



Wave function

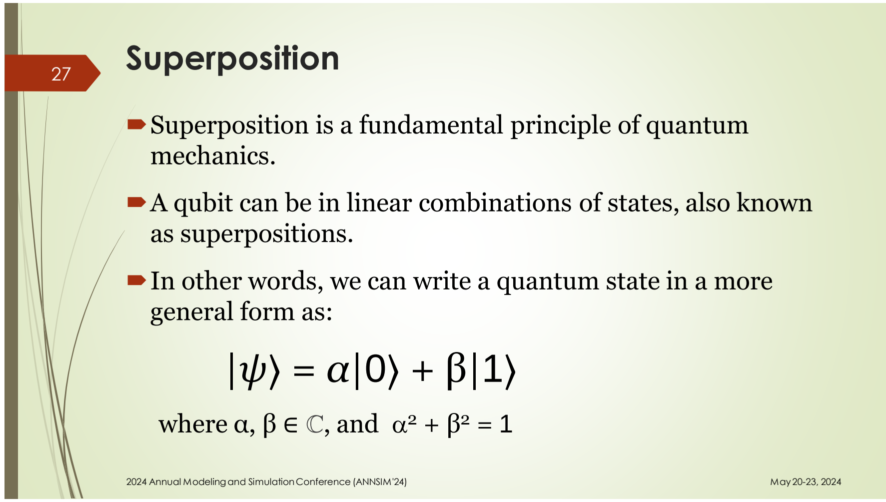
- A particular quantum state can be represented either by a wave function $\psi(x)$ which depends upon the position variable x.
- It is convenient to employ the Dirac notation $|\psi\rangle$ to denote a quantum state without referring to the function.
- For every ket $|\psi\rangle$ there is a bra $\langle\psi|$ which represents the complex conjugate of the wave function.



Complex number space

- Complex numbers can easily be simulated as:

- So, to simplify, we can think of $|\psi\rangle$ as a vector in a 2D complex vector space spanned by the two basis states $|0\rangle$ and $|1\rangle$.

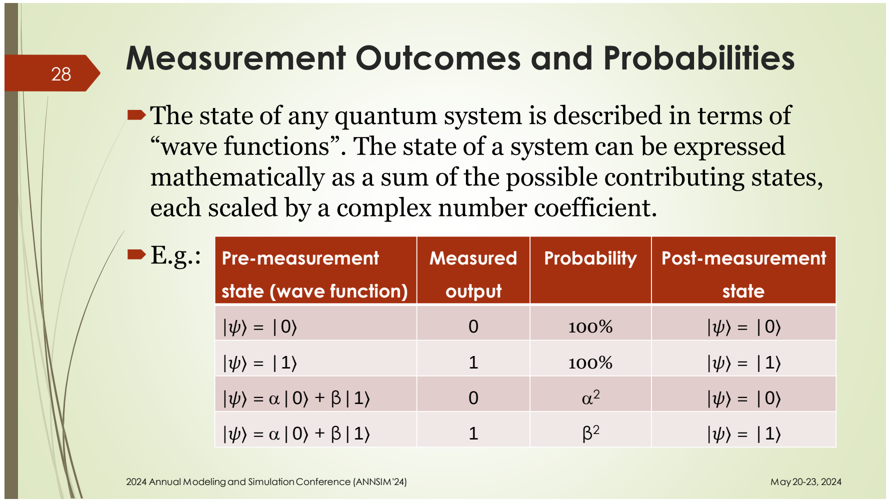


Superposition

- Superposition is a fundamental principle of quantum mechanics.
- A qubit can be in linear combinations of states, also known as superpositions.
- In other words, we can write a quantum state in a more general form as:

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

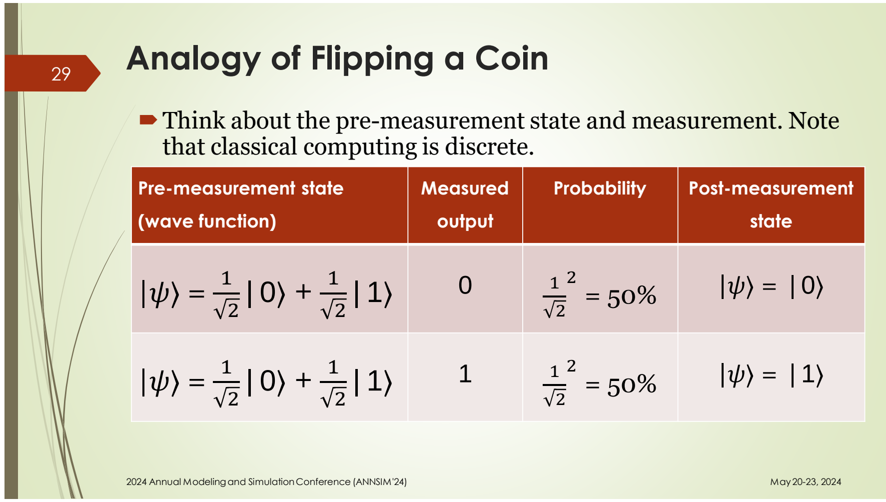
where $\alpha, \beta \in \mathbb{C}$, and $\alpha^2 + \beta^2 = 1$



Measurement Outcomes and Probabilities

- The state of any quantum system is described in terms of "wave functions". The state of a system can be expressed mathematically as a sum of the possible contributing states, each scaled by a complex number coefficient.
- E.g.:

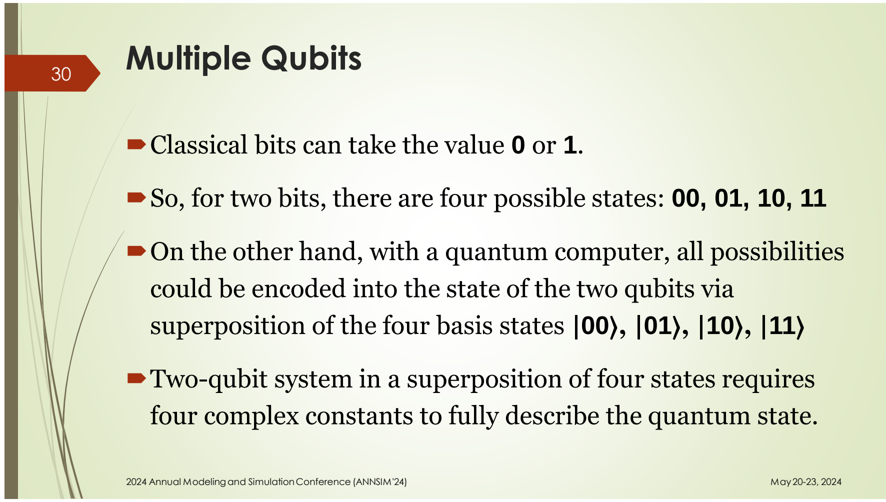
Pre-measurement state (wave function)	Measured output	Probability	Post-measurement state
$\|\psi\rangle = \|0\rangle$	0	100%	$\|\psi\rangle = \|0\rangle$
$\|\psi\rangle = \|1\rangle$	1	100%	$\|\psi\rangle = \|1\rangle$
$\|\psi\rangle = \alpha\|0\rangle + \beta\|1\rangle$	0	α^2	$\|\psi\rangle = \|0\rangle$
$\|\psi\rangle = \alpha\|0\rangle + \beta\|1\rangle$	1	β^2	$\|\psi\rangle = \|1\rangle$



