An Introduction to Quantum Speedups: How Superposition Creates Computational Advantages

Today we'll see how quantum computers can solve certain problems with fewer function evaluations than any classical algorithm, using mathematical concepts accessible to algorithms researchers.

No prior knowledge of quantum mechanics required!

Classical Bits vs Qubits

Classical Bits:

- Possible values: 0 or 1
- To observe the value: read the bit directly
- That's it!

Qubits:

|2

- Basic states: $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ (equivalent to classical 0 and 1)
- Key difference: qubits can exist in **superposition**

Ket Notation: $|\mathbf{0}\rangle$ is read as "ket zero," $|\mathbf{1}\rangle$ is "ket one"

Superposition States: A qubit can be in a combination of $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$

The Four Main Superposition States

In reality, superposition involves complex numbers, but we'll use a simplified model where weights are just +1 or -1.

The four key superposition states for this talk:

- $\underline{|+\rangle} = \underline{|\mathbf{0}\rangle + |\mathbf{1}\rangle}$ ← signs "agree"
- $\underline{|-\rangle} = \underline{|\mathbf{0}\rangle - |\mathbf{1}\rangle}$ ← signs "disagree"
- $-|+\rangle = -|\mathbf{0}\rangle - |\mathbf{1}\rangle$ ← signs agree
- $-|-\rangle = -|\mathbf{0}\rangle + |\mathbf{1}\rangle$ ← signs disagree

Key Insight: These different superposition states contain different information!

Measurement Overview

Classical bits: You can determine the state of a bit by simply looking at it. Is the switch on, or is it off?

Qubits: You cannot learn the state of a qubit by looking at it. You have to perform an operation called *measurement* that will reveal certain aspects of the state to us but may alter/destroy certain aspects of the state as well.

Important capability: If we know a qubit is in one of two specific superposition states, a quantum computer can determine with certainty which one it is.

For example:

- If we know the state is either $\underline{|+\rangle}$ or $\underline{|-\rangle}$, we can determine which one with certainty
- However, if the state is $\underline{-|+\rangle}$, measurement will reveal $\underline{|+\rangle}$ (we lose the sign information)
- In other words, the quantum computer can determine if the signs "agree" or "disagree", but they don't let us know exactly what the signs actually are.

This measurement capability is the key to quantum speedup in our algorithm!

Multiple Qubit States

If qubit 1 is in state $\underline{|\mathbf{0}\rangle}$ and qubit 2 is in state $\underline{|\mathbf{1}\rangle}$:

Joint state: $\underline{|\mathbf{01}\rangle}$

If qubit 1 is in state $|\mathbf{0}\rangle$ and qubit 2 is in superposition $(|\mathbf{0}\rangle - |\mathbf{1}\rangle)$:

$$|0\rangle(|0\rangle - |1\rangle) = |00\rangle - |01\rangle$$

If qubit 1 is in state $(|\mathbf{0}\rangle + |\mathbf{1}\rangle)$ and qubit 2 is in state $(|\mathbf{0}\rangle - |\mathbf{1}\rangle)$:

$$(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = |00\rangle - |01\rangle + |10\rangle - |11\rangle$$

Basics of Quantum Algorithms

Example Problem: Implement the logical AND function

- Input: two qubits
- Output: $|\mathbf{1}\rangle$ if input is $|\mathbf{11}\rangle$, otherwise $|\mathbf{0}\rangle$

Key Constraint: Quantum algorithms must be **reversible**

Problem: AND is not reversible!

- If output is $|\mathbf{0}\rangle$, input could be $|\mathbf{00}\rangle$, $|\mathbf{01}\rangle$, or $|\mathbf{10}\rangle$
- Cannot determine input from output alone

Reversible AND Implementation

Algorithm: Takes 3 qubits as input, outputs 3 qubits

- First two qubits: input values for AND
- Third qubit: output storage location

Pseudocode:

```
If both input qubits are $|\mathbf{1}\rangle$, flip the output qubit.
Else, do nothing.
```

Truth Table:

$$\text{AND}(|\mathbf{000}\rangle) = |\mathbf{000}\rangle$$

$$\text{AND}(|\mathbf{001}\rangle) = |\mathbf{001}\rangle$$

$$\text{AND}(|\mathbf{010}\rangle) = |\mathbf{010}\rangle$$

$$\text{AND}(|\mathbf{011}\rangle) = |\mathbf{011}\rangle$$

$$\text{AND}(|\mathbf{100}\rangle) = |\mathbf{100}\rangle$$

$$\text{AND}(|\mathbf{101}\rangle) = |\mathbf{101}\rangle$$

$$\text{AND}(|\mathbf{110}\rangle) = |\mathbf{111}\rangle$$

$$\text{AND}(|\mathbf{111}\rangle) = |\mathbf{110}\rangle$$

Quantum Algorithms and Superposition

Key Property: Quantum algorithms apply to superposition states linearly

Example:

$$\mathrm{AND}(\underbrace{(|001\rangle - |110\rangle)}) = \mathrm{AND}(|001\rangle) - \mathrm{AND}(|110\rangle)$$

$$= |001\rangle - |111\rangle$$

Note this is only one evaluation of AND

Quantum parallelism.

