# Quantum Computing

Fundamentals and Frontiers

“All information is ultimately physical” - Landauer

“Erasure of Information is a dissipative process” – Landauer

Intel Pentium discards something like 100,000 bits per flop with each discarded bit incurring at least the minimum Landauer energy loss.

# Reversible Computation

- In 1961, Rolf Landauer and John Swanson at IBM began researching information dissipation, heat generation and reversible computing.
- The Fredkin gate and the Toffoli gate, which were constructed in the late 1970s and early 1980s at M.I.T., were the first investigations on reversible computing.

# Implications of Reversibility

- The reversibility of physics means that we can never truly erase information in a computer.
- Whenever we overwrite a bit of information with a new value, the previous information may be lost for all practical purposes, but it hasn't been physically destroyed.
- It has been pushed out into the machine's thermal environment, where it becomes entropy -in essence, randomized information and manifests as heat.

# Reversible Computation

- In 1973, Charles Bennett of IBM Research made a remarkable discovery.
- Classical computation can be broken down into a series of steps, each logically reversible, and this in turn allows physical reversibility of the computation.
- This result has implications for the energy dissipated by the computation.
- Rolf Landauer, Bennett's long-term colleague, had earlier shown that it is the act of discarding information that incurs an unavoidable energy loss.

# Reversible Computation and Drifting Approach

- Bennett's result means that we can arrange our computer to calculate reversibly, very slowly, with an energy as small as we please.
- In his lectures on computation in the 1980's, Feynman discusses a reversible computer that calculates for a few steps, then drifts back a bit, ‘uncalculating’ as it goes, before it drifts forward again to eventually complete the calculation with almost zero energy loss.

# Reversible Computation and Classical Gates

- To build such a reversible computer requires us to use new types of logic gates that are reversible, i.e. from the output of the gate one can reconstruct the input.
- It is easy to see that a conventional AND gate is not reversible. If the output of an AND gate is 0, the signals on the two input wires could be any one of three possibilities - 00, 01 and 10.

The price for reversibility is that we need to carry round extra bit of information

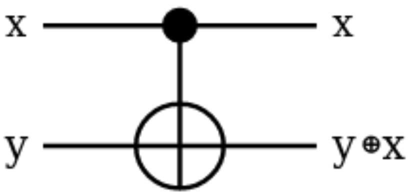
As we are not discarding any information, such gate is more energy efficient than classical gates.

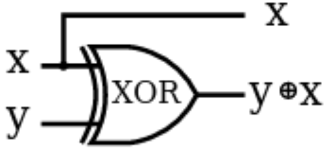
# Reversible Computation and Classical Gates

- The possibility of reversible logic gates was considered by Fredkin and Toffoli nearly many years ago.
- The truth table of classical NOT gate shows that it is reversible. From its output, we can deduce the input.
- Two NOT gates put back to back bring us back to the same place and demonstrate reversibility.

# Controlled Not Gate

- The NOT operation on the lower input line is only operative when there is a ‘1’ on the upper input:
- A ‘0’ on the upper input means that the lower bit passes through unchanged.
- What appears on the lower output is just the XOR operation on the two input bits.
- However, the CN gate is more than just an XOR gate since we retain information about the control bit.