Analogy of Flipping a Coin

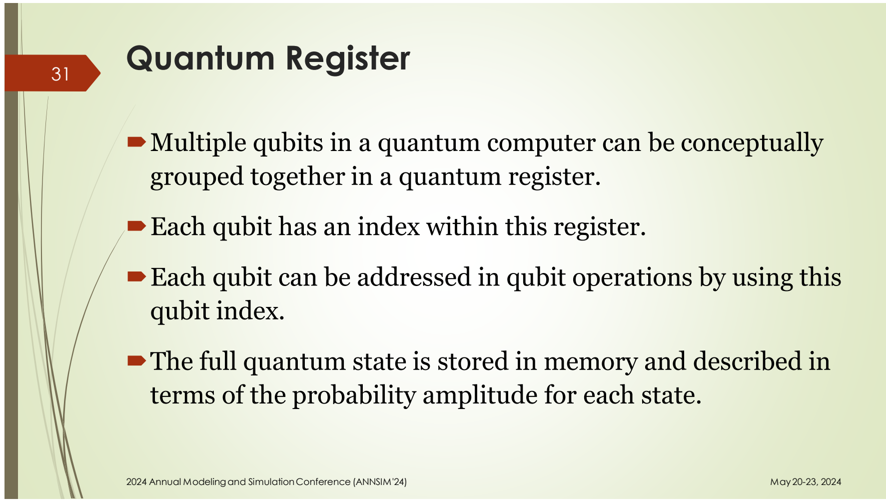
- Think about the pre-measurement state and measurement. Note that classical computing is discrete.

Pre-measurement state (wave function)	Measured output	Probability	Post-measurement state
$\lvert\psi\rangle = \frac{1}{\sqrt{2}}\lvert 0\rangle + \frac{1}{\sqrt{2}}\lvert 1\rangle$	0	$\frac{1}{\sqrt{2}}^{2} = 50\%$	$\lvert\psi\rangle = \lvert 0\rangle$
$\lvert\psi\rangle = \frac{1}{\sqrt{2}}\lvert 0\rangle + \frac{1}{\sqrt{2}}\lvert 1\rangle$	1	$\frac{1}{\sqrt{2}}^{2} = 50\%$	$\lvert\psi\rangle = \lvert 1\rangle$



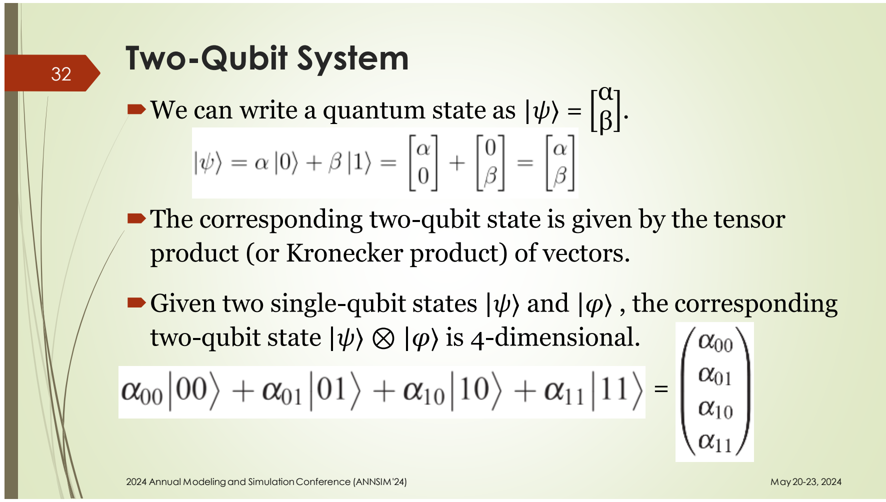
Multiple Qubits

- Classical bits can take the value **0** or **1**.
- So, for two bits, there are four possible states: **00, 01, 10, 11**
- On the other hand, with a quantum computer, all possibilities could be encoded into the state of the two qubits via superposition of the four basis states **|00⟩, |01⟩, |10⟩, |11⟩**
- Two-qubit system in a superposition of four states requires four complex constants to fully describe the quantum state.



Quantum Register

- Multiple qubits in a quantum computer can be conceptually grouped together in a quantum register.
- Each qubit has an index within this register.
- Each qubit can be addressed in qubit operations by using this qubit index.
- The full quantum state is stored in memory and described in terms of the probability amplitude for each state.



Two-Qubit System

- We can write a quantum state as $\lvert\psi\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix}$.

$$\lvert\psi\rangle = \alpha\lvert 0\rangle + \beta\lvert 1\rangle = \begin{bmatrix}\alpha \\ 0\end{bmatrix} + \begin{bmatrix}0 \\ \beta\end{bmatrix} = \begin{bmatrix}\alpha \\ \beta\end{bmatrix}$$

- The corresponding two-qubit state is given by the tensor product (or Kronecker product) of vectors.
- Given two single-qubit states $\lvert\psi\rangle$ and $\lvert\varphi\rangle$, the corresponding two-qubit state $\lvert\psi\rangle \otimes \lvert\varphi\rangle$ is 4-dimensional.

$$\alpha_{00}\lvert 00\rangle + \alpha_{01}\lvert 01\rangle + \alpha_{10}\lvert 10\rangle + \alpha_{11}\lvert 11\rangle = \begin{pmatrix}\alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11}\end{pmatrix}$$

Basis States in 2-Qubit System

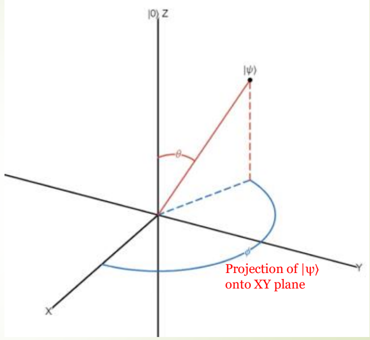
$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \qquad |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$$

$$|01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \qquad |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

- Note that $|00\rangle = |0\rangle \otimes |0\rangle$, $|01\rangle = |0\rangle \otimes |1\rangle$ and so on.

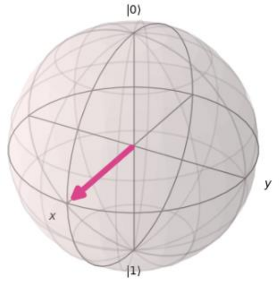
Bloch Sphere

- A qubit state can be illustrated with Bloch sphere.
- $|\psi\rangle$ is pointing from the origin to a point on the surface of the unit sphere.
- The direction of $|\psi\rangle$ is specified by polar angle θ and azimuthal angle φ.



Bloch Sphere Simulators

- Usually, three parameters are needed.
  - [<x>, <y>, <z>] coordinates
  - [<r>, <theta>, <phi>] spherical



Quantum Simulators

- Quantum simulators play an important role in bridging the theoretical and practical aspects of quantum computing.
- Recent developments in quantum hardware have facilitated the development of quantum simulators that mimic the behaviour of quantum computers.
- For example, IBM Quantum Composer is a graphical quantum programming tool that lets you drag and drop operations to build quantum circuits and run them on real quantum hardware or simulators. https://quantum.ibm.com/composer/

Available Quantum Simulators

- Sparse quantum simulator (default on Azure Quantum)
- IBM quantum simulator services
- Other backend simulators compatible with Microsoft platform:
  - IonQ
  - PASQAL
  - Quantinuum
  - Rigetti
- and others

Entanglement: “spooky action at a distance”

- In quantum computing, we can generate pairs of qubits that are “entangled,” which means they exist in a single quantum state.
- Changing the state of one of the qubits will instantly change the state of the other one.

