Quantum Computing
A Second Year Vacation Essay

Student ID: 8926382
School of Physics and Astronomy
The University of Manchester

September 28, 2015

1 Introduction

Computation has come a long way since pioneers, such as Charles Babbage and Alan Turing, laid the theoretical foundations of what a computer is. Once abstract concepts of memory and algorithms now underpin almost all of modern life, from banking to entertainment. Following Moore's law, computer processing power has rapidly improved in the past 50 years. This is due to the number of transistors on a semi conductor chip doubling every two years. As these semi conductor chips get smaller and smaller, nowadays approaching atomic dimensions of a few nanometres, tunnelling and other quantum effects will start to disrupt the chip. Many people predict the breakdown of Moore's law in the not too distant future. [1]

It took the genius of Richard Feynman to suggest, back in 1981, that perhaps these quantum effects could instead of being a hindrance, be used to usher in a new type of computer, the quantum computer. Feynman's original suggestion was to use this new computer to probe and study quantum mechanics further. To perform simulations that classical computers would never be able to complete in a feasible time frame. [2]

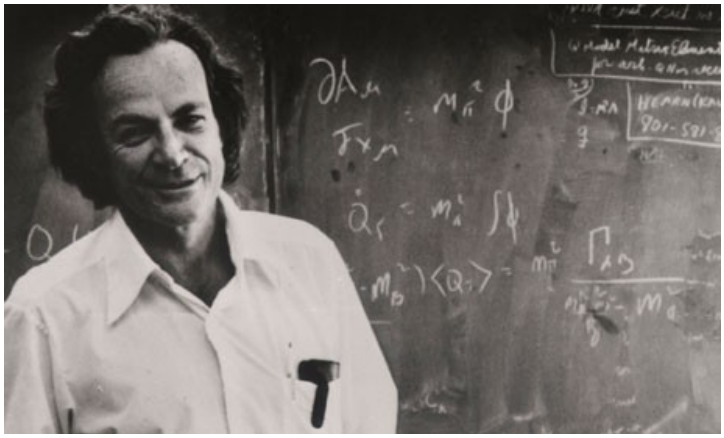

Figure 1: Richard Feynman, a theoretical physicist and a key contributor towards the start of quantum computing. [13]

However, interest in the field has since expanded to include not just theoretical physicists but computer scientists, the security services and even the general public. This increased amount of research has lead to key advancements. Indeed in the last decade working quantum computers have been built, although short on practicality: they require extremely cold temperatures, only contain a handful of quantum bits and can only contain a calculation for a very short time.

2 What is a qubit?

In a classical computer the basic unit of information is a bit, taking the value of either 0 or 1. This is usually physically represented by a high or low voltage. Different combinations of 1's and 0's are taken as codes for letters, numbers etc. and operations on the 1's and 0's allow calculations to be performed.

The basic unit of information in a quantum computer is a quantum bit or a qubit for short. The qubit is not just a 0 or a 1, it is a linear superposition of the two states. Therefore, the general state of a single qubit is given by[1],

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

where a and b are probability amplitudes for the states 0 and 1 respectively. Physically, a qubit can be represented by any two-state quantum mechanical system, such as: the polarisation of a photon, the alignment of nuclear spin in a uniform magnetic field and the two states of an electron orbiting an atom. [3]

When a qubit is measured the wave function will collapse down to one of the basis states and the superposition will be lost. The probability of measuring a 0 or a 1 is given by,

$$P(|0\rangle) = |a|^2 \quad \text{and} \quad P(|1\rangle) = |b|^2$$

respectively [4]. It can be seen then that the maximum information that can be extracted from a qubit by measurement is the same as a classical bit, either a 0 or a 1. So, what is different about quantum computing?

3 The power of quantum

The superior power of a quantum computer becomes apparent when you consider multiple qubits. A classical 2 bit computer's state is described very simply by two numbers. In total, there are four possible states, {00,01,10,11}. This is the set of basis states for a 2 qubit quantum computer, the general state given by,

$$|\psi_2\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \quad .$$

Four states are in superposition and four amplitudes accompany them. This means that four numbers are required to fully describe the state of a 2 qubit system.