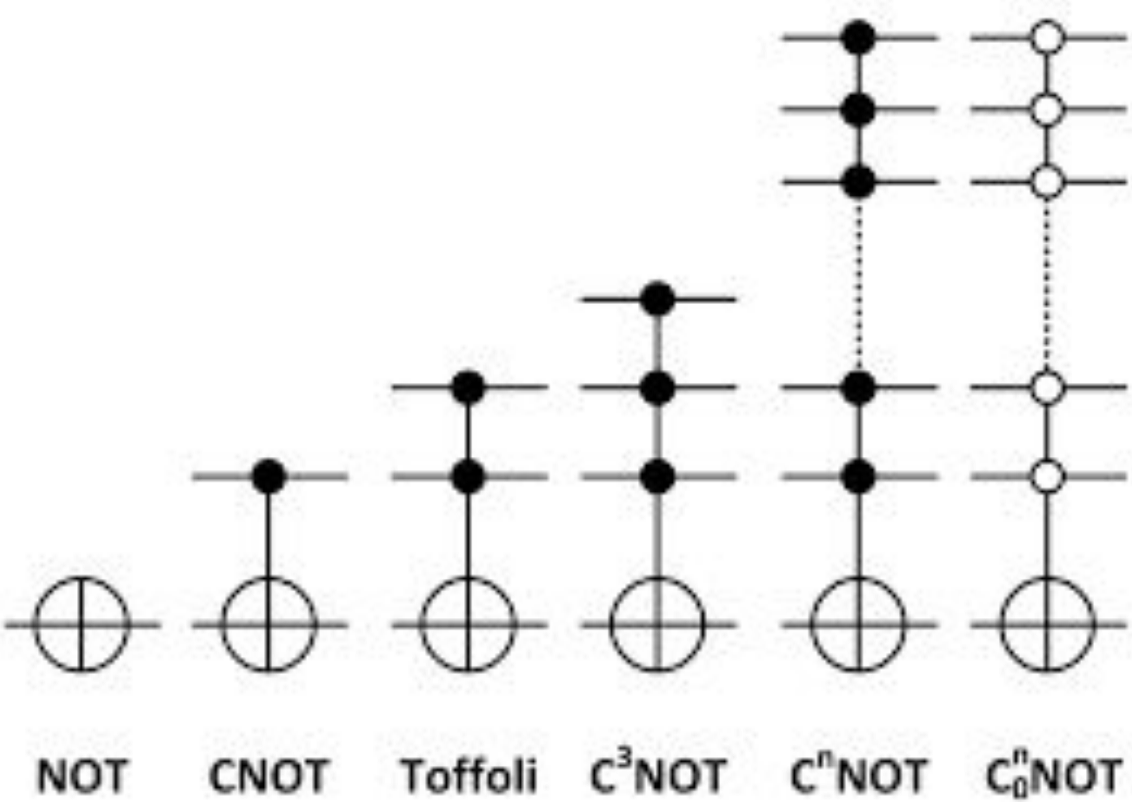



| input | | output | |
|---|---|---|---|
| x | y | x | y+x |
| $\|0\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|0\rangle$ |
| $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ |
| $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|1\rangle$ |
| $\|1\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ |

| input | | output | |
|---|---|---|---|
| x | y | x | y+x |
| 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 |

# Variants of CNOT Gates



# Essential Concepts

# Superposition

- Classical bits can exist in two possible states, typically labeled as "0" and "1".
- In contrast, because a qubit can exist in the “0” state, the “1” state, or any state that is a linear combination of 0 and 1.
- The state of superposition can be maintained only while a quantum system is unobserved. Once measured, the wave function of a quantum system in a state of superposition "collapses" into one of the basis states.
- A qubit can be in a superposition of 0 and 1, the quantum computer can perform multiple computations in parallel by processing all possible states of the qubits at once.

# Entanglement

- Entanglement is a fundamental concept of quantum mechanics that describes a non-classical correlation, or shared quantum state, between two or more quantum systems (or quantum particles) even if they are separated by a large distance.
- This phenomenon is also known as quantum non-locality, and it is one of the key features of quantum mechanics that distinguishes it from classical mechanics.

# Entanglement

- Quantum systems are described by a mathematical object called a wavefunction, which contains information about the possible outcomes of measurements that can be performed on the systems.
- When two or more quantum systems are entangled, their wave function cannot be expressed as a product of individual wavefunctions for each system.
- Instead, the systems are described by a single wave function that captures the correlation between them.
- The fact that entangled systems are described by a single wave function means that any actions or measurements made on one of the systems affect the state of the other systems.

# Entanglement

- In quantum computing, entanglement is used to enable quantum parallelism, which is the ability of quantum computers to perform multiple calculations simultaneously.
- Entanglement allows quantum computers to manipulate many qubits in a single operation, instead of manipulating each qubit individually, as in classical computing.

# Entanglement

- Entanglement enables quantum computers to implement various protocols and algorithms that are not possible with classical systems.
- For example, it is used in quantum teleportation, which allows for the transfer of quantum states between two distant systems.
- Entanglement is also a key resource for quantum error correction, which is necessary to protect quantum information from decoherence and other errors.
- By creating and manipulating entangled states, quantum computers can detect and correct errors in a way that is not possible for classical computers.