Quantum teleportation

- Quantum teleportation is a method to send qubits using entanglement.
- Quantum teleportation can transmit a qubit without really using a physical carrier.
- It does not allow for faster than light communication.

Quantum Supremacy

- Quantum supremacy is the point at which a quantum computer can complete a mathematical calculation that is demonstrably beyond the reach of even the most powerful supercomputer.
- Quantum computers have the potential to exceed the performance of conventional computers for complex problems such as cryptography, chemistry, pharmaceuticals, etc.
- Quantum advantage is also a related topic, but considered to be slightly different as it is the point at which quantum applications deliver a significant, practical benefit beyond what classical computers alone are capable.

Part 2:

Quantum Circuits and their Execution on Quantum Simulators, Examples and Applications

Quantum Parallelism

- Quantum parallelism is based on the ability of a quantum register to exist in a superposition of base states.
- It is the possibility of performing large number of operations in parallel without the need of extra resources.
- For 3 classical bits, there are $2^n = 2^3 = 8$ cases.
- For 3 qubits, all 8 cases can be represented in a single quantum state simultaneously in superposition.

Non-Disturbance Principle

- A unique feature of quantum mechanics is that any attempt to measure a qubit inevitably disturbs its state providing a detectable sign of an unauthorised interception.
- If a state in superposition is measured, the superposition (and so the amplitudes) gets lost.
- To utilise the power of quantum bits, the computations should be performed in superposition.

No Cloning Theorem

- In physics, the no-cloning theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state.
- So, we say it is impossible to replicate with certainty an arbitrary quantum bit., i.e., it is not possible to copy qubits.

Amplitude

- The parameter θ expresses the relative amplitude of the basis states, while φ expresses their relative phase.
- A quantum state has a value and an **amplitude α** which is a complex number.
- $|\alpha|^2$ determines the probability of a quantum program being in that state if the qubits are measured.
- The amplitudes comprise of two elements, a magnitude and a phase.

Phase

- The phase ranges from 0° to 360°.
- We can introduce 90° phase shifts represented by $\pi/2$ radians, so θ and φ can take value from 0 to 2π.

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

$$0 \leq \theta \leq \pi$$
$$0 \leq \varphi \leq 2\pi$$

+/- Quantum Basis States

$$|+\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$
$$|-\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$

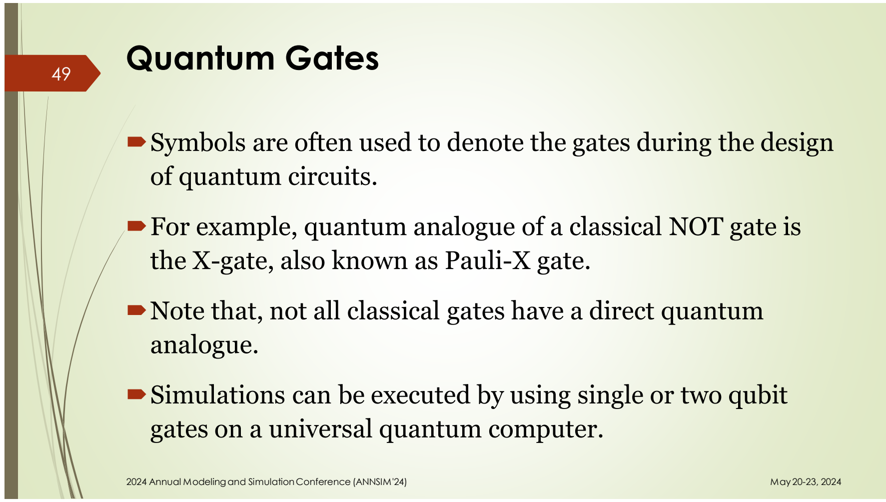
- Measurement basis: $|+\rangle$, $|-\rangle$

Pre-measurement state (wave function)	Measured output	Probability	Post-measurement state
$\|\psi\rangle = \|+\rangle$	+	100%	$\|\psi\rangle = \|+\rangle$
$\|\psi\rangle = \|-\rangle$	−	100%	$\|\psi\rangle = \|-\rangle$
$\|\psi\rangle = \alpha\|+\rangle + \beta\|-\rangle$	+	α^2	$\|\psi\rangle = \|+\rangle$
$\|\psi\rangle = \alpha\|+\rangle + \beta\|-\rangle$	−	β^2	$\|\psi\rangle = \|-\rangle$

↑/↓ Quantum Basis States

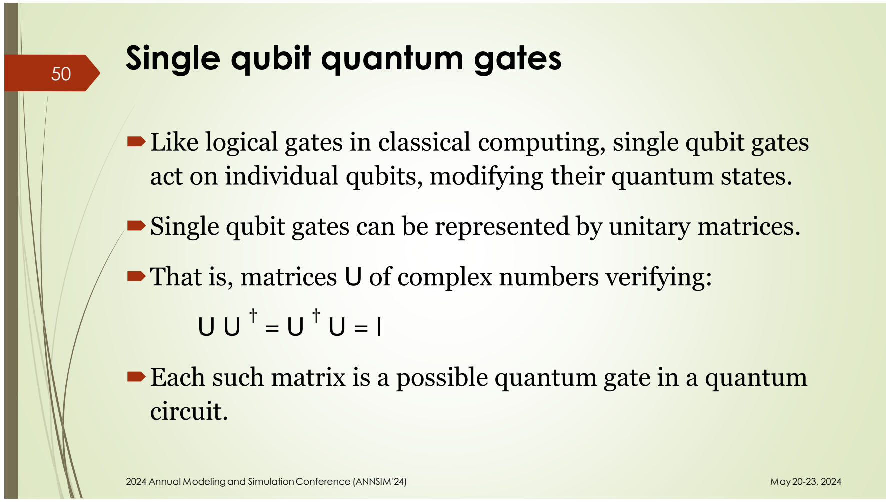
- Consider a ground state $|\uparrow\rangle$ and excited state $|\downarrow\rangle$.

Pre-measurement state (wave function)	Measured output	Probability	Post-measurement state
$\|\psi\rangle = \|\uparrow\rangle$	↑	100%	$\|\psi\rangle = \|\uparrow\rangle$
$\|\psi\rangle = \|\downarrow\rangle$	↓	100%	$\|\psi\rangle = \|\downarrow\rangle$
$\|\psi\rangle = \alpha\|\uparrow\rangle + \beta\|\downarrow\rangle$	↑	α^2	$\|\psi\rangle = \|\uparrow\rangle$
$\|\psi\rangle = \alpha\|\uparrow\rangle + \beta\|\downarrow\rangle$	↓	β^2	$\|\psi\rangle = \|\downarrow\rangle$



Quantum Gates

- Symbols are often used to denote the gates during the design of quantum circuits.
- For example, quantum analogue of a classical NOT gate is the X-gate, also known as Pauli-X gate.
- Note that, not all classical gates have a direct quantum analogue.
- Simulations can be executed by using single or two qubit gates on a universal quantum computer.

