Quantum Computing Basics

Jackson Walters

February 22, 2025

Quantum computers

Outline

- Quantum computers

Outline

- Quantum computers
- Qubits

Outline

- Quantum computers
- Qubits
- Quantum gates

Outline

- Quantum computers
- Qubits
- Quantum gates
- Quantum algorithms

Outline

- Quantum computers
- Qubits
- Quantum gates
- Quantum algorithms
- Grover's algorithm

Outline

- Quantum computers
- Qubits
- Quantum gates
- Quantum algorithms
- Grover's algorithm
- Demo!

Richard Feynman on Quantum Computing

"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem because it doesn't look so easy." - Richard Feynman

"Trying to find a computer simulation of physics seems to me to be an excellent program to follow out... and I might be very surprised if it turned out that a classical simulation of physics could ever work." - Richard Feynman

Background and History of Quantum Computing

- 1981: Richard Feynman proposed quantum computers to efficiently simulate quantum systems.
- 1985: David Deutsch introduced the concept of a universal quantum computer.
- 1994: Peter Shor developed an algorithm for efficient integer factorization, threatening classical cryptography.
- Early 2000s: Experimental implementations of quantum gates and circuits began advancing.
- Present: Rapid progress in quantum hardware (superconducting qubits, trapped ions) and error correction.

What is a quantum computer?

- Classical computers operate by manipulating bits (0 or 1) using logic gates (AND, OR, NOT)

What is a quantum computer?

- Classical computers operate by manipulating bits (0 or 1) using logic gates (AND, OR, NOT)
- These gates form a boolean algebra, and every algorithm can be represented by a Boolean circuit

What is a quantum computer?

- Classical computers operate by manipulating bits (0 or 1) using logic gates (AND, OR, NOT)
- These gates form a boolean algebra, and every algorithm can be represented by a Boolean circuit
- Quantum computers are a generalization of classical computers

What is a quantum computer?

- Classical computers operate by manipulating bits (0 or 1) using logic gates (AND, OR, NOT)
- These gates form a boolean algebra, and every algorithm can be represented by a Boolean circuit
- Quantum computers are a generalization of classical computers
- In a QC, we have two states $|0\rangle$ and $|1\rangle$ which can be in superposition

What is a quantum computer?

- Classical computers operate by manipulating bits (0 or 1) using logic gates (AND, OR, NOT)
- These gates form a boolean algebra, and every algorithm can be represented by a Boolean circuit
- Quantum computers are a generalization of classical computers
- In a QC, we have two states $|0\rangle$ and $|1\rangle$ which can be in superposition
- The gates are now unitary operators (complex rotations). They're invertible!

What is a quantum computer?

- Classical computers operate by manipulating bits (0 or 1) using logic gates (AND, OR, NOT)
- These gates form a boolean algebra, and every algorithm can be represented by a Boolean circuit
- Quantum computers are a generalization of classical computers
- In a QC, we have two states $|0\rangle$ and $|1\rangle$ which can be in superposition
- The gates are now unitary operators (complex rotations). They're invertible!
- The basic gates are Hadamard, Pauli (X, Y, Z), phase (S, T), CNOT, SWAP, CCNOT

What is a quantum computer?

- Classical computers operate by manipulating bits (0 or 1) using logic gates (AND, OR, NOT)
- These gates form a boolean algebra, and every algorithm can be represented by a Boolean circuit
- Quantum computers are a generalization of classical computers
- In a QC, we have two states $|0\rangle$ and $|1\rangle$ which can be in superposition
- The gates are now unitary operators (complex rotations). They're invertible!
- The basic gates are Hadamard, Pauli (X, Y, Z), phase (S, T), CNOT, SWAP, CCNOT
- Hadamard, CNOT, and T-gates together are **universal**

What is a qubit?

- A qubit is a physical system which can be in one of two possible eigenstates we can measure

What is a qubit?

- A qubit is a physical system which can be in one of two possible eigenstates we can measure
- e.g. an electron with a spin which can be either $|\uparrow\rangle$ (spin up) or $|\downarrow\rangle$ (spin down)

What is a qubit?

- A qubit is a physical system which can be in one of two possible eigenstates we can measure
- e.g. an electron with a spin which can be either $|\uparrow\rangle$ (spin up) or $|\downarrow\rangle$ (spin down)
- physically, the electron is in a magnetic field, and can be aligned or anti-aligned with it. $\Delta E = 2\mu_B B$

What is a qubit?