# Interference

- When a particle is in a superposition of multiple states, these states can interfere with each other leading to constructive or destructive interference.
- In quantum computing, interference is used in various ways to manipulate and control quantum states and to perform computational tasks.
- By applying quantum gates that create superpositions of qubits, and by controlling the relative phases of the states, interference can be used to amplify certain outcomes and suppress others.

# Interference

- Interference is the basis of many quantum algorithms and can lead to significant speedups in computation.
- One example of such an application is Grover's algorithm, which is used for unstructured search.
- Another example of interference being used in an algorithm is the Quantum Fourier transform (QFT), an algorithm in quantum computing that allows for efficient computation of certain mathematical functions.
- The QFT uses superpositions of different states, and quantum interference between them, to compute the Fourier transform of a quantum state.
- The interference between different paths in the QFT can be used to enhance the probability of measuring the correct solution and suppress the probability of measuring incorrect solutions, leading to a speedup in the computation.

# Interference

- Quantum interference is also used in quantum phase estimation, which is a technique used in various quantum algorithms to estimate the phase of a quantum state.
- Quantum phase estimation involves the interference between different quantum states, which can be controlled by applying quantum gates and measuring the resulting probability distribution.
- Furthermore, interference is a key concept in quantum error correction, which is necessary to protect quantum information from decoherence and other errors.
- By measuring the interference pattern of qubits, quantum computers can detect and correct errors that may have occurred during computation.

# Essential Mathematics

# Vector Space

In simple terms, a Vector Space V over a Field (F) is a set of vectors (objects) satisfying addition and multiplication of scalars.

Vector space is closed under addition and scalar multiplication.

1. $a(\alpha+\beta) = a\alpha+b\beta$ 2. $(a+b)\alpha = a\alpha+b\alpha$
3. $(ab)\alpha = a(b\alpha)$ 4. $1\alpha = \alpha$; $\forall a,b \in F$ and $\alpha,\beta \in V$;
here $1$ is the unity element of $F$.

# Dirac Notation

In Dirac notation, a quantum state is represented by a column vector denoted as a variable name enclosed in special symbols, e.g. $|\psi\rangle$.

The corresponding bra is the conjugate transpose of the ket, represented by a row vector also enclosed in special symbols, e.g., $\langle\psi|$.

The bra-ket notation allows for easy computation of quantum mechanical probabilities and amplitudes using linear algebra.

# Dirac Notation

Quantum states are represented by kets, such as $|0\rangle$ and $|1\rangle$, which correspond to the computational basis states of a single qubit.

Quantum operations are represented by linear operators, which correspond to unitary transformations on quantum states.

# Dirac Notation

- In quantum computing, it is often used to represent the state of a qubit, for example: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

  where $\alpha$ and $\beta$ are complex numbers called the probability amplitudes, and they satisfy the condition $|\alpha|^2 + |\beta|^2 = 1$, which ensures that the state is normalized.

- The example above tells us that the qubit is in a superposition of the $|0\rangle$ and $|1\rangle$ states, with probability amplitudes $\alpha$ and $\beta$, respectively.

# Dirac Notation

- Row vector can be represented as a Ket with the symbol |v>
- Column vector can be represented as a Bra with the symbol <v|
- The inner product will be written as <u|v> ‘bra-kets’

# Inner Product Space

It is a vector space with an inner product. Inner product associates with each pair of vectors in the space with a scalar quantity known as inner product of the vectors.

An inner product space is a vector space V over the field F together with an inner product, i.e., with a map

$$\langle x, y \rangle \; : \; V \times V \longrightarrow F \; ; \; x, y \in V$$

# Inner Product Space

Inner product space satisfies the three properties for all vectors and all scalars.

$$x,y,z \in V \; ; \; a \in F$$

1. *Conjugate Symmetry:* $\langle x,y\rangle = \overline{\langle y,x\rangle}$
2. *Linearity is the first argument:*

$$\langle ax,y\rangle = a\langle x,y\rangle$$

$$\langle x+y,z\rangle = \langle x,z\rangle + \langle y,z\rangle$$

3. *Positive-definite:*

$$\langle x,x\rangle > 0, \; x \in V - \{0\}$$

*Positive semi-definite Herimitian Form: if* $\langle x,x\rangle \geq 0$ *then* $x=0$.