In general, an *n* qubit system has *N* basis states and amplitudes, where

$$N = 2^n \quad .$$

Therefore, the amount of numbers being stored by the system increases exponentially. Indeed, a system of 500 qubits would require a number larger than the estimated amount of atoms in the universe to describe it's state [3]. Even better, is the fact that performing an operation on the state, performs it on all the numbers simultaneously. This quantum parallelism allows certain types of calculation to be performed significantly quicker on a quantum computer. [5]

---

1 The bra-ket notation is commonly used for describing quantum computation. A ket is simply a vector, as an example the vector, $\underline{v} = x\hat{i} + 0\hat{y} + z\hat{k}$,could be expressed in ket notation as, $|v\rangle = x|i\rangle + z|k\rangle$.

However, simply plugging classical algorithms into a quantum computer won't see any benefit, infact it could run slower. Also, the calculation may be performed on infinitely many numbers but these values are all hidden to us and through direct measurement of *n* qubits we would only get a string of *n* 1's and 0's. A new way of thinking is required to design special types of algorithms that make the most of a quantum computer's power.

4 Shor's algorithm

The standard example for a quantum algorithm and one of the most important is Shor's algorithm, discovered in 1994 by Peter Shor [3]. The algorithm took advantage of quantum computing to solve the problem of finding the two prime factors of an integer. This problem is of great importance, as most security systems are based on RSA encryption, which relies on a number being the product of two large prime numbers. Shor's algorithm can factor a large number in polynomial time[2], whereas a classical computer has no known efficient algorithm to factor large numbers [4]. If a person had a quantum computer with enough qubits, they could use Shor's algorithm to break into online banks, access other people's emails and access countless amounts of other private data. This security risk is what really got governments and security services interested in funding quantum computing research.

How does the algorithm work? The algorithm makes use of a mathematical trick discovered by Leonhard Euler in the 1760's. Let *N* be the product of the two primes *p* and *q*. The sequence,

$$x \bmod N\,,\, x^2 \bmod N\,,\, x^3 \bmod N\,,\, \ldots \quad [3]$$

will repeat with a period that evenly divides *(p-1)(q-1)* provided *x* isn't divisible by *p* or *q*. A quantum computer can be used to create a superposition over the aforementioned sequence. A quantum Fourier transform is then performed on the superposition to find the period. These are the key steps that can be implemented on a quantum computer but not on a classical one. Repeating this with random values of *x* allows *(p-1)(q-1)* to be found and from this the values of *p* and *q* can be discovered. [6]

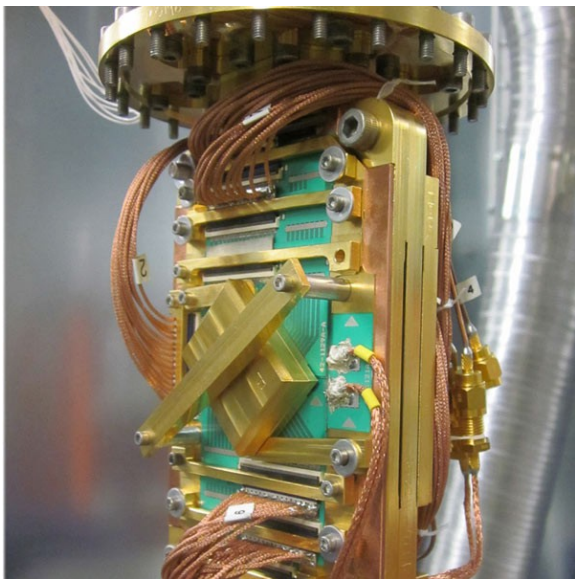

Figure 2: A D-Wave computer, the first commercial quantum computer. [14]

2 In computing, when considering a problem of size *n*, the solution is considered efficient if it is solved in $O(n^x)$ steps, called polynomial time. It is considered inefficient if solved in $O(x^n)$ steps, called exponential time.

3 The modulo operation, a mod b, gives the remainder of a divided by b. For example, 9 mod 3 is 0 but 11 mod 3 is 2.

Shor's algorithm has been experimentally validated on prototype quantum computers and has been demonstrated to factor small numbers. On a photon based computer in 2009, fifteen was factored into five and three [7]. It is important to note that Shor's algorithm is not the only other useful quantum algorithm. Grover's algorithm allows for faster searching. Specifically, when searching a space of 2^n possible solutions for the correct one. Classically, this will take on average $2^n/2$ queries but Grover's algorithm can do it in $2^{n/2}$ queries (the optimal amount) [4]. This speed up is something that peaked Google's interest in quantum computing as the future for their search technology. The technology giant has already bought a D-Wave quantum computer, they're performing their own research and looking at building a quantum computer [8].