- A qubit is a physical system which can be in one of two possible eigenstates we can measure
- e.g. an electron with a spin which can be either $|\uparrow\rangle$ (spin up) or $|\downarrow\rangle$ (spin down)
- physically, the electron is in a magnetic field, and can be aligned or anti-aligned with it. $\Delta E = 2\mu_B B$
- the spin is like quantum angular momentum, and has units $\pm\hbar/2$

What is a qubit?

- A qubit is a physical system which can be in one of two possible eigenstates we can measure
- e.g. an electron with a spin which can be either $|\uparrow\rangle$ (spin up) or $|\downarrow\rangle$ (spin down)
- physically, the electron is in a magnetic field, and can be aligned or anti-aligned with it. $\Delta E = 2\mu_B B$
- the spin is like quantum angular momentum, and has units $\pm\hbar/2$
- label our qubits $|0\rangle$ and $|1\rangle$ since they are two distinct states

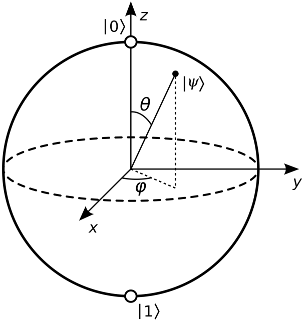
What is a qubit? (cont.)

$$c_0, c_1 \in \mathbb{C}$$

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

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

$$c_{00}^2 + c_{01}^2 + c_{10}^2 + c_{11}^2 = 1$$



What is a qubit? (cont.)

- state space of a qubit appears to be a 3-sphere

What is a qubit? (cont.)

- state space of a qubit appears to be a 3-sphere
- however, there is also a "global phase" $e^{i\theta}$ since $|e^{i\theta}c_0|^2 + |e^{i\theta}c_1|^2 = 1$ for all θ

What is a qubit? (cont.)

- state space of a qubit appears to be a 3-sphere
- however, there is also a "global phase" $e^{i\theta}$ since $|e^{i\theta}c_0|^2 + |e^{i\theta}c_1|^2 = 1$ for all θ
- the resulting quotient space is a 2-sphere known as the Bloch sphere

What is a qubit? (cont.)

- state space of a qubit appears to be a 3-sphere
- however, there is also a "global phase" $e^{i\theta}$ since $|e^{i\theta}c_0|^2 + |e^{i\theta}c_1|^2 = 1$ for all θ
- the resulting quotient space is a 2-sphere known as the Bloch sphere
- i.e. can parameterize states with two angles

What is a measurement?

- complex amplitudes associated to “wavefunction”

What is a measurement?

- complex amplitudes associated to “wavefunction”
- when we measure, we get only one eigenstate $|0\rangle$ or $|1\rangle$

What is a measurement?

- complex amplitudes associated to “wavefunction”
- when we measure, we get only one eigenstate $|0\rangle$ or $|1\rangle$
- $\text{prob}(|0\rangle) = |c_0|^2$, $\text{prob}(|1\rangle) = |c_1|^2$

What is a measurement?

- complex amplitudes associated to “wavefunction”
- when we measure, we get only one eigenstate $|0\rangle$ or $|1\rangle$
- $\text{prob}(|0\rangle) = |c_0|^2$, $\text{prob}(|1\rangle) = |c_1|^2$
- prob. always in $[0, 1]$ since $\sum_i |c_i|^2 = 1$

What is a measurement?

- complex amplitudes associated to “wavefunction”
- when we measure, we get only one eigenstate $|0\rangle$ or $|1\rangle$
- prob$(|0\rangle) = |c_0|^2$, prob$(|1\rangle) = |c_1|^2$
- prob. always in $[0,1]$ since $\sum_i |c_i|^2 = 1$
- can manipulate amplitudes, but outcome is random w.r.t. prob. distribution $\{|c_i|^2\}$

Tensor products, input register

- we can combine single qubit states to get multi-qubit states

Tensor products, input register

- we can combine single qubit states to get multi-qubit states
- e.g. $|0\rangle \otimes |0\rangle = |00\rangle$, $|0\rangle \otimes |1\rangle = |01\rangle$