# Inner Product with Different Spaces

Hilbert Space: A complete space with an inner product

Pre-Hilbert Space: An incomplete space with an inner product

Unitary Space: Inner product space over the field of complex numbers.

# Orthonormal Basis

For an Inner product space V with finite dimension there is a basis for V whose vectors are Orthonormal. They are all unit vectors and orthogonal to each other.

# Hilbert Space

- The combination of the vector space V with the inner product is Hilbert space. A Hilbert space is an abstract vector space of infinite dimensions possessing the structure of an inner product that allows length and angle to be measured.
- It generalizes the notion of Euclidean space and extends the methods of vector algebra and calculus from the two-dimensional Euclidean plane and three-dimensional space to spaces with any finite or infinite number of dimensions

# Operators

A linear Operator on a vector space H is a linear transformation T : H → H of the vector space to itself. It is a linear transformation which maps vectors in H to vectors in H.

The best example is the outer product

*The outer product of a Vector* $|\psi\rangle$ *with itself is written* $|\psi\rangle\langle\psi|$

$$|\psi\rangle\langle\psi||\varphi\rangle \longrightarrow |\psi\rangle\langle\psi||\varphi\rangle = \langle\psi|\varphi\rangle\,|\psi\rangle.$$

# Qubits

# Qubit

- A Quantum Bit is a two level quantum system.
- We can label the states $|0>$ and $|1>$.
- A qubit can be in state $|0\rangle$, $|1\rangle$ or in a linear combination of both states.
- A general pure qubit state is expressed as: $\psi=\alpha|0\rangle+\beta|1\rangle$ where $\alpha$ and $\beta$ are the complex probability amplitudes for each basis state.
- The choice of basis states is arbitrary, each set of orthogonal states can be used as basis states.

# Qubit

- Unlike a classical bit, which is definitely in either state, the state of Qubit is a general mix of |0> and |1>. We assume normalized states here.

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle$$

$$|c_0|^2 + |c_1|^2 = 1$$

# Qubit

Qubit could be represented as a superposition of two states with 2D vectors.

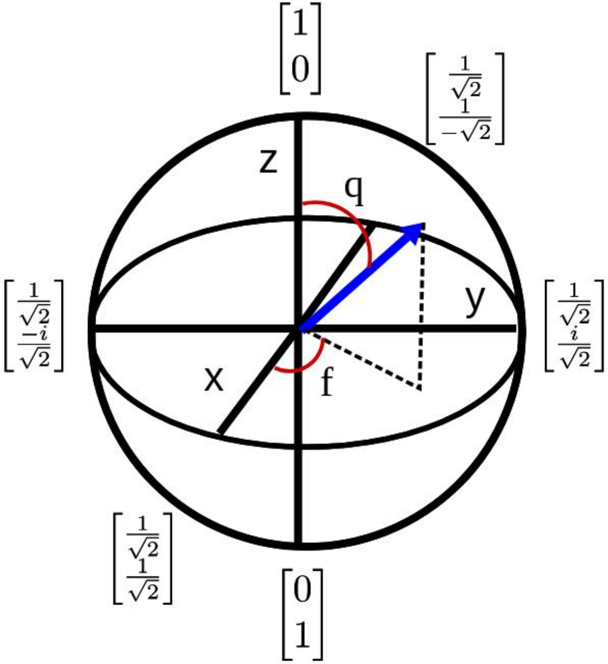
$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle =$$

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} =$$

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

# Bloch Sphere

- The Bloch sphere is a 3D sphere that represents the possible states of a qubit, with the north and south poles of the sphere corresponding to the |0⟩ and |1⟩ states, respectively.
- All other points on the surface of the sphere represent superposition states, which are linear combinations of the |0⟩ and |1⟩ states.
- By representing quantum states as points on the sphere, it is possible to visualize the effects of quantum operations on those states.
- For example, applying a Hadamard gate to a qubit in the |0⟩ state causes the qubit to move from the north pole of the sphere to the equator, which represents an equal superposition of |0⟩ and |1⟩ states.
- Similarly, applying an X-gate to a qubit in the |0⟩ state causes the qubit to move from the north pole to the south pole, which represents a flip of the qubit state from |0⟩ to |1⟩ .



