An Introduction to Quantum Computing

By Jonathan Arnold

20 January 2009

In this essay I intend to give a review of the rapidly advancing field of Quantum Computing. The theory and motivation behind these developments will be outlined, together with the problems faced in its implementation and some of the methods currently being developed to realise quantum computing.

The Origins of Quantum Computing

Over the past 30 years the introduction of the silicon chip and transistors has transformed the world into a technological one; personal computers, mobile devices and other electronics have massively improved the processing power available to the public. Electronics manufacturers strive to reduce the size and increase the computing power of their devices; Moore's Law, a fundamental law in electronics, says that the number of transistors (the essential building blocks of integrated electronics) that can be placed on an integrated circuit doubles every two years[1].

Despite the fast pace of conventional computers, there are still a number of problems which cannot be solved particularly quickly, such as factorising large integers. It is anticipated that – unless a particularly clever algorithm is devised – this problem is a fundamental deficiency in conventional computing. Because of this, the search for new computational technologies has been around for as long as computing has.

Quantum computing was an idea first popularised by famous physicist Richard Feynman in the 1950s. He proposed that large computational advantages lie in quantum theory, but it took Peter Shor to show scientifically that the quantum computer would trump conventional computing with his quantum algorithm for factoring integers[2] (see *The Future of Quantum Computing*). Since then significant research has been applied to building a reliable quantum computer.

Quantum Mechanics and Qubits

Quantum mechanics, like electronics, has been a science that has undergone great development during the 20th Century. In essence, it outlines a method of statistical mathematics that models the behaviour of electrons and other subatomic particles. Although not an entirely complete theory (many questions are still being asked in relation to the metaphysics of quantum mechanics), the predictions it makes are significantly accurate – as such, it has been a widely accepted theory by the physics community.

One of the most interesting features of quantum mechanics is that the behaviour of a particle is not deterministic; a set of similarly prepared quantum mechanical systems will exhibit a number of different behaviours, rather than just one. This is due to the system not being in a single state, but a *superposition* of states; however, if the system is observed then the system 'collapses' into a single state. Famously this behaviour was the basis of Schroedinger's Cat[3], and is especially advantageous in quantum computing.

Most computers store and manipulate a sequence of *bits*, which are either on or off (usually represented by 1 and 0 respectively). *Qubits* are the quantum mechanical equivalent to bits. They perform the same duty as bits, but due to their quantum mechanical nature their state can be a superposition of 1 and 0. Using bra-ket notation to abstract from a specific wavefunction, the state of a two-state qubit Ψ can be written as

$$|\Psi\rangle = \alpha|1\rangle + \beta|0\rangle$$

where α and β are (complex) coefficients, often named *probability amplitudes,* as the square of each gives the probability of their respective state. This property is advantageous to quantum computing, as demonstrated in the following example: consider a two-qubit quantum computer with qubits B_0 and B_1, with

$|B_0\rangle = |1\rangle$ and $|B_1\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle)$ (i.e. B_1 has equal chance of being in state 1 or state 0).

By superimposing the two bits then

$$|B_0 B_1\rangle = \begin{Bmatrix} |10\rangle & \text{(decimal 2)} \\ |11\rangle & \text{(decimal 3)} \end{Bmatrix}$$

with equal probability. If we were to perform an operation on this system, then the result would be the equivalent of performing an operation on $|10\rangle$ and $|11\rangle$. This implies that operations can be performed on 2^n states simultaneously. Obviously this gives huge performance increases over current computing, but does not come without its problems (see *Implementing the Quantum Computer*).

Superposition also allows quantum cryptography to be possible: since the wavefunction of a particle collapses as it is observed, if a message is sent with particles in a superposition of states then a message cannot be intercepted without the host computer knowing (as the interception would cause the wavefunction of both particles to collapse).