Tensor products, input register

- we can combine single qubit states to get multi-qubit states
- e.g. $|0\rangle \otimes |0\rangle = |00\rangle$, $|0\rangle \otimes |1\rangle = |01\rangle$
- $c_0|0\rangle + c_1|1\rangle \in \mathcal{V}_2$

Tensor products, input register

- we can combine single qubit states to get multi-qubit states
- e.g. $|0\rangle \otimes |0\rangle = |00\rangle$, $|0\rangle \otimes |1\rangle = |01\rangle$
- $c_0|0\rangle + c_1|1\rangle \in \mathcal{V}_2$
- $\mathcal{V}_2 \otimes \mathcal{V}_2 \otimes \ldots \otimes \mathcal{V}_2 = \mathcal{V}_2^{\otimes n} = \mathcal{V}_{2^n} := \mathcal{H}$

Tensor products, input register

- we can combine single qubit states to get multi-qubit states
- e.g. $|0\rangle \otimes |0\rangle = |00\rangle$, $|0\rangle \otimes |1\rangle = |01\rangle$
- $c_0|0\rangle + c_1|1\rangle \in \mathcal{V}_2$
- $\mathcal{V}_2 \otimes \mathcal{V}_2 \otimes \ldots \otimes \mathcal{V}_2 = \mathcal{V}_2^{\otimes n} = \mathcal{V}_{2^n} := \mathcal{H}$
- $\mathcal{H} = 2^n$ dim'l Hilbert space w/ inner product $\langle x, y\rangle = \sum_i x_i \overline{y_i}$

Tensor products, input register

- we can combine single qubit states to get multi-qubit states
- e.g. $|0\rangle \otimes |0\rangle = |00\rangle$, $|0\rangle \otimes |1\rangle = |01\rangle$
- $c_0|0\rangle + c_1|1\rangle \in \mathcal{V}_2$
- $\mathcal{V}_2 \otimes \mathcal{V}_2 \otimes \ldots \otimes \mathcal{V}_2 = \mathcal{V}_2^{\otimes n} = \mathcal{V}_{2^n} := \mathcal{H}$
- $\mathcal{H} = 2^n$ dim'l Hilbert space w/ inner product $\langle x, y \rangle = \sum_i x_i \overline{y_i}$
- e.g. $|00\ldots0\rangle \in \mathcal{H}$, $|10\ldots0\rangle \in \mathcal{H}$, $N := 2^n$ states, n qubits

Tensor products, input register

- we can combine single qubit states to get multi-qubit states
- e.g. $|0\rangle \otimes |0\rangle = |00\rangle$, $|0\rangle \otimes |1\rangle = |01\rangle$
- $c_0|0\rangle + c_1|1\rangle \in \mathcal{V}_2$
- $\mathcal{V}_2 \otimes \mathcal{V}_2 \otimes \ldots \otimes \mathcal{V}_2 = \mathcal{V}_2^{\otimes n} = \mathcal{V}_{2^n} := \mathcal{H}$
- $\mathcal{H} = 2^n$ dim'l Hilbert space w/ inner product $\langle x, y\rangle = \sum_i x_i \overline{y_i}$
- e.g. $|00\ldots0\rangle \in \mathcal{H}$, $|10\ldots0\rangle \in \mathcal{H}$, $N := 2^n$ states, n qubits
- basis $\{|00\ldots0\rangle, |01\ldots0\rangle, |11\ldots0\rangle\}, \ldots, |11\ldots1\rangle\}$

Quantum Gates (Hadamard)

Action on Qubit:

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

$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Matrix Representation:

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

Note $(1/\sqrt{2})^2 = .5$, so fully mixed. 1 qubit $=$ 2 dim'l space.

Action of n Hadamard Gates on a Register

Consider the initial state of a quantum register with n qubits, all in the state $|0\rangle$:

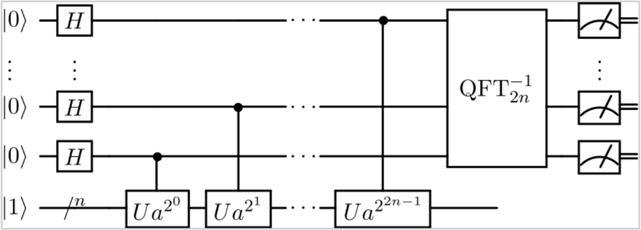
$$|0\rangle^{\otimes n} = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle.$$

After applying n Hadamard gates, one on each qubit, the state transforms into a uniform superposition of all 2^n basis states:

$$H^{\otimes n}|0\rangle^{\otimes n} = \underbrace{H|0\rangle \otimes H|0\rangle \otimes \cdots \otimes H|0\rangle}_{n \text{ times}} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

Here, the state is now a superposition of all possible 2^n computational basis states, each with equal amplitude.