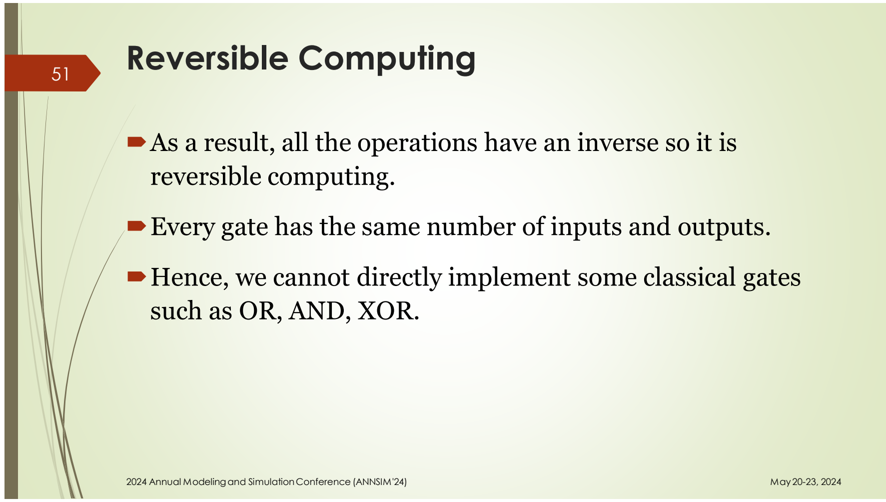


Single qubit quantum gates

- Like logical gates in classical computing, single qubit gates act on individual qubits, modifying their quantum states.
- Single qubit gates can be represented by unitary matrices.
- That is, matrices U of complex numbers verifying:

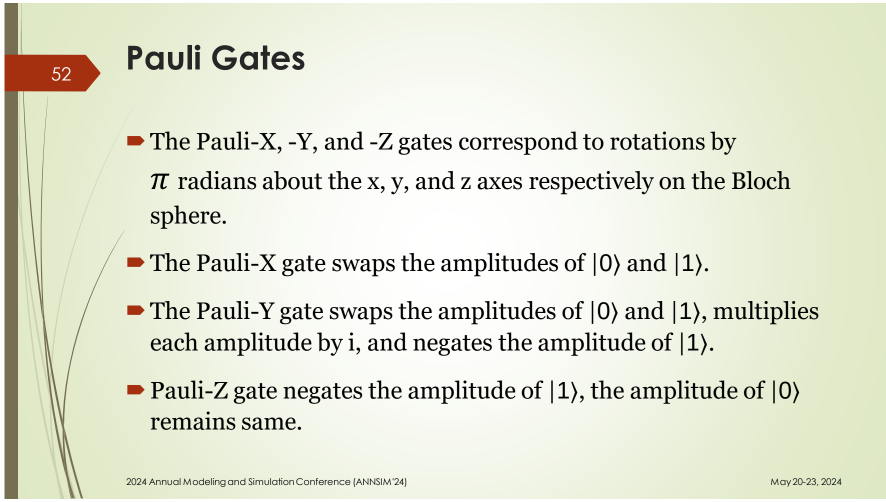
$$U U^{\dagger} = U^{\dagger} U = I$$

- Each such matrix is a possible quantum gate in a quantum circuit.



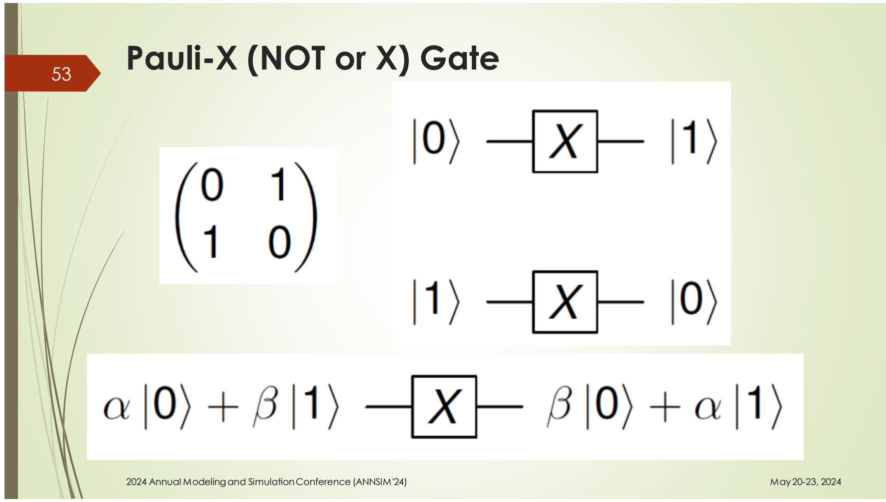
Reversible Computing

- As a result, all the operations have an inverse so it is reversible computing.
- Every gate has the same number of inputs and outputs.
- Hence, we cannot directly implement some classical gates such as OR, AND, XOR.



Pauli Gates

- The Pauli-X, -Y, and -Z gates correspond to rotations by π radians about the x, y, and z axes respectively on the Bloch sphere.
- The Pauli-X gate swaps the amplitudes of $|0\rangle$ and $|1\rangle$.
- The Pauli-Y gate swaps the amplitudes of $|0\rangle$ and $|1\rangle$, multiplies each amplitude by i, and negates the amplitude of $|1\rangle$.
- Pauli-Z gate negates the amplitude of $|1\rangle$, the amplitude of $|0\rangle$ remains same.



53

Pauli-X (NOT or X) Gate

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

$$|0\rangle \;-\boxed{X}-\; |1\rangle$$

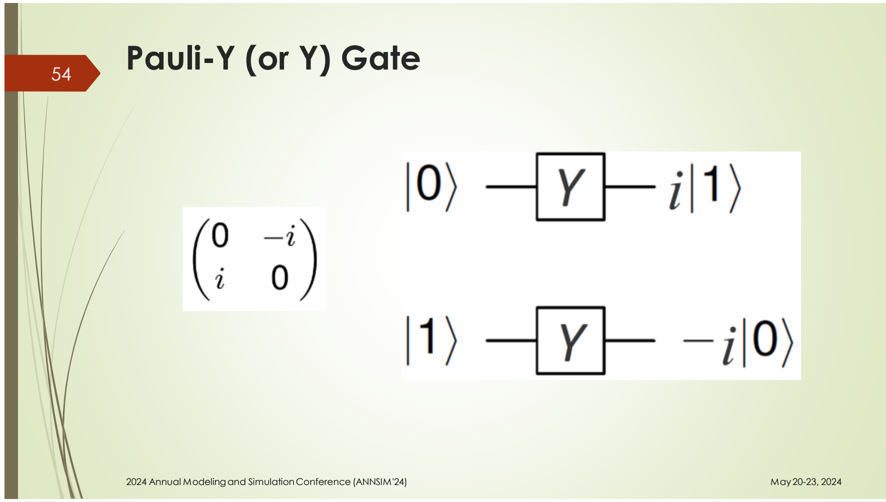
$$|1\rangle \;-\boxed{X}-\; |0\rangle$$

$$\alpha\,|0\rangle + \beta\,|1\rangle \;-\boxed{X}-\; \beta\,|0\rangle + \alpha\,|1\rangle$$

