History and Progression of Quantum Computing

Early in 1982, Richard Feynman observed that certain quantum mechanical effects could not be simulated on a traditional computer. This lead to research and progression into more efficient and effective ways of computing[6]. From this, the thought of using said quantum mechanical effects to compute and execute programs was developed, branching away from traditional computing methods[6]. Despite this, it wasn't until 1994 when Peter Shor developed a quantum algorithm for factorising integers into its primes, that interest into the field began to grow. This was due to the fact that a quantum computer would be able to compute the answer exponentially quicker than a conventional computer[7].

Conventional and quantum computers differ most significantly in the way in which they encode data. The base concept of a quantum computer is that, unlike a traditional computer that uses bits, it uses qubits. While a bit can be in one of two different states (1 or 0), a qubit can be encoded as both states simultaneously (1 and 0)[6] due to the superposition quality of quantum particles. It is not until the qubit is observed, or manipulated in some way, that its state is defined[2][6]. Therefore, this enables a quantum computer to be many times faster and more efficient at calculating results than a conventional computer, as you can essentially calculate multiple values simultaneously[6]. For example, searching an unordered list on a conventional computer has time complexity O(n), while on a quantum computer the same task has time complexity O(√n)[6][7], making them exponentially faster.

Clearly this benefit of quantum computers is highly desirable when computing large amounts of data, or manipulating large data structures. Due to this, David DiVincenzo outlined five minimal requirements for creating such a machine, which he believes will ensure that such a machine can fulfil its potential[3]. These include; being able to scale qubit arrays, the ability to initialise qubits to an initial state, and having a universal set of quantum gates[3][5].

Recently, quantum computers have started to emerge, with companies such as Google, IBM, and D-Wave all making use of them. Notably, IBM has allowed anyone who signs up access to their quantum computer via the cloud[4], enabling people all around the world to experience their machine, and also try out their own algorithms. Additionally, D-Wave announced in January 2017, that they are releasing a 2000 qubit quantum computer, the 2000Q[1], which has twice as many qubits as the previous most powerful quantum computer. This allows the 2000Q to perform computational tasks up to 10,000 times quicker than a conventional supercomputer[1], hinting already at how useful quantum computers will be in the future when the number of qubits is at the level of todays supercomputer's bit count.

Algorithms and mathematical modelling aren't the only tasks that quantum computers are useful for. Their use in cryptography could prove vital to ensure data is kept private for years to come[1]. Due to the nature of quantum particles, once it is measured its state changes. This makes it very easy to see if someone has tried to eavesdrop on the communication when exchanging encryption keys[6]. This versatility in the way that they can be used ensures the future of quantum computers in all aspects of our lives.

Bibliography

[1] Burnaby, B., 2017. *D-Wave Announces D-Wave 2000Q Quantum Computer and First System Order.* [Online]
Available at: https://www.dwavesys.com/press-releases/d-wave%C2%A0announces%C2%A0d-wave-2000q-quantum-computer-and-first-system-order
[Accessed 30 November 2017].

[2] DiVincenzo, D. P., 1995. Quantum Computation. *Science,* 270(5234), pp. 255-261.

[3] DiVincenzo, D. P., 2008. *The Physical Implementation of Quantum Computation,* New York: IBM T.J. Watson Research Center.

[4] IBM, 2016. *Applications of Quantum Computing.* [Online]
Available at: https://www.research.ibm.com/ibm-q/learn/quantum-computing-applications/
[Accessed 30 November 2017].

[5] IBM, 2016. *What is IBM Q? A Short History of Quantum Computing.* [Online]
Available at: https://www.research.ibm.com/ibm-q/learn/what-is-ibm-q/
[Accessed 2 12 2017].

[6] Rieffel, E. & Polak, W., 2000. An Introduction to Quantum Computing for Non-Physicists. *ACM Computing Surveys,* 32(3), pp. 300-335.

[7] Shor, P. W., 1999. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review,* 41(2), pp. 303-332.