# Quantum Gates

# Quantum Gate

- A Quantum Logic Gate is an operation that we perform on one more qubits that yield another set of qubits.
- We can represent them as linear operators in the Hilbert Space of the system.

# Single Qubit Gates

Some of the most important single qubit gates are:

- **X gate**: This gate is analogous to the NOT gate in classical computing. It flips the state of the qubit from $|0\rangle$ to $|1\rangle$ or from $|1\rangle$ to $|0\rangle$.
- **Z gate**: This gate flips the phase of the $|1\rangle$ state, leaving the $|0\rangle$ state unchanged.
- **Y gate**: This gate is equivalent to applying both X and Z gates and a global phase.
- **Hadamard gate**: This gate creates a superposition state by transforming the $|0\rangle$ state into an equal superposition of the $|0\rangle$ and $|1\rangle$ states.
- **S gate**: This gate is a 90-degree phase shift gate that introduces a phase shift of $\pi/2$ radians to the $|1\rangle$ state.
- **Arbitrary rotation gates**: Arbitrary rotation gates are a class of single-qubit gates that allow for arbitrary rotations around the three axes of the Bloch sphere (see definition of a Bloch sphere below). There are three arbitrary rotation gates in quantum computing: $Rx(\theta)$, $Ry(\theta)$, and $Rz(\theta)$. These gates are sometimes referred to as single-qubit rotation gates, or simply rotation gates.
- **T gate**: This gate is a 45-degree phase shift gate that introduces a phase shift of $\pi/4$ radians to the $|1\rangle$ state.

# Pauli Gates

- Named after physicist Wolfgang Pauli, the Pauli gates are the X gate, Y gate, and Z gate. Pauli gates perform a rotation of 180 degrees around the X, Y, and Z axes of the Bloch sphere, respectively.
- When a Pauli gate is applied to a qubit, the state of the qubit is rotated around the corresponding axis of the Bloch sphere. For example, the X gate is also known as the NOT gate and corresponds to a rotation of 180 degrees around the X axis.
- If a qubit is initially in the state $|0\rangle$, applying the X gate will result in the state $|1\rangle$, and vice versa. The Y and Z gates work similarly but correspond to rotations around the Y and Z axes of the Bloch sphere, respectively.
- The Y gate performs a rotation of 180 degrees around the Y axis, and the Pauli Z gate performs a rotation of 180 degrees around the Z axis. These gates are important for manipulating the phase of a qubit, which is essential for many quantum algorithms.

# Pauli Gate

- The X gate is often used as the basic building block for quantum circuits, and the Y and Z gates are important for performing phase shifts and other manipulations of quantum states.
- In addition to their importance in quantum algorithms, the Pauli gates are also essential for quantum error correction.
- Errors in quantum states typically correspond to deviations from the Pauli group, which means that the ability to manipulate states within the Pauli group is important for detecting and correcting errors.

# Multi Qubit Gates

Multi-qubit gates are a type of quantum gate that act on two or more qubits simultaneously. Multi-qubit gates enable the creation and manipulation of entangled states. Some of the commonly used multi-qubit gates are:

- **CNOT (Controlled-NOT) gate**: A two-qubit gate that performs a NOT operation on the target qubit if - and only if - the control qubit is in the state $|1\rangle$.
- **SWAP gate**: A two-qubit gate that swaps the states of two qubits.
- **Toffoli gate**: A three-qubit gate that performs a NOT operation on the target qubit only if both of the control qubits are in state $|1\rangle$. It is also known as the CCNOT gate (Controlled-Controlled-NOT) and is a key building block for many quantum algorithms.
- **Fredkin gate:** A three-qubit gate that swaps the states of two target qubits only if the control qubit is in the state $1\rangle$. It is also known as the CSWAP gate (Controlled-SWAP).