2024 Annual Modeling and Simulation Conference (ANNSIM'24)

May 20-23, 2024

53



54

Pauli-Y (or Y) Gate

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

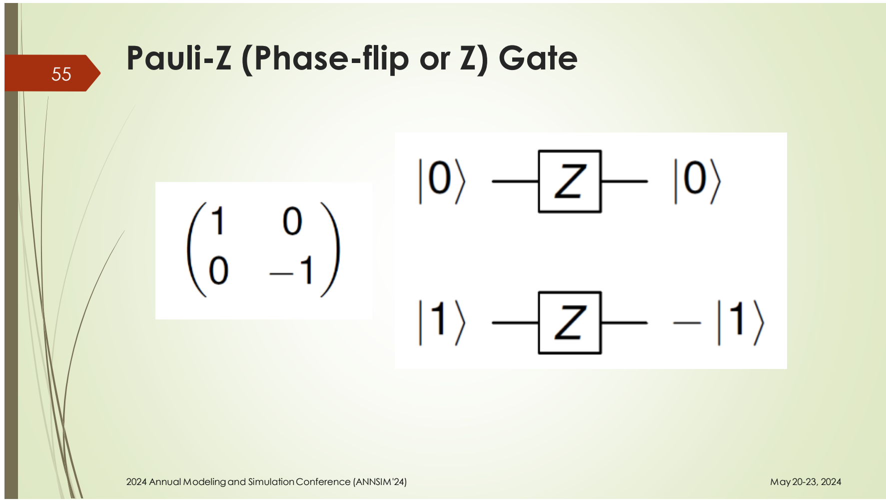
$$|0\rangle \;-\boxed{Y}-\; i|1\rangle$$

$$|1\rangle \;-\boxed{Y}-\; -i|0\rangle$$

2024 Annual Modeling and Simulation Conference (ANNSIM'24)

May 20-23, 2024

54



55

Pauli-Z (Phase-flip or Z) Gate

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

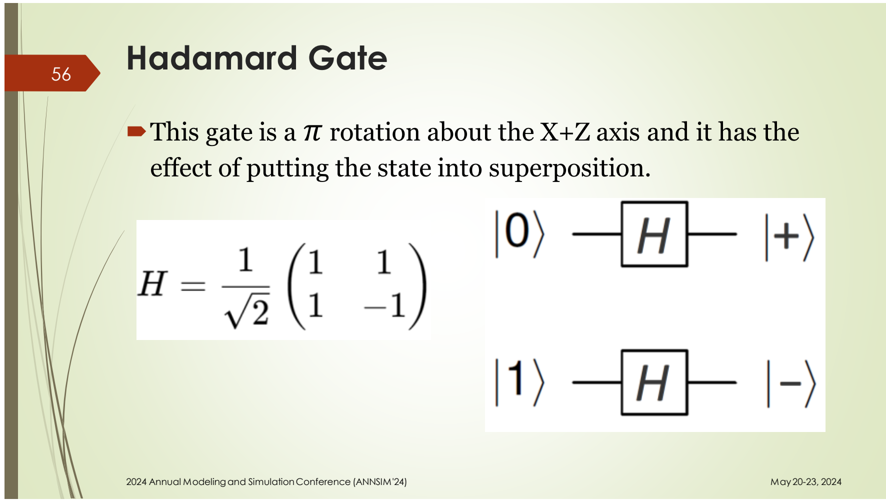
$$|0\rangle \;-\boxed{Z}-\; |0\rangle$$

$$|1\rangle \;-\boxed{Z}-\; -|1\rangle$$

2024 Annual Modeling and Simulation Conference (ANNSIM'24)

May 20-23, 2024

55



56

Hadamard Gate

- This gate is a π rotation about the X+Z axis and it has the effect of putting the state into superposition.

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

$$|0\rangle \;-\boxed{H}-\; |+\rangle$$

$$|1\rangle \;-\boxed{H}-\; |-\rangle$$

2024 Annual Modeling and Simulation Conference (ANNSIM'24)

May 20-23, 2024

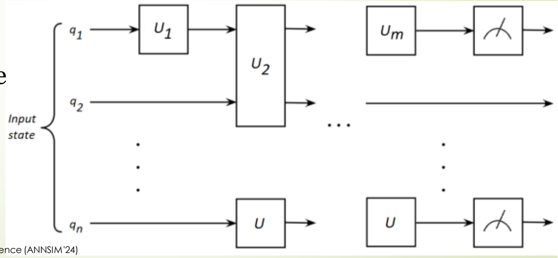
56

Measuring Qubits

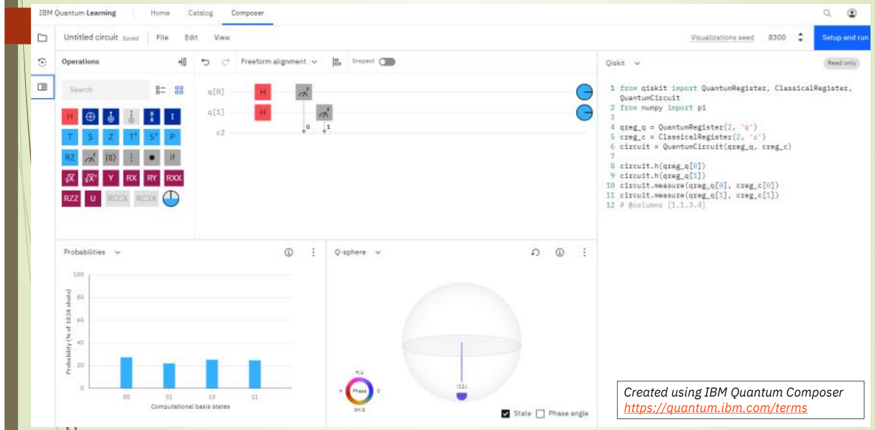
- One way to determine the state of a qubit is to measure the projection of its state vector along a given axis.
- We use the  building block to exit the quantum state and read a qubit's state.
- Once measured, the qubit will be in either one of its computational basis states.

Quantum Circuits

- A quantum circuit is a model for quantum computation.
- It can be represented as a network of quantum gates followed by a quantum measurement element.
- Gates are linked to each other as in the classical circuits and each gate perform some unitary operator.



