What are quantum computers and how do they compare to classical computers?

Julie Butler

Why should we learn quantum computing and quantum information?

How Does a Classical Computer Work?

- Components: RAM, Hard Drive, Graphics Card, Monitor, Keyboard, Mouse, etc.
- The computer is controlled by the central processing unit (CPU) which is made up of millions or billions of transistors
  - Transistor: a small electrical component that can be off (no electricity flows through it) or on (electricity flows through it)
  - The state of the transistors is actually what controls the computer and controls how it responds to inputs and produces outputs

Classical Bits

- These are the building blocks of a classical computer, the components that produce the 1's and 0's which make-up binary code
  - The transistors that make up the computer (no electricity flowing is 0, electricity flowing is 1)
  - Bit = Binary Digit
- After writing code (in human language), a computer compiles the code into binary (computer language) by changing the states of the transistors on the CPU

Classical Physics

- Classical mechanics (of macroscopic objects), Electricity, Magnetism, Optics, etc. (PHY 101 and 102)
- Given a set of initial conditions and knowing everything about the system, you can predict what state the system will be in at any given time
  - It may be complicated but it is (at least theoretically) solvable
  - **Deterministic**

Quantum Physics (Quantum Mechanics)

- Quantum physics (or quantum mechanics) is the study of very small objects (atoms, nuclei, electrons, protons, etc.)
- At this scale the known laws of physics break down and we are left with something new
- We describe the particles using a wavefunction, which is not physically real but rather a mathematical representation of the particle
  - We determine physical quantities of the particle through performing mathematical operations on the wavefunction
- However, there is a caveat $\longrightarrow$ quantum mechanics is **probabilistic**, we can never know anything for certain

Important Concepts in Quantum Mechanics

- Particle-Wave Duality: microscopic objects behave as a particle in some cases, but as a wave in others (this is why we describe them with a **wave**function)
- Superposition: a classical object can have many possible state but can only be in one at a time, a quantum object can have many possible states and can be in one or more at a time (it is in a superposition of all states at all times)
    - Schrodinger's Cat

Important Concepts in Quantum Mechanics (Continued)

- Measurement and Collapse: If we want to determine the state of a particle we **measure** it (by some means). This forces the wavefunction to collapse into a single state (even if it was in a superposition of states).
- Entanglement: If the wavefunction of two different particles interact then the wavefunctions entangle; the two particles are no longer independent, changing the state of one particle changes the state of the other particle

Qubits

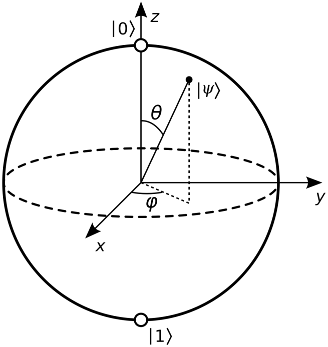

Figure 1: Bloch Sphere

- The building blocks of a quantum computer are qubits (quantum bits :))
  - They can be 0's or 1's or any number in between all at the same time (a quantum superposition of states)
    - Can think about a qubit as a Bloch sphere
  - When measured the qubit collapses to either 0 or 1, but with different probabilities (probabilistic computing versus deterministic computing)

What is a Quantum Computer?

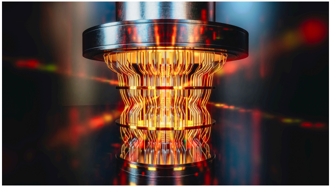

Figure 2: Quantum Computer

- A quantum computer is a collection of qubits and *gates* (which control the states of the qubits without measuring them)

- You “write” quantum computing code by applying quantum gates to certain qubits in a certain order followed by measuring the resulting system
  - You can think of a gate as an operation that rotates the qubit in the Bloch sphere
  - This part will make more sense in the next few weeks
- There are many ways to make a quantum computer

Are Quantum Computers Better than Classical Computers?

- Maybe?
- Quantum computers do have an advantage over classical computers on some types of problems
  - Bits can only be in one state at a time, qubits can be in many states at the same time (this can be exploited!)
- Scalability is currently an issue preventing more large scale calculations

Shor's Algorithm

- What is 3 x 7?
  - This is multiplication, this is easy for a computer to do no matter how large the numbers are
- What two prime numbers can be multiplied together to make 21?
  - This is prime factorization, this is hard for computers to do, especially when the prime factors are large numbers (there are just so many options; large search space)
  - This is one method of modern encryption (common with banks)
- Computational Complexity: To factor an N digit number on a classical computer the scaling will be $2^{N/2}$ (big O notation)
  - This is exponential scaling, which is bad if we want to apply an algorithm to a large number
  - Factoring a 2 digit number will take twice as long as a 1 digit number, factoring a 4 digit number will take four times as a 1 digit number, etc

Shor's Algorithm

- Thirty years ago Peter Shor proposed an algorithm which could run on a quantum computer which makes factoring numbers significantly easier (Shor's algorithm)
    - Shor's algorithm has a quantum computational complexity of log(N) (polynomial scaling)
    - Shor's algorithm is SIGNIFICANTLY faster than the classical versions, factoring a 2 digit number is only 30% longer than a 1 digit number, factoring a 4 digit number is only 60% slower than a 1 digit number
- Shor's algorithm could pose a major hazard to modern encryption schemes but currently quantum computers are too small to handle the size numbers used in encryption (and we are working on making new encryption schemes)

Grover's Search Algorithm

- Another classical algorithm which has significant speed-up on a quantum computer is searching an unordered list
- Grover's algorithm can search an unordered list of N elements on a quantum computer in $\sqrt{N}$ time, the very best classical algorithm can not do better that N
  - Quadratic speed-up (or better!)
- The same limitations that apply to Shor's algorithm also apply here (current quantum computers are small)

What Else Can You Use a Quantum Computer For?

- Quantum Simulation (Richard Feynman)
  - Classical computers can struggle to simulate quantum systems as small as 30 components
  - Why not simulate quantum systems with a quantum system?
- Optimization problems
- Machine Learning and Artificial Intelligence
  - Some machine learning algorithms do have a speed up on a quantum computer!
- Financial modeling
- Climate change and weather forecasting (this is a classically hard problem)
- Cybersecurity

Resources and References

1. The Map of Quantum Computing (Video)
2. If You Don't Understand Quantum Physics, Try This! (Video)
3. What is Quantum Computing? (Article)
4. Why Do Computers Use 1s and 0s? Binary and Transistors Explained. (Video)