# QUANTUM COMPUTERS AND THE CLUSTER STATE

In quantum mechanics, the world is studied from a microscopic perspective, presenting a rather strange view indeed. The field has revolutionised understanding of the universe, but now the next step is within reach: applying its peculiarities to develop new technologies. Transistor-based computers have operated for decades using semiconductor physics derived from quantum mechanics, but recently interest has turned to employing quantum mechanical phenomena, like state superposition and entanglement, to perform quantum computation. First proposed by Manin and Feynman[1] in the early 1980s, the past two decades have seen much advancement in the theoretical development and physical implementation of quantum computers. Furthermore, one-way quantum computers based on cluster state substrates present a promising potential for a single universal quantum computer.

## QUBITS

The fundamental difference between quantum and classical computers is that rather than the basic unit of information being the bit, the memory consists of its quantum analogue: the qubit[2]. A qubit can be formed by any two-state quantum system in which the measured state is independent of time: a stationary state. This allows, for example, using the polarisation state of a photon or the spin state of a nucleus. Whereas a classical bit has binary states 0 or 1, the qubit additionally has the superposition state of 0 and 1 available to it. This means that a system of n qubits can simultaneously be in a superposition of $2^n$ states, compared to the classical system of n bits with n simultaneous states.

The possible measurement outcomes $|0\rangle$ and $|1\rangle$ form the computational basis states. The Bloch sphere model[2] (Figure 1) provides a geometric representation of a qubit with superposition state $|\psi\rangle$. Measurement gives the definite state of the projection of $|\psi\rangle$ onto the axis of measurement, which is an arbitrary choice here. Thus, the polar angle θ reflects the probabilities for the two measurement outcomes (related because $|\psi\rangle$ is normalised) and the azimuthal angle ϕ records the phase difference between the two states, which must be included as state coefficients can be complex. Whether qubits are in superposition or definite states is dependent on the orientation of the measurement basis: choosing a measurement axis in Figure 1 parallel to $|\psi\rangle$ results in a definite state outcome, while measuring in the $\hat{\boldsymbol{z}}$ direction gives a superposition state.

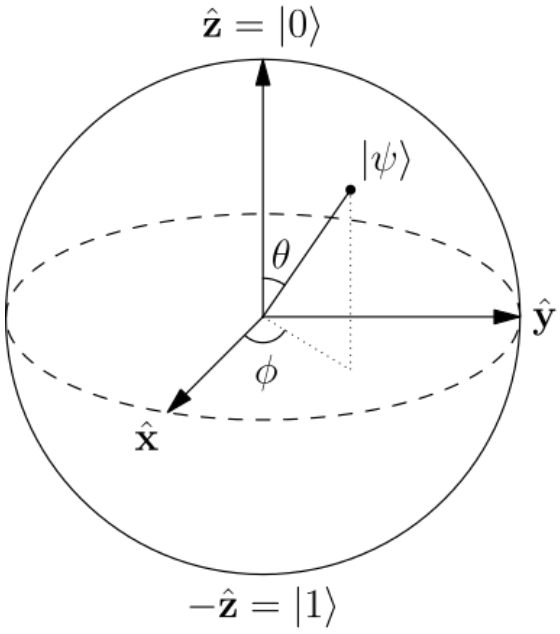


**FIGURE 1**
**THE BLOCH SPHERE, NAMED AFTER THE PHYSICIST FELIX BLOCH, GEOMETRICALLY VISUALISES THE STATE SPACE OF A QUBIT.**

## QUANTUM CIRCUIT MODEL

The quantum computation process can be constructed in an abstract sense using the quantum logic circuit model[3], also called the quantum circuit or quantum gate array model. This is the most commonly used model[3], so will be regarded as the standard model. Horizontal lines in a quantum circuit (Figure 2) represent qubits and are called quantum wires; traversing the wire from left to right shows the qubit's passage through time (independent of the qubit's spatial movement). Qubits begin in a known state and are manipulated through a series of quantum logic gates: one-qubit gates are represented by squares over a wire, and two-qubit gates by circles and a vertical line starting

at and terminating with the involved qubits. The operation performed by the gate sequence builds the desired algorithm. The calculation is completed with a measurement, represented by the meter terminating the top wire in Figure 2, providing a probabilistic solution with known probability.