Superposition is not the only quantum phenomenon advantageous to quantum computing (since theoretically this could be achieved with a three-state electronic system); entanglement is a phenomena exclusive to the world of quantum mechanics. It arises when two particles (often created at the same time) exhibit correlations in their properties – so much so, in fact, that one cannot describe the state of one of the entangled particles without consideration of its counterpart. For instance, two photons produced by firing a high-power laser at a transparent crystal lattice are entangled[4], and will have equal polarisation. Similarly, two electrons produced at the same time will have opposing spin.

It's not immediately obvious how entanglement is beneficial to quantum computing, but the phenomenon brings with it some interesting properties. Because this correlation is kept no matter how far apart the two entangled particles are, quantum teleportation is possible (and has been shown[5]), meaning that qubits (or more specifically their states) can be 'teleported' across to different areas of the quantum computer very quickly and efficiently.

Computing With Qubits

In order to compute, operations have to be performed on bits/qubits. This is achieved using *logic gates.* In conventional electronics, a number of logic gates exist, such as AND, OR and NOT. However, it can be shown that every possible logical operation can be performed using a combination of NAND gates[6]; this means that the NAND gate is (on its own) the *universal set* of gates for conventional electronics*.

Quantum logic gates have additional restrictions to conventional logic gates. For instance, the gate has to be *reversible*, otherwise information will be lost and the system will decohere (see *Implementing the Quantum Computer* for a more detailed explanation of decoherence). Because of this, a 'quantum NAND gate' would not be useful (as it is not reversible); instead, a new set of gates is required.

For 2-bit logic, a universal set of quantum gates can be found, in the form of the *Hadamard gate,* the *phase rotation gate* and the *controlled NOT gate*[7]. The Hadamard gate performs operations on a single qubit as represented by the Hadamard matrix

$$\mathrm{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

which splits a single state into a superposition of two states, and vice versa. (i.e. $\mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$,

* There are a number of universal sets of gates, as any set that can map out all logic operations is a universal set. The NAND gate is the smallest such set for 2-bit processing.

etc.). The set of phase rotation gates operate on a single qubit and is given by the operator

$$R(\theta)=\begin{pmatrix}1 & 0\\ 0 & e^{2\pi i\theta}\end{pmatrix}$$, where θ is the phase shift.

For the universal set of gates, only one phase rotation gate is needed, $R\left(\arccos\frac{3}{5}\right)$. The controlled NOT gate takes two qubits as input and is defined by the operator

$$CNOT=\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}.$$

Using H, $R\left(\arccos\frac{3}{5}\right)$ and CNOT, all 2-bit operations can be performed on qubits. A quantum computer with gates like this is defined as a *universal quantum computer,* but at the time of writing no such computer has been built.

Implementing the Quantum Computer

Although the fundamental theory of quantum computing is universal, the ideal implementation for a quantum computer is still undecided, and research is currently concerned with developing a number of these implementations to find the limits of each.

Ion trapping is one of the most promising quantum computer implementations currently being researched. Ions (or more specifically their electrons) store the qubit information, and lasers are used to entangle ions together. They are then trapped in a strong electromagnetic field. Ion trapping is one of the most promising methods as it holds the record for the largest number of entangled particles (8 calcium ions, set in 2005[8]). Developments show that, using a series of ion traps, ions can be moved from one trap to another[9], meaning that different traps can be specialised as different quantum gates if required.

The quantum nature of superposition is one of the fundamental advantages of quantum computing over conventional computing. However, the process of taking a measurement in quantum mechanics removes this superposition, and the particle collapses to a certain, definite state. This is known as the collapse of the wavefunction (in reference to the mathematical object used to describe the state of the system), and is obviously not ideal in quantum computers as superposition is no longer present. More currently, this problem has been termed decoherence. Because of this, steps have to be taken to avoid 'measuring' the system during calculation, where the meaning of 'measurement' here is anything that will give details about a quantum mechanical system to its environment, such as heat transfer. Obviously one of the simplest ways to avoid heat noise would be to supercool the atoms to extremely low temperatures – this does work, but is impractical if quantum computers are going to become widespread. A number of quantum computing methods are still functional at room temperature, such as NMR quantum computing (which uses the spin state of an entire molecule as a qubit, and performs operations based on applying large magnetic fields, as in traditional NMR).