# Multi Qubit Gates

- Multi-qubit gates are often used in combination with single-qubit gates to perform operations on multiple qubits.
- For example, the CNOT gate is often used in combination with the single-qubit Hadamard gate to create a Bell state.
- Hadamard gates are used to create a superposition of the qubit's states.

# Multi Qubit Gates

- Multi-qubit gates play an important role in quantum computing in a number of ways. For example, the CNOT gate is used to create Bell states.
- The Bell state, also known as the Einstein-Podolsky-Rosen (EPR) state, is a maximally entangled state of two qubits.
- This means that the state of one qubit is entirely dependent on the state of the other qubit.

# Multi Qubit Gates

- To create a Bell state on a quantum computer, an algorithm will start by initializing two qubits to the $|0\rangle$ state, which is represented by the state vector $|00\rangle$.
- The algorithm would then apply a Hadamard gate to the first qubit, which will put it in a state of superposition. Next, the algorithm would apply a CNOT gate to the two qubits, with the first qubit acting as the control and the second qubit acting as the target.
- This gate will flip the state of the second qubit if the first qubit is in the $|1\rangle$ state, resulting in the following state vector: $(1/\sqrt{2})(|00\rangle + |11\rangle)$.
- The resulting state is the Bell state $|\Phi^+\rangle$, which is a maximally entangled state of the two qubits.

# Multi Qubit Gates

- Multi-qubit gates also play a crucial role in constructing universal gate sets, which are essential for performing arbitrary quantum computations.
- For example, the CNOT gate, along with single-qubit Hadamard and phase gates, is a universal gate set for a two-qubit quantum computer.
- Similarly, the Toffoli gate, along with single-qubit gates, is a universal gate set for a three-qubit quantum computer.

# Universal Gate Sets

- There are several universal gate sets in quantum computing. In general, a universal gate set for a quantum system requires a combination of single-qubit gates and multi-qubit gates. The specific set of gates depends on the architecture of the quantum system.
- One example of a universal gate set is the set of T gate, Hadamard gate, phase gate, and CNOT gate. Another combination is a Toffoli gate and a Hadamard gate.

# Universal Gate Sets

- Universal gate sets must be able to approximate any unitary operation to arbitrary precision.
- A unitary operation takes an input state and produces an output state, with the property that the input state can be recovered from the output state using the inverse of the unitary operation.
- Mathematically, a unitary operation is a linear transformation that preserves the inner product of quantum states and corresponds to a reversible quantum operation.
- Similar to how classical operations are implemented using smaller components like NAND or NOR gates, quantum computing unitaries are implemented using smaller single-qubit and few-qubit operations.

# Classical NAND Gate

One universal set for Classical Computation consists of only the NAND gate which returns 0 only if the two inputs are 1.

$$NOT(P) = NAND(P, P)$$

$$AND(P, Q) = NAND(NAND(P, Q), NAND(P, Q))$$

$$OR(P, Q) = NAND(NAND(P, P), NAND(Q, Q))$$

# Reversible Computation and Unitary Operations

- In Quantum Computing, we use unitary operations
- This ensures that all of the operations that we perform are reversible
- This is important because there is no way to perfectly copy a state in quantum computing as per no-cloning theorem.

# No-Cloning Theorem

- The No-Cloning Theorem says that there is no linear operation that copy an arbitrary state to one of the basis states:
- We can get around this if we are only interested in copying basis vectors.

$$|\psi\rangle|e_i\rangle \rightarrow |\psi\rangle|\psi\rangle$$

# DiVincenzo’s Criteria

- Any physical implementation of a quantum computer must have the following properties to be practical.
    - The number of Qubits can be increased
    - Qubits can be arbitrarily initialized
    - A Universal Gate Set must exist
    - Qubits can be easily read
    - Decoherence time is relatively small

# Decoherence

- As the number of Qubits increases, the influence of external environment perturbs the system.
- This causes the states in the computer to change in a way that is completely unintended and is unpredictable, rendering the computer useless.
- This is called decoherence.