1985

Deutsch's Algorithm: The Problem

$f(0) = 0$ or 1
$f(1) = 0$ or 1

Given: A black-box function $f : \{0,1\} \rightarrow \{0,1\}$

Goal: Determine if $f(0) = f(1)$ (both map to 0 or both map to 1), or $f(0) \neq f(1)$ (one maps to 0, other maps to 1)

Classical Solution: Need to compute $f(0)$, then compute $f(1)$, then compare the results. This is 2 function evaluations.

Quantum Solution: Need only 1 function evaluation!

Quantum Black-Box Setup

We can send any two-qubit quantum state to the black-box and get it back after the function has been applied.

Black-box behavior:

- Input qubit: represents input to function f
- Output qubit: gets flipped if $f(\text{input}) = 1$

The Standard Algorithm

$(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$

Step 1: Prepare state $|+-\rangle = |00\rangle - |01\rangle + |10\rangle - |11\rangle$

Step 2: Apply black-box function

$f(0)=0,\ f(1)=1$

$$= |00\rangle - |01\rangle + |11\rangle - |10\rangle$$

$$= \underbrace{|00\rangle - |01\rangle}_{\text{signs same as input}} \underbrace{-|10\rangle + |11\rangle}_{\text{signs flipped from input}}$$

$$= (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$$

$$= |--\rangle$$

$f(0)=1,\ f(1)=1$

$$= |01\rangle - |00\rangle + |11\rangle - |10\rangle$$

$$= \underbrace{-|00\rangle + |01\rangle}_{\text{signs flipped}} \underbrace{-|10\rangle + |11\rangle}_{\text{signs flipped}}$$

$$= (-|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$$

$$= -|+-\rangle$$

Key Insight: How the Black-Box Affects Signs

When $f(\text{input}) = 1$: flip the output qubit

This effectively swaps the signs in our superposition!

For input 0:

- If $f(0) = 0$: signs preserved
- If $f(0) = 1$: signs flipped

For input 1:

- If $f(1) = 0$: signs preserved
- If $f(1) = 1$: signs flipped

The Two Cases

Case 1: $f(0) = f(1)$

- Both inputs agree on whether signs should flip
- Both $f(0)$ and $f(1)$ are 0, OR both are 1
- Result: Input qubit ends up in state $|+\rangle$

Case 2: $f(0) \neq f(1)$

- Inputs disagree on whether signs should flip
- One of $f(0), f(1)$ is 0, the other is 1
- Result: Input qubit ends up in state $|-\rangle$

Step 3: The quantum computer determines the state of the input qubit

- $|+\rangle \Rightarrow f(0) = f(1)$
- $|-\rangle \Rightarrow f(0) \neq f(1)$

Why This Algorithm Works: Building Intuition

Let's build intuition for why this works by seeing what happens with different input preparations.

What if we prepare $|++\rangle$ instead?

$$|++\rangle = |\mathbf{00}\rangle + |\mathbf{01}\rangle + |\mathbf{10}\rangle + |\mathbf{11}\rangle$$

Problem: All signs are positive!

Flipping the output qubit doesn't change anything meaningful.

Result: Cannot learn anything about the function.

What about $|-+\rangle$?

$$|-+\rangle = |\mathbf{00}\rangle + |\mathbf{01}\rangle - |\mathbf{10}\rangle - |\mathbf{11}\rangle$$

We have two +1s and two -1s, but...

Problem: Both +1s correspond to input $= 0$, both -1s correspond to input $= 1$

Whether we flip signs for an input or not, the overall pattern stays the same.

Result: Cannot learn anything about the function.

What about $|{-}{-}\rangle$?

$$|{-}{-}\rangle = |\mathbf{00}\rangle - |\mathbf{01}\rangle - |\mathbf{10}\rangle + |\mathbf{11}\rangle$$

Perfect! Each input value (0 and 1) has different signs for different output values.

Flipping the output qubit **will** create a detectable change in the quantum state.

However, the measurement interpretation is flipped:

- $|+\rangle \Rightarrow f(0) \neq f(1)$
- $|-\rangle \Rightarrow f(0) = f(1)$

Key Takeaways

Critical requirement: The output qubit must be prepared in state $|-\rangle$

This is what allows the quantum computer to detect whether signs have flipped or not.

Flexible choice: The input qubit can be in state $|+\rangle$ or $|-\rangle$

Whatever we choose determines how we interpret the final result.

The Quantum Advantage:

- Classical: 2 function evaluations required
- Quantum: 1 function evaluation sufficient
- Achieved through superposition and careful state preparation

This demonstrates the essence of quantum speedup: extracting global properties of functions with fewer queries than classically possible.