Quantum Computing for Normals

Takeaways

- **Quantum computers use qubits instead of standard binary bits.**
    - A bit in a classical computer represents either a 0 or a 1, while a qubit (quantum bit) can represent 0, 1, or both simultaneously, thanks to the concept of superposition. This allows quantum computers to perform complex computations on a massive number of possibilities at the same time.
- **Quantum Environment**
    - Quantum computers require extremely cold, near absolute zero temperatures (like those achieved with dilution refrigerators) because heat and electromagnetic interference can disturb qubits, causing them to lose their quantum state, a process known as decoherence. Even slight disturbances like vibrations or a nearby sound can destabilize the computation.
- **Encryption Threat.**
    - Quantum computers, due to their ability to process huge combinations of data in parallel, can potentially break encryption techniques that are secure today. Current encryption methods like RSA rely on the difficulty of factoring large prime numbers, which quantum computers, using Shor's algorithm, could solve exponentially faster.
    - The US National Security Agency and other government agencies are working on "quantum proof encryption" to defend against this threat.
- **Specialized use cases.**
    - Quantum computers aren't suited for every task. They're specialized for problems where classical computers struggle, like factoring large numbers, simulating quantum systems, or solving optimization problems. They leverage **quantum parallelism** through superposition and **quantum entanglement** to handle multiple possibilities simultaneously.
- **Limitations and Stability**:
    - Despite their potential, quantum computers are still in the experimental phase. They are extremely sensitive to environmental factors, and achieving stable qubits for a long duration (known as **coherence time**) is still a significant challenge. For broader use, we'll need more robust error correction and better isolation from noise.

Understanding Superpositions

[1]Quantum superposition is a fundamental principle in quantum mechanics that describes how quantum systems can exist in multiple possible states at once. The phrase **"two states at the same time"** is often used to describe this, but it's more nuanced than simply being in two physical states simultaneously. Instead, it reflects the fact that, until a measurement is made, we can only describe the system as being in a *combination* (or superposition) of these states.

Superposition Explained: In quantum mechanics, a particle, such as an electron, can exist in a state that is a *superposition* of two or more possible outcomes. For example, in the famous thought experiment **Schrödinger's cat**, the cat is described as being in a superposition of "alive" and "dead" states until someone observes it. In reality, this means that the quantum system (here, the cat) is in an indeterminate or probabilistic state described by a wavefunction.

Mathematically, the wavefunction is a combination (sum) of possible outcomes, each with a certain probability. For example, a quantum system could be in a superposition of states $|A\rangle$ and $|B\rangle$, where we represent this superposition as:

$$|\phi\rangle = c1|A\rangle + c2|B\rangle$$

The coefficients c1 and c2 describe the relative "weights" or probabilities associated with each state.

Not "Physically" in Two States: When people say that a particle is in two states at the same time, we don't mean that it is physically doing two things simultaneously, like being in two places at once. Instead, it's more accurate to say that, *before we measure it*, the system doesn't have a definite state that we can know. It only has a range of potential outcomes, each associated with a probability.

It's like having a coin that is spinning in the air. Until the coin lands and we observe it, it's neither heads nor tails—it's in a superposition of heads and tails. However, in reality, the coin still has one specific side up at any moment; we just don't know which one until we observe it. This is where quantum mechanics diverges: in the quantum case, it's not simply that we *don't know* which state it's in; it doesn't have a defined state until the act of measurement forces it into one.

Measurement "Collapses" the Superposition: In the quantum world, the act of measuring the system forces it to "choose" one of the possible states. This process is known as **wavefunction collapse**. For example, if we measure the position of an electron, it might have been in a superposition of many positions, but after measurement, it collapses to a specific position. Before measurement, the electron isn't in any *one* of these positions—it's in a superposition of all of them.

[1] https://www.youtube.com/watch?v=ZUipVyVOm-Y

Final Remarks

While quantum computers show promise in breaking encryption and performing specific computations much faster than classical computers, they are still in the experimental stage and far from being stable or reliable for everyday use. Overcoming the challenges of decoherence and error correction will be critical in bringing quantum computing into broader applications. In the future, we may access quantum computing through cloud services, but that reality is still some time away.

Glossaryck

Bits vs Qubits:

- **Bit**: A classical binary digit (0 or 1).
- **Qubit**: A quantum bit, which can exist in a **superposition** of 0 and 1 simultaneously.

Superposition:

- Superposition is a key quantum concept where a qubit can exist in a combination of both 0 and 1 states at the same time. Imagine a spinning coin — until you observe it, it's neither heads nor tails but rather an indeterministic mix of both. For qubits, this allows them to store more information than classical bits. The power comes from quantum systems' ability to explore multiple possibilities (both 0 and 1 states) until they are "measured" and collapse into a definitive state.

Entanglement:

- Quantum entanglement is a phenomenon where two or more qubits become linked, such that the state of one instantly determines the state of the other, regardless of the distance between them. If you entangle two qubits, and then observe one qubit, the other qubit's state will instantly be known. This property is key for quantum teleportation and secure communication.

Probability Amptitudes:

- In quantum computing, qubits don't simply exist in 0 and 1 states. Instead, they are described by **probability amplitudes**, which are complex numbers that determine the likelihood of the qubit collapsing into either the 0 or 1 state upon measurement. These amplitudes interfere with each other, which is how quantum computers can perform some calculations much faster than classical computers.

Sources

https://www.youtube.com/watch?v=g_IaVepNDT4&list=WL&index=5
https://www.youtube.com/watch?v=zNzzGgr2mhk
https://www.youtube.com/watch?v=zmL3JGG7ywU&list=LL&index=3&t=3s
https://www.youtube.com/watch?v=-UrdExQW0cs&list=LL&index=3