5 Cryptography

Quantum computers will break the currently used security systems, however quantum mechanics can be used to introduce a new type of security that has been proven to be unbreakable. Unlike a classical state, an unknown quantum state cannot be cloned. This is stated in the no-cloning theorem. Indeed this principle formed the basis of quantum money proposed by Stephen Wiesner. A form of money, secured with unknown quantum states of photon polarisation (where the basis states of 0 or 1 would be horizontal or vertical polarisation etc.). Fraudsters wouldn't be able to copy the money to create counterfeit notes and only people who knew the states could produce and verify the notes. [4]

The fundamental quantum property of decoherence imposes the largest barrier on infiltrating a communications channel. Supposing someone was trying to listen in, the act of them measuring the state would cause it to decohere and change. Checks between the parties communicating would then allow the receiver to notice the state has been tampered with and knowledge that someone is trying to intercept the messages. Combined with the inability to make a copy, these quantum principles form a solid foundation for strong quantum based cryptography.

The main example of quantum cryptography is quantum key distribution. Here the sender sends a stream of individual photons using a laser and randomly chooses the basis states (horizontal/vertical or 45 degrees from an axis) and assignment of 0 and 1 to the basis states for each photon sent. The receiver randomly chooses a mode and assignment when measuring the photons. A classical channel is then used by the sender to send the receiver the detail of which modes were used for each photon**.** The receiver then ignores any values he measured in the wrong mode. The correctly measured values then make up the encryption key. Potential interceptors will take the photons and measure them but will be unable to clone them. A stream of guessed photons will then be sent to the receiver. Measuring a sample of the photons will allow any statistical difference from the intended signal to be noticed and the key is discarded. This creates a key that is almost impossible to steal. While still early in being implemented a key has been exchanged over 730m of free space at a rate of almost 1Mb/s using an infrared laser. [9]

6 Technical details

As qubits can be represented by any two-state quantum systems there are many different options for building a quantum computer. The biggest problem with building any quantum computer is decoherence, the qubits need to interact with each other and quantum logic gates but not the surrounding environment. If the environment was to interact with the qubits, effectively measuring them, the superposition would be lost and calculations would be erroneous and fail. Quantum computing is extremely fragile. Factors such as heat and stray electromagnetic radiation

that would leave classical computers unaffected can disturb the simplest quantum calculation.

One of the candidates for quantum computing is the use of photons and optical phenomena. The basis states can be represented by orthogonal polarisation directions or by the presence of a photon in on of two cavities. Decoherence can be minimised by the fact photons don't interact strongly with matter. The photons can also easily be prepared by a laser in the initial states, guided around a circuit by optical fibres or wave guides and measured by photomultiplier tubes.

An ion trap can also be used for quantum computing. Here atoms are trapped by the use of electromagnetic fields and subsequently cooled to a very low temperature. This cooling allows the energy difference in spin to be observed and spin can be used as the basis states of the qubit. Incident light on the atom can then cause transitions between spin states, making calculations possible. In March 2011, 14 trapped ions were entangled as qubits [10].

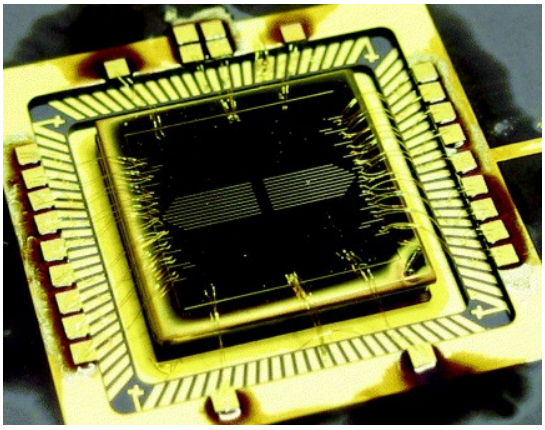

Figure 3: An ion trap, potentially part of a future quantum computer. [15]

The field of nuclear magnetic resonance (NMR) is also being explored as a potential physical basis for quantum computing and provides the most well known concepts. Here an ensemble of molecules are contained and spins are measured and manipulated using radio frequency electromagnetic waves. [3]

7 Conclusion

The quantum computer has moved beyond the realm of mere theoretical fancy into a real object that is currently being fine tuned by researchers. Large amounts of research and understanding has been gained on the theoretical underpinnings of quantum computation, a field now 30 years old. Large leaps in coherence times, temperature conditions and the number of qubits stored will need to be made before the quantum computer becomes widespread. Impressive steps are being taken though, such as qubits being stored at room temperature for 39 minutes [11]. The quantum computer will definitely be built in our lifetime.