Shor's algorithm circuit



Quantum subroutine in Shor's algorithm

T Gate and Its Matrix Representation

T Gate:

The T gate, also known as the $\pi/4$-rotation gate, applies a phase of $\frac{\pi}{4}$ to the $|1\rangle$ state, while leaving $|0\rangle$ unchanged.

Action on Qubits:

$$T|0\rangle = |0\rangle, \quad T|1\rangle = e^{i\frac{\pi}{4}}|1\rangle.$$

Matrix Representation:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

Quantum gates (CNOT)

The Controlled-NOT (CNOT) gate flips the target qubit if the control qubit is in the state $|1\rangle$, otherwise it leaves the target unchanged.
It operates on two qubits (so a $2^2 = 4$ dim'l space).

$$\mathrm{CNOT}|c, t\rangle = |c, t \oplus c\rangle,$$

where c is the control qubit and t is the target qubit, and $\oplus$ denotes addition modulo 2.

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

Unitarity in Quantum Mechanics

Unitarity of Quantum Gates:
A quantum operation is said to be *unitary* if it preserves the total probability, i.e., the norm of the quantum state. This ensures that the probabilities of all possible outcomes add up to 1.

Definition of Unitarity: A matrix U is unitary if it satisfies the condition:

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

where $U^\dagger$ is the conjugate transpose of U, and I is the identity matrix. Generalization of rotations $(RR^T = I)$ to complex vector spaces.

In QM, $|\psi(t)\rangle = e^{i\hbar Ht}|\psi(0)\rangle$ is solution to Schrödinger equation, and $e^{i\hbar Ht}$ is unitary.

Grover's algorithm (cont.)

Grover's Algorithm:
Grover's algorithm is a quantum algorithm designed to search an unsorted database of N items in $O(\sqrt{N})$ time. This provides a quadratic speedup over classical search algorithms, which take $O(N)$ time.

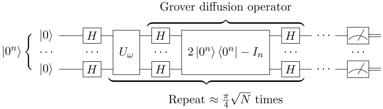
Key Idea: Rotation in State Space The core of Grover's algorithm is performing a series of quantum operations that rotate the quantum state towards the correct answer in the Hilbert space. Each iteration applies two key operations that amplify the amplitude of the correct solution.

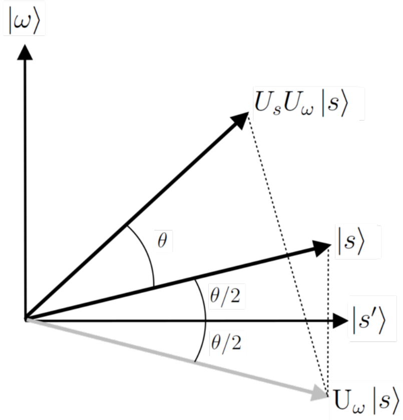
Quantum Speedup: - Classically, $O(N)$ queries are needed to search through N items. - Grover's algorithm achieves $O(\sqrt{N})$ queries, providing a quadratic speedup.

Grover's algorithm (cont.)

1. **Initialization**: Start with a uniform superposition of all possible states using Hadamard gates.
2. **Oracle Query**: The oracle flips the phase of the state corresponding to the correct solution, creating a difference between the correct state and all others.
3. **Amplitude Amplification**: Apply the Grover operator, which acts as a rotation in the space, amplifying the amplitude of the correct state.
4. **Iteration**: Repeat the amplitude amplification step $O(\sqrt{N})$ times, effectively rotating the state closer to the solution.
5. **Measurement**: After $O(\sqrt{N})$ iterations, measure the state to collapse it to the correct solution with high probability.

Grover's algorithm circuit, geometry


Grover diffusion operator
$|0^n\rangle$
$|0\rangle$
$\cdots$
$|0\rangle$
H
U_ω
H
$2\,|0^n\rangle\langle 0^n| - I_n$
H
$\cdots$
Repeat $\approx \frac{\pi}{4}\sqrt{N}$ times



Demo

https://github.com/jacksonwalters/shors-algorithm