Quantum Computing: Past, Present, and Future

A look into quantum computing's origins, modern-day real-world applications, and future potential in the scientific community…

Hannah Culver | Honors Tutorial College

Background

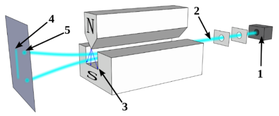
Quantum computing is a combination of quantum physics and computer science. Like how computer science works with bits, the most basic unit of quantum computing is the **qubit**, or quantum bit. [2]

There are three key ideas behind the field of quantum mechanics:

1. **Superposition:** A classical bit can be either 0 or 1, much like an on-off switch, while a qubit can be in one of an infinite number of states, otherwise known as a *superposition* of both 0 and 1. This can be likened to a spectrum between the two, with the state of the qubit falling anywhere in between them at any given time.

2. **Measurement:** The act of *measuring* a qubit yields 0 or 1, however, unlike the classical case, it changes the state of the qubit.

3. **Entanglement:** Qubits can be *entangled*, meaning that measuring one affects the state of the other.



Qubits can be represented in several ways, the most common examples being the **spin** of an electron (Stern-Gerlach apparatus) or the **polarization** of a photon (polarized film).

Stern–Gerlach experiment: Silver atoms traveling through an inhomogeneous magnetic field, and being deflected up or down depending on their spin; (1) furnace, (2) beam of silver atoms, (3) inhomogeneous magnetic field, (4) classically expected result, (5) observed result [11]

Origins & Historical Timeline

The earliest instances of quantum computing can be traced back to the early 80s, though the theory behind the concept of quantum mechanics was heavily debated throughout much of the twentieth century. [7]

1980 – U.S. scientist Paul Benioff proposes a computer that operates under quantum mechanical principles

1981 – physicist Richard Feynman proves it is impossible to simulate quantum systems on a classical computer

1985 – physicist David Deutsch publishes a paper describing the world's first universal quantum computer

1994 – Peter Shor, a mathematician at Bell Labs, proposes a method for factorizing large integers (first demonstrated in 2001 by a group at IBM, **Shor's algorithm** boosted research on new cryptosystems that are secure from quantum computers)

1995 – Christopher Monroe and David Wineland of NIST (National Institute of Standards & Technology) demonstrate the first quantum logic gate, the C-NOT gate

1996 – another Bell researcher, Lov Grover, uses quantum mechanics to solve an old problem: unstructured search (**Grover's algorithm**)

1998 – first experimental demonstration of a quantum algorithm, **Deutsch's problem**, by a quantum computer

2000 – the first working 5-qubit NMR computer is put through its paces at the Technical University of Munich

2006 – scientists at the Institute for Quantum Computing and Perimeter Institute for Theoretical Physics present a new operational standard by controlling a 12-qubit quantum system with only minimal decoherence; Bonn researchers take a step closer to the building of a quantum gate; researchers at the University of Arkansas create molecules of quantum dot pairs; scientists at the University of Camerino develop a theory for entangling macroscopic objects

2007 – the first use of Deutsch's algorithm in a cluster state quantum computer; a company called D-Wave Systems claims to have built the first working 28-qubit quantum computer (demonstrated on November 12, and continued to increase to 128-qubits in 2008, followed by 512 in 2012, 1,152 in 2015, and 2,048 in 2017)

2011 – D-Wave Systems develops quantum annealing; a quantum computer was devised with Von Neumann architecture

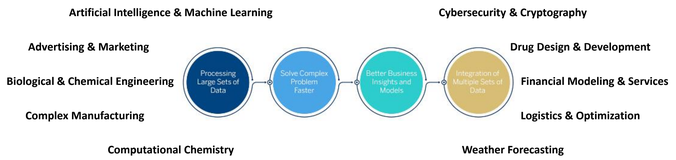
2013 – D-Wave Systems publishes a report comparing the speed of a quantum computer with a high-end PC; the record for avoiding qubit decoherence at room temperature is beaten (the previous two-second record, set in 2012, was smashed by a whopping 39 minutes)

2016 – NIST calls for proposals to standardize quantum-secure cryptographic primitives [5]

Applications

Our world is currently undergoing a technological revolution and has been for quite some time now. With our ever-increasing reliance upon electronic devices, it is no surprise that quantum computing has been utilized as a powerful tool in order to analyze and keep track of the plethora of data being produced daily. Now more than ever, we require quick and precise calculations when organizing, managing, and storing these large amounts of data, and advancements in quantum algorithms and computers have shown promise.

Over the years quantum computing has proven useful in a variety of diverse fields, spanning industries such as insurance, retail, healthcare, agriculture, and gaming. [4]



Of course, quantum computing is not limited to just these broad categories; within each one exists a realm of its own.

Bell's Theorem

Albert Einstein once referred to qubits' ability to interact with one another as "spooky action at a distance". He, along with a handful of other great physicists at the time, such as Erwin Schrödinger, believed that there was no way for qubits to do so without some underlying force, or **hidden variables**, involved. They thought there should be a better model to explain and eliminate the seeming randomness, one that preserved **local realism**, as opposed to the standard *Copenhagen interpretation.*

While it certainly was a mysterious property, many challenged Einstein's proposal. In 1964, Irish physicist **John Stewart Bell** set out to disprove Einstein by devising a test that could distinguish between the two competing models, showing that not only were they just philosophies, but rather testable theories.