Despite measures taken to avoid decoherence, it is inevitable that some qubits will decohere, so some error correction is still required. Quantum error correction is a tricky business, however, as any measurement of the quantum system will cause it to decohere and the data will be lost. There are two major types of error in quantum computing: bit flip errors, where a bit changes from 1 to 0 (and vice versa), and phase shift errors, where the probability density of measuring either state is altered. A number of algorithms have been designed to correct these errors, the most famous of which being Shor's code. Shor's code diagnoses and corrects both bit flip and phase shift errors, but requires 9 qubits to correct errors in a single qubit[10]. Recent developments have reduced this to 5[11], together with a proof stating that this is the limit[12].

The Future of Quantum Computing

Quantum computing cannot be thought of as an 'upgrade' to conventional computing; most algorithms that worked in conventional computing will not work in quantum computing without modification, as has been shown. As a result, much of the power of quantum computing has not yet been realised, as the algorithms have not yet been deduced. Quantum computing has, however, already produced some impressive results: an algorithm devised by Peter Shor shows that a quantum computer can factorise integers faster than any conventional computer[2] (specifically, for an integer N it takes time to the order of $(\log N)^3$ to factorise it on a quantum computer, compared to $\exp\left((\log N)^{1/3}(\log\log N)^{2/3}\right)$ for conventional computers).

It is interesting to note that a conventional computer has the ability to simulate a quantum computer. However, since a significant amount of computing power is required to maintain correlations among qubits, the conventional computer does not provide the increase in computing power possible from quantum computers. Not only this, but the complexity of keeping track of qubits increases significantly with each qubit added. It would be easier and more practical to build a quantum computer, as it would reap the advantages of the quantum computing theory discussed above.

As mentioned before, quantum computing has a number of hurdles to overcome before becoming a feasible computing technology, and is as such a subject is still in its infancy. Currently, research is focussing on increasing the number of entangled qubits and improvements to manipulating them, the development of quantum gates and techniques of reducing decoherence.

As a subject that has only been around for the last 30-or-so years, the potential for quantum computing is still great, and I believe it is only a matter of time before the technological and theoretical barriers are overcome and a fully functioning universal quantum computer is demonstrated.

Acknowledgements

- Many thanks to Dr. Andrew Brinkman and Dr. Matthew Jones of Durham University Physics Department for their time and guidance.

Bibliography

[1] G. E. Moore, *Cramming More Components onto Integrated Circuits*, Electronics, **38**, 8 (1965)

[2] P. W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, Proceedings of the 35th Annual Symposium on Foundations of Computer Science (1994)

[3] J. D. Trimmer, *The Present Situation in Quantum Mechanics: A Translation of Schroedinger's 'Cat Paradox' Paper*, Proceedings of the American Philosophical Society, **124**, 5 (1980)

[4] A. D. Aczel, *Entanglement*, Wiley (2003)

[5] D. Bouwmeester et al., *Experimental Quantum Teleportation*, Nature, **390**, p. 575-579 (1997)

[6] C. Pierce, *A Boolean Algebra with One Constant* [1880], reprinted in *Collected Papers of Charles Sanders Peirce [Vol. IV],* Harvard University Press, p. 12-20

[7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000)

[8] H. Haffner et al, *Scalable Multiparticle Entanglement of Trapped Ions*, Nature, **438**, p. 643-646 (2005)

[9] F. Schmidt-Kaler et al., *How to Realize a Universal Quantum Gate with Trapped Ions*, App. Phys. B, **77**, p. 789-796 (2003)

[10] P. W. Shor, *Scheme for Reducing Decoherence in Quantum Computer Memory*, Phys. Rev. A, **52**, 4 (1995)

[11] R. Laflamme, C. Miguel, J. P. Paz, W. H. Zurek, *Perfect Quantum Error Correction Code*, Phys. Rev. Lett., **77**, (1996)

[12] A. R. Calderbank, P. W. Shor, *Good Quantum Error Correcting Codes Exist*, Phys. Rev. A, **54**, p. 1098-1105 (1996)