# Quantum Algorithms

## Shor’s Algorithm

- One of the most famous quantum algorithms is Shor’s algorithm, developed by Peter Shor in 1994 to efficiently factor large numbers.
- The key to Shor’s algorithm is a step that uses Quantum Phase Estimation and the Quantum Fourier Transform to find a mathematical pattern that can be used to solve the problem.
- Quantum computers can perform this step much faster than classical computers, enabling a potentially large speed-up.

# Shor’s Algorithm

- It is important to note that Shor’s algorithm is a theoretical demonstration of the power of quantum computing.
- While it has been successfully implemented on small-scale quantum computers, factoring large numbers requires a fault-tolerant, large-scale quantum computer, which is still under development.

# Quantum amplitude amplification

- This is a technique used in quantum algorithms to intensify the amplitudes of the marked states in a quantum superposition, while decreasing the amplitudes of unmarked states.

# Quantum Fourier Transform

- The QFT is a quantum analogue of the classical discrete Fourier transform, which is used to transform a classical signal from its original time domain to a frequency domain.
- The QFT works by applying a sequence of quantum gates, called the QFT circuit, which consists of a sequence of Hadamard and controlled phase gates.
- This algorithm is a fundamental component of many other quantum algorithms, including Shor’s and quantum phase estimation.

# Draper adder

- An adder is a quantum circuit that uses quantum gates to perform addition of two numbers on a quantum computer.
- The Draper adder is based on the Quantum Fourier Transform and works by applying a sequence of controlled phase gates and single-qubit gates to input qubits, followed by the inverse QFT.
- The controlled phase gates encode the sum of the two input numbers, while the single-qubit gates are used to correct the carry bits.

# Beauregard adder:

- The Beauregard adder has a different structure than the Draper adder and can be more efficient in certain cases.
- It can be parallelized to compute multiple additions in parallel, and it is more fault tolerant than the Draper adder.

# Quantum Oracles

- Quantum oracles are used in many quantum algorithms, including Grover's search algorithm and Shor's algorithm.
- Grover's search algorithm uses a quantum oracle to take a superposition of all possible inputs and marks the inputs that satisfy the search criterion.
- Repeating this process several times with a cleverly chosen number of repetitions allows the algorithm to identify the desired item with high probability.

# Quantum Oracles

- Shor's algorithm uses a quantum oracle to perform modular exponentiation. The quantum oracle takes a superposition of all possible inputs and applies a function that maps each input to its modular exponentiation.
- By applying Quantum Fourier Transform on the resulting superposition, the algorithm can find the period of the function, which is used to factor the integer.

# Quantum Oracles

- Other examples of quantum oracles include the Deutsch-Jozsa algorithm, which determines whether a closed box function is constant or balanced, and Simon's algorithm, which finds a hidden period in a closed box function.
- These algorithms demonstrate the power of quantum oracles to perform computations more efficiently than is possible using classical algorithms.

# Quantum Error Correction

# Quantum Error Correction

- The error rates for quantum computers are typically much higher due to the nature of quantum mechanics and the challenges associated with building and operating quantum systems.
- Noise, decoherence, and imperfections in quantum gates can cause errors in quantum computations.

# Error Rates

- Current state-of-the-art quantum computers have error rates that are typically in the range of 1% to 0.1%.
- In other words, this means that on average one out of every 100 to 1000 quantum gate operations will result in an error. In classical computing, errors often occur as bit flips, where a 0 changes to a 1 or vice versa.

# Bit Flips and Phase Flips

- Errors on quantum computers can manifest as bit flips as well. However, unlike classical computers, quantum errors can also manifest as phase flips or a combination of both.
- Overall, error rates in quantum computing are more common than on classical chips because quantum states are extremely fragile and sensitive to their environment.

# Encoding Techniques

Quantum error correction works by encoding the quantum information in a way that allows errors to be detected and corrected.

This is typically done by encoding the information into a larger set of qubits, called a “quantum error-correcting code,” which is designed to be resilient to errors.

# Error Correcting Codes

- Shor code: This was the first quantum error correction code, developed by Peter Shor. It uses nine qubits to encode a single logical qubit and can correct both bit flip and phase flip errors.
- Steane code: This is a seven-qubit code that can correct both bit flip and phase flip errors. It has the advantage of being fault-tolerant, meaning that the error correction process itself does not introduce additional errors.