Bell's Theorem, or Bell's Inequality, can be thought of as follows: Suppose two separate teams of scientists from different labs are given the task of measuring a pair of entangled electrons. They agree on a set of three possible measurement axes which, when chosen at random, will be used to measure the spin of one electron from each pair. [3]

In the classical case, the labs will obtain opposite results when measuring along different axes at least 33% of the time; equivalently, they will obtain the same result at most 67% of the time.

In the case of quantum mechanics, stronger correlations are exhibited. So long as the three axes are all as far apart as possible (i.e. 120° apart), both labs will obtain the same result 75% of the time, exceeding Bell's upper bound of 67%.

Classical case: possible sets of values for hidden variables (measurement axes labeled A, B, and C)

Bell's result in this experiment is a bit tricky to carry out in practice. There are several loopholes that have yet to be sufficiently closed (distance, too many missing entangled particles, true randomness, etc.), hence the search for a loophole-free bell test. [9]

Future Potential & Discussion

It is impossible to pinpoint exactly where the field of quantum computing will be in 5, 10, or even 20 years' time. Yet predictions have been made as to what we can expect. For instance, it is estimated that "the quantum computing market will reach $2.2 billion, and the number of installed quantum computers will reach around 180 in 2026, with about 45 machines produced in that year" alone. [1]

We are also on the brink of reaching **quantum supremacy**, or the "goal of demonstrating that a programmable quantum device can solve a problem that no classical computer can solve in any feasible amount of time". (*Wikipedia*) In fact, Google and NASA have already done so, achieving this milestone in late October of 2019 after displaying "the ability to compute in seconds what would take even the largest and most advanced supercomputers thousands of years." [8]

Quantum practicality is another feat we soon hope to attain, making quantum computers commercially viable and available to solve real-world problems. [10] Before that can happen, however, we still need to learn how to better handle and maintain qubits, as they are extremely fragile. [6] Any bit of outside noise or interference could disrupt their quantum state, resulting in a loss of information.

Quantum computing has without a doubt made its mark and left a striking impact on the scientific community, and it still has a long way to go given its relative infancy. It is impressive that an area with such widespread implications and possibilities can be beautifully illustrated with linear algebra, and it is even more exciting to see where the field will be taken next.

Polarized Filters Demo

References & Acknowledgements

[1] Banafa, A. (2021, March 15). Quantum Computing and AI: A Transformational Match. OpenMind. Retrieved from https://www.bbvaopenmind.com/en/technology/digitalworld/quantum-computing-and-ai/

[2] Bernhardt, C. (2019). Quantum Computing for Everyone. MIT Press.

[3] Brubaker, B. (2021, August 19). How Bell's theorem proved 'spooky action at a distance' is real. Quanta Magazine. Retrieved from https://www.quantamagazine.org/how-bells-theorem-proved-spooky-action-at-a-distance-is-real-20210720/

[4] Chattopadhyay, T. (2019, November 28). Business Applications of Quantum Computing. Mantra AI. Retrieved from https://mantra.ai/blogs/business-applications-of-quantum-computing/

[5] Chimal-Dzul, H. (2023, March 23). Quasi-cyclic Low-Density Parity-Check Codes of Girth g ≥ 6. Ohio University AMS Graduate Student Chapter.

[6] Giles, M. (2021, October 20). Explainer: What is a quantum computer? MIT Technology Review. Retrieved from https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing

[7] Quantum-Computing 101. (n.d.). Timeline of Quantum Computers and The History of Quantum Computing. Retrieved from http://quantumly.com/timeline-of-quantum-computing-history-of-quantum-computers-dates.html

[8] Tavares, F. (2019, October 23). Google and NASA Achieve Quantum Supremacy. NASA. Retrieved from https://www.nasa.gov/feature/ames/quantum-supremacy

[9] TU Delft. (2015). Tu Delft – A loophole-free Bell test. YouTube. Retrieved from https://www.youtube.com/watch?v=AE8MaQJkRcg&list=PLffnjQLIqxmB5jpTQQfE5DzQHqGCeeUaa&index=3&t=63s.

[10] Viswanathan, S. (2023, January 23). The future of quantum computing and paving the pathway for 'quantum practicality'. IndiaTimes. Retrieved from https://www.indiatimes.com/technology/news/the-future-of-quantum-computing-591033.html#:~:text=Quantum%20computers%20have%20been%20decades,sector%20for%20research%20and%20development

[11] Wikimedia Foundation. (2023, January 29). Stern–Gerlach Experiment. Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Stern%E2%80%93Gerlach_experiment

I would like to give a special thanks to my tutor, Dr. Lopez, for encouraging me to construct this research poster and for picking such a fascinating topic for our tutorial! From here I plan to continue studying post-quantum cryptography for my thesis project next year! :)