A handful of quantum algorithms have been designed and the potential power is starting to be unlocked. Real life applications have been demonstrated in security and searching, as well as future applications in drug design, cancer diagnosis, safer aeroplane design and analysis of complex weather patterns [12]. It should be noted that it will probably not revolutionise home computing, like the silicon chip did, with the classical computer remaining quicker for some tasks. It will revolutionise the specialist task of simulation of quantum systems, allowing larger tests of quantum properties and furthering our understanding of quantum mechanics. However, this comes with the price of potentially redefining our concept of what proof is and handing over trust to the computer.

For the calculations being performed on the multitude of hidden numbers cannot be tracked by any human or classical machine and the proof will simply boil down to inputting initial conditions, waiting for the computers output and accepting what it gives without meticulous checking of each line of calculation.

Maybe the deepest implication of quantum computing is the simulation of AI. The new found power and large number storage of quantum computers could assist in more complicated simulations of humans. It has even been suggested, by the theoretical physicist Roger Penrose, that the brain is a quantum computer. Although it is hard to understand how superpositions could survive decoherence in the wet, hot and generally messy environment of the brain. Genius mathematician, Carl Friedrich Gauss, was said to be able to factor large numbers in his head. A special case or is it proof of the brain solving a problem only efficiently solvable on a quantum computer. Would a large, working quantum computer eventually be able to simulate human conciousness? [3]

References

[1] D. Takahashi, **Forty years of Moore's law**, The Seattle Times (April 2005), Accessed on 15/09/2015, URL: http://www.seattletimes.com

[2] R. Feynman, **Simulating Physics with Computers**, International Journal of Theoretical Physics (May 1981), Accessed on 15/09/2015, URL: http://www.cs.berkeley.edu/~christos/classics/Feynman.pdf

[3] M. Nielsen and I. Chuang, **Quantum Computation and Quantum Information**, Cambridge University Press (December 2010)

[4] S. Aaronson, **Quantum Computing Since Democritus**, Cambridge University Press (March 2013)

[5] S. Bone, **The Hitchiker's Guide to Quantum Computing**, Accessed on 16/09/2015, URL: http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol1/spb3/

[6] S. Aaronson, **Shor, I'll do it**, (February 2007), Accessed on 18/09/2015, URL: http://www.scottaaronson.com/blog/?p=208

[7] **Quantum computer slips onto chips**, BBC News, Accessed on 27/09/2015, URL: http://news.bbc.co.uk/1/hi/sci/tech/8236943.stm

[8] N. Jones, **Google and NASA snap up quantum computer**, Nature (May 2013), Accessed on 27/09/2015, URL: http://www.nature.com/news/google-and-nasa-snap-up-quantum-computer-1.12999

[9] J. Ouellette, **Quantum Key Distribution**, The Industrial Physicist (December 2004)

[10] **Calculations with 14 Quantum Bits**, University of Innsbruck (May 2011), Accessed on 28/09/2015, URL: http://www.uibk.ac.at/ipoint/news/2011/mit-14-quantenbits-rechnen.html.en

[11] J. Kastrenakes, **Researchers smash through quantum computer storage record**, The Verge (November 2013), Accessed on 28/09/2015, URL: http://www.theverge.com/2013/11/14/5104668/qubits-stored-for-39-minutes-quantum-computer-new-record

[12] M. Vella, **9 Ways Quantum Computing Will Change Everything**, Time (February 2014), Accessed on 28/09/2015, URL: http://time.com/5035/9-ways-quantum-computing-will-change-everything/

[13] **Figure 1 –** Richard Feynman, Image source: http://www.theguardian.com

[14] **Figure 2 –** D-Wave quantum computer, Image source: http://www.dwavesys.com

[15] **Figure 3 –** Ion trap, Image source: http://iopscience.iop.org

Number of words (excluding references): 2301