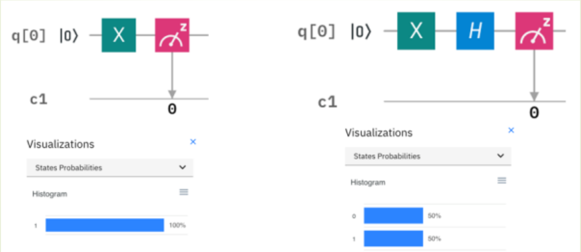
Designing Quantum Circuits



```
from qiskit import QuantumRegister, ClassicalRegister,
QuantumCircuit
from numpy import pi

qreg_q = QuantumRegister(2, 'q')
creg_c = ClassicalRegister(2, 'c')
circuit = QuantumCircuit(qreg_q, creg_c)

circuit.h(qreg_q[0])
circuit.h(qreg_q[1])
circuit.measure(qreg_q[0], creg_c[0])
circuit.measure(qreg_q[1], creg_c[1])
# @columns [1,1,3,4]
```

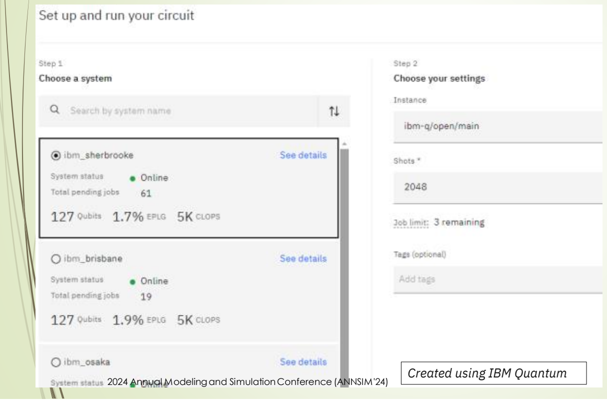
Created using IBM Quantum Composer
https://quantum.ibm.com/terms

Demonstration (video)



Created using IBM Quantum

Running Quantum Circuits



Set up and run your circuit

Step 1

Choose a system

○ ibm_sherbrooke — See details
System status ● Online
Total pending jobs 61
127 Qubits 1.7% EPLG 5K CLOPS

○ ibm_brisbane — See details
System status ● Online
Total pending jobs 19
127 Qubits 1.9% EPLG 5K CLOPS

○ ibm_osaka — See details
System status ● Online

Step 2

Choose your settings

Instance: ibm-q/open/main

Shots *: 2048

Job limit: 3 remaining

Tags (optional): Add tags

Completed: May 17, 2024 3:22 PM (in 2h 1m 33s)

Compute resource: ibm_sherbrooke

Status timeline — Completed

Details

Results

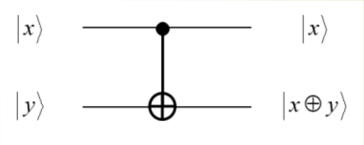
Histogram for register "c"

Created using IBM Quantum

Quantum controlled NOT (CNOT or CX gate)

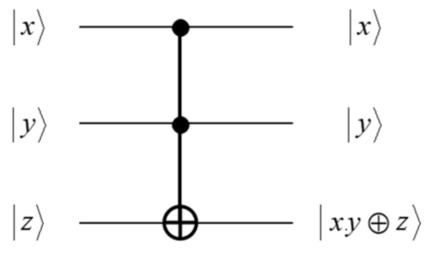
- Multi-qubit gates act on two or more qubits simultaneously and enable the creation and manipulation of quantum states.
- The CNOT gate flips the second qubit (the target qubit) if and only if the first qubit (the control qubit) is |1⟩.

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

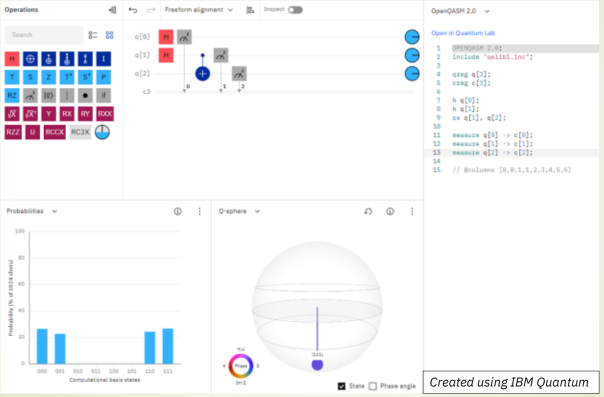


Toffoli (CCNOT or CCX) Gate

- The Toffoli gate, also known as the double controlled-NOT gate, has two control qubits and one target. It applies a NOT to the target only when both controls are in state |1⟩.



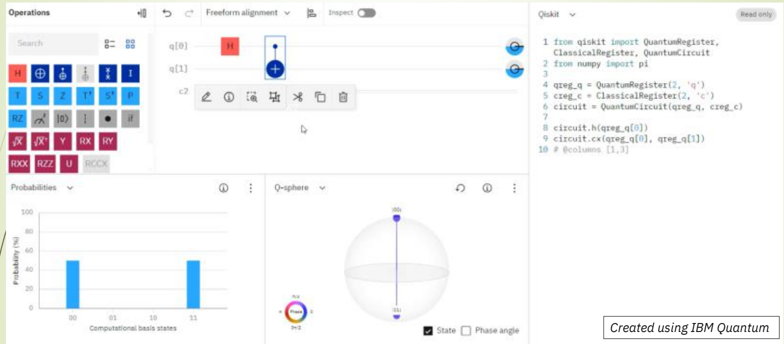
Example



```
OPENQASM 2.0;
include "qelib1.inc";

qreg q[3];
creg c[3];

h q[0];
h q[1];
cx q[1], q[2];

measure q[0] -> c[0];
measure q[1] -> c[1];
measure q[2] -> c[2];

// @columns [0,0,1,1,2,3,4,5,6]
```

Created using IBM Quantum

Bell State Demonstration (video)



```
from qiskit import QuantumRegister,
ClassicalRegister, QuantumCircuit
from numpy import pi

qreg_q = QuantumRegister(2, 'q')
creg_c = ClassicalRegister(2, 'c')
circuit = QuantumCircuit(qreg_q, creg_c)

circuit.h(qreg_q[0])
circuit.cx(qreg_q[0], qreg_q[1])
# @columns [1,3]
```

Created using IBM Quantum

Quantum Algorithms

- Many problems are too hard to be solved by a computer such as Travelling Salesman Problem (TSP), Knapsack problem, Vehicle routing problem, Scheduling problem, and many more.
- Quantum advantage can start with having useful quantum algorithms.
- Algorithms can be based on mathematical theorems and their proofs, e.g. Shor's algorithm and Grover's algorithm.
- Alternatively, a quantum algorithm can be first proposed and then tested.

Integer Factoring

- Integer factorisation decomposes a number into its prime factors.
- It is an important operation in cryptography.
- Assume that there is a number M made up of the multiplication of two large prime numbers M = p*q.
- Finding p and q is NP hard such as we use it as the basis of all encryption, RSA.

Shor’s Algorithm (Prime factoring)

- Shor’s algorithm can factor large numbers exponentially faster than classical machines.
- That ability means a quantum computer could crack systems like RSA, a widely used method for encrypting data.
- A key component is Quantum Fourier Transform (QFT) which is exponentially faster than its classical counterpart Discrete Fourier Transform.

Grover’s Algorithm (Searching)

- Polynomial speed up over the best possible classical search algorithms.
- To implement Grover's algorithm, we need an operational block that can recognize if a test value of x satisfies our function or not. This operation is called an oracle.
- Subject to data loading problem which is an active research area.

Quantum Software and Tools

- Quantum programming environments with remote access,
- Quantum simulators
- Many simple gates, Bloch sphere, circuit visualization tools,
- Access to quantum computers via interfaces,
- Code libraries for quantum computing, e.g. Python,
- Problem specific models or tools,
- Programming languages, software development kits (SDKs), etc.