# Error Correcting Codes

- Surface code: This is a topological error correction code that uses a two-dimensional lattice of qubits to encode logical qubits. It has a high error correction threshold and is considered one of the most promising techniques for large-scale, fault-tolerant quantum computing.
- Hastings-Haah code: This quantum error correction code offers better space-time costs than surface codes on Majorana qubits in many regimes. For gate-based instruction sets, the overhead is larger, and makes it less interesting compared to the surface code.

# Quantum Information

# Quantum Information Theory - An Introduction

- In quantum information theory we study quantum states independently on the exact physical system they describe.
- It is a theory about the quantum mechanical state space.
- It is about the general structure of quantum states and their potential and limitations for information processing, such as computational tasks, communication, or error correction.

# Quantum Information - Basic Framework

- Quantum states as vectors with complex number entries that allow classical information to be extracted from quantum states and operations on quantum states are described by unitary matrices
- Quantum states can be represented by density matrices, which is a powerful representation. It is very effective to model the effect of noise in quantum computations or the state of one piece of an entangled pair.

# Quantum State Vectors

- A quantum state of a system is represented by a column vector.
- Vectors representing quantum states are characterized by two properties:
  - The entries of a quantum state vector are complex numbers.
  - The sum of the absolute values squared of the entries of a quantum state vector is 1.
- Quantum state vectors are unit vectors with respect to the Euclidean norm.

The *Euclidean norm* of a column vector

$$v = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

is denoted and defined as follows:

$$\|v\| = \sqrt{\sum_{k=1}^{n} |\alpha_k|^2}.$$

# Examples of Qubit States

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \quad \text{and} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle,$$

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

$$\begin{pmatrix} \frac{1+2i}{3} \\ -\frac{2}{3} \end{pmatrix} = \frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle.$$

Laws of quantum physics are reversible in time

Thus probability is conserved as a quantum state evolves with time.

# Quantum States Evolve in Time!

Quantum states evolve in time according to the Schrödinger equation.

$$i\hbar\frac{\partial}{\partial t}\left|\Psi\right\rangle = \hat{H}\left|\Psi\right\rangle$$

Schrodinger time evolution operator is unitary and preserves the norm of quantum mechanical states

# Hamiltonian Operator generates the time evolution of quantum states

Hamiltonian of a system is an operator corresponding to the total energy

The Planck constant ħ=h/2π is a constant of action in the dynamic geometrical process that we see and feel as the passage of time.

This quantity describes how the wave function Ψ changes from one moment to another as the future unfolds

A mathematical quantity called an ‘imaginary number’. This is equal to the square root of minus one.

The process is squared representing a dynamic geometry

$$-\frac{\hbar^2}{2m}\nabla^2\Psi + V\Psi = i\hbar\frac{\partial\Psi}{\partial t}$$

This describes the forces acting on the particle

Mass is relative to this process

If this is reformulated as a linear vector | Ψ (t) > each new vector is formed by adding the two previous vectors together. This naturally forms the Fibonacci Sequence 0, 1, 1, 2, 3, 5, 8, 13, 21... Over a period of time this forms the Fibonacci Spiral in plant growth.

Describes how Ψ changes its geometrical shape as a process that forms the passage of time.

# Hilbert Space

- In quantum computing, Hilbert space is a linear vector space that is complete and has an inner product.
- A wave function in a complex Hilbert space specifies the state of a quantum mechanical system, and wave functions can be thought of as vectors in Hilbert space.
- The term "Hilbert space" is often reserved for an infinite-dimensional inner product space having the property that it is complete or closed.

# Formalism of Hilbert Space

- Every isolated quantum system can be associate with a Hilbert space H, which is a complex vector space together with an inner product.
- The system is completely described by its state vector $\psi \in H$ (density operator $\rho$ on H).

# A Closer Look at Hilbert Space

A Hilbert space is an abstract vector space of infinite dimensions possessing the structure of an inner product that allows length and angle to be measured.

It generalizes the notion of Euclidean space and extends the methods of vector algebra and calculus from the two-dimensional Euclidean plane and three-dimensional space to spaces with any finite or infinite number of dimensions

# Questions?