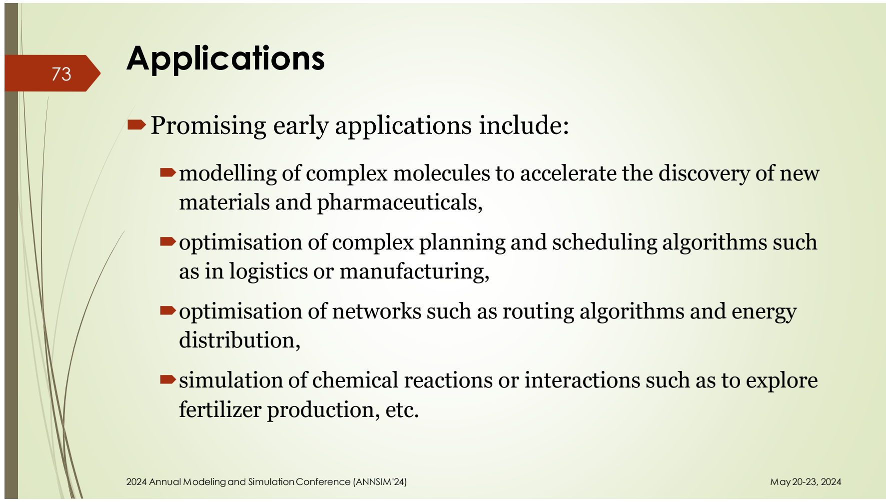
Quantum Programming Languages

- Q# by Microsoft on Azure Quantum Platform
- Cirq by Google
- Qiskit by IBM
- Open Quantum Assembly Language - a machine independent programming interface
- Python or other general purpose programming language with specific libraries

---

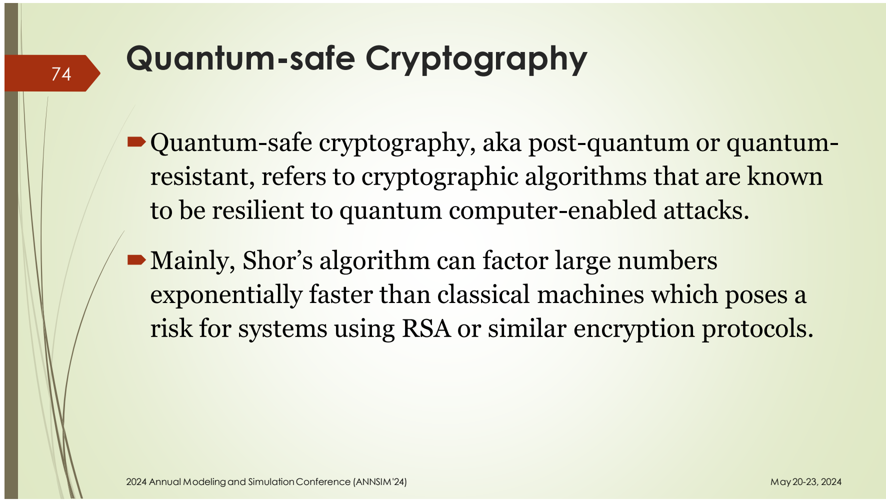
Potential Applications of Quantum Computing

- The potential impact is expected in many sectors for better efficiency, productivity and competitiveness.
- There is opportunity to exceed the performance of classical computers for complex and important problems in areas such as:
  - Pharmaceuticals,
  - Chemistry,
  - Cybersecurity,
  - Materials science,
  - Machine learning and AI,
  - Optimization,
  - Simulation, etc.



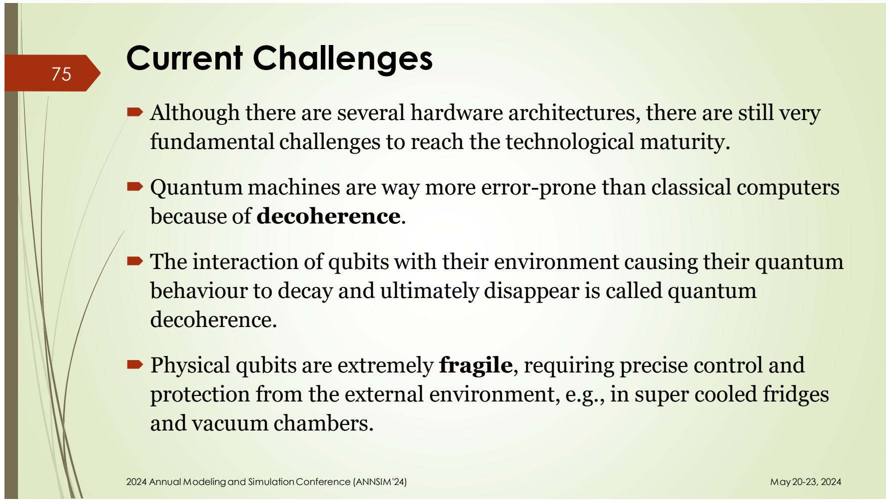
Applications

- Promising early applications include:
  - modelling of complex molecules to accelerate the discovery of new materials and pharmaceuticals,
  - optimisation of complex planning and scheduling algorithms such as in logistics or manufacturing,
  - optimisation of networks such as routing algorithms and energy distribution,
  - simulation of chemical reactions or interactions such as to explore fertilizer production, etc.



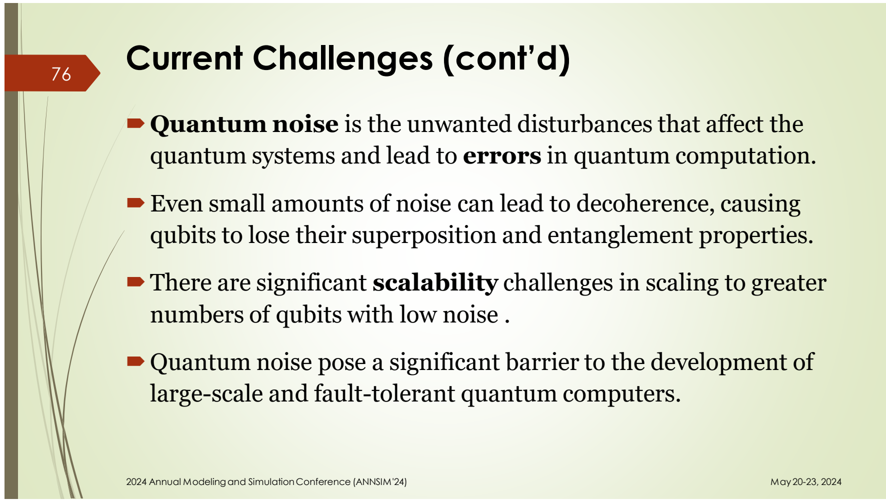
Quantum-safe Cryptography

- Quantum-safe cryptography, aka post-quantum or quantum-resistant, refers to cryptographic algorithms that are known to be resilient to quantum computer-enabled attacks.
- Mainly, Shor's algorithm can factor large numbers exponentially faster than classical machines which poses a risk for systems using RSA or similar encryption protocols.



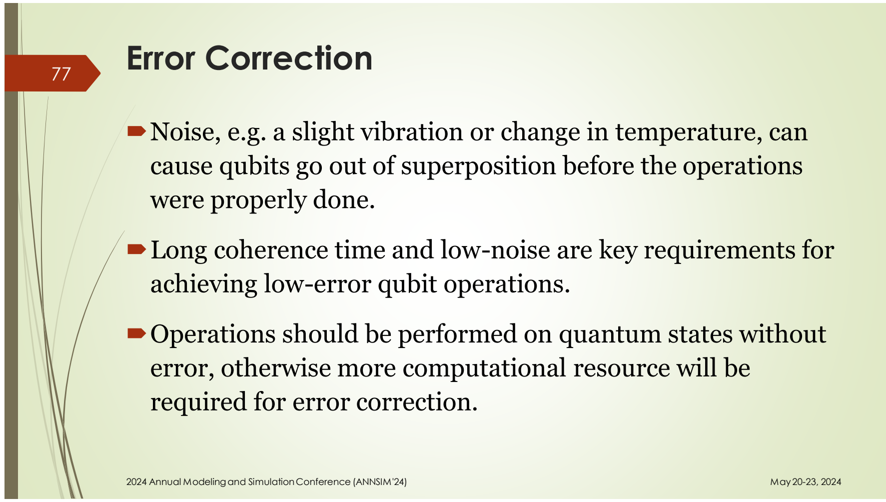
Current Challenges

- Although there are several hardware architectures, there are still very fundamental challenges to reach the technological maturity.
- Quantum machines are way more error-prone than classical computers because of **decoherence**.
- The interaction of qubits with their environment causing their quantum behaviour to decay and ultimately disappear is called quantum decoherence.
- Physical qubits are extremely **fragile**, requiring precise control and protection from the external environment, e.g., in super cooled fridges and vacuum chambers.



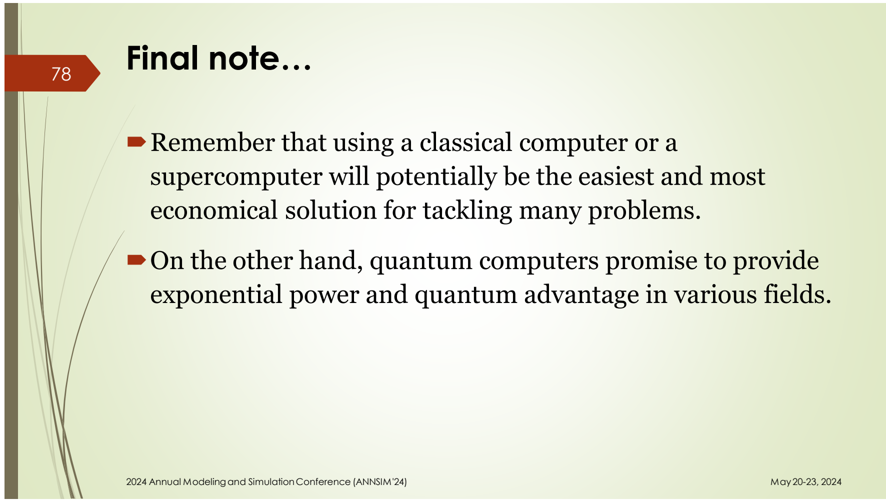
Current Challenges (cont'd)

- **Quantum noise** is the unwanted disturbances that affect the quantum systems and lead to **errors** in quantum computation.
- Even small amounts of noise can lead to decoherence, causing qubits to lose their superposition and entanglement properties.
- There are significant **scalability** challenges in scaling to greater numbers of qubits with low noise .
- Quantum noise pose a significant barrier to the development of large-scale and fault-tolerant quantum computers.



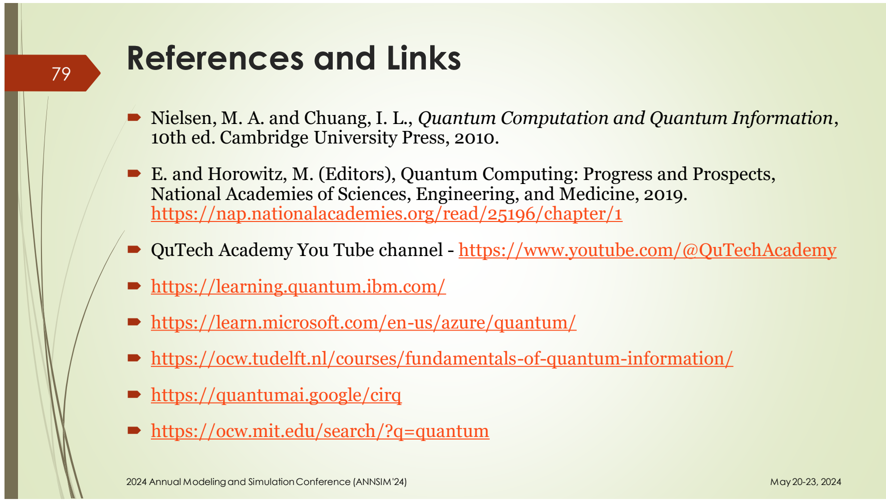
Error Correction

- Noise, e.g. a slight vibration or change in temperature, can cause qubits go out of superposition before the operations were properly done.
- Long coherence time and low-noise are key requirements for achieving low-error qubit operations.
- Operations should be performed on quantum states without error, otherwise more computational resource will be required for error correction.



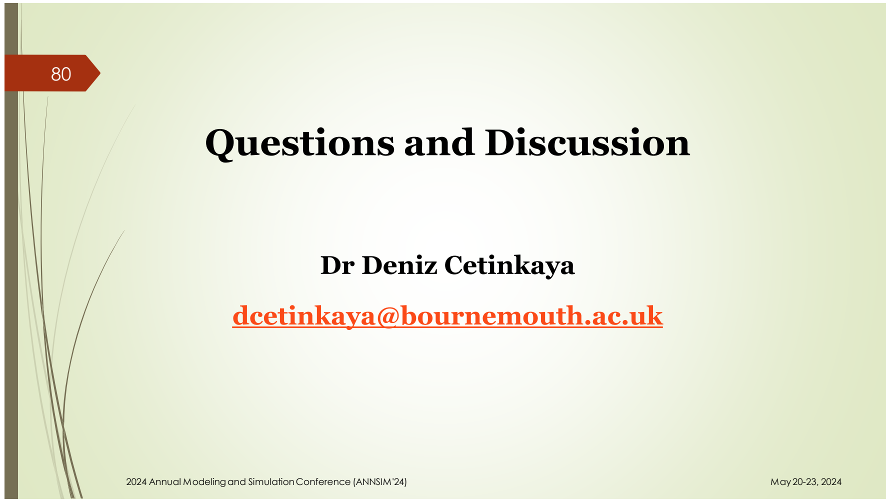
Final note…

- Remember that using a classical computer or a supercomputer will potentially be the easiest and most economical solution for tackling many problems.
- On the other hand, quantum computers promise to provide exponential power and quantum advantage in various fields.



References and Links

- Nielsen, M. A. and Chuang, I. L., *Quantum Computation and Quantum Information*, 10th ed. Cambridge University Press, 2010.
- E. and Horowitz, M. (Editors), Quantum Computing: Progress and Prospects, National Academies of Sciences, Engineering, and Medicine, 2019. https://nap.nationalacademies.org/read/25196/chapter/1
- QuTech Academy You Tube channel - https://www.youtube.com/@QuTechAcademy
- https://learning.quantum.ibm.com/
- https://learn.microsoft.com/en-us/azure/quantum/
- https://ocw.tudelft.nl/courses/fundamentals-of-quantum-information/
- https://quantumai.google/cirq
- https://ocw.mit.edu/search/?q=quantum



Questions and Discussion

Dr Deniz Cetinkaya

dcetinkaya@bournemouth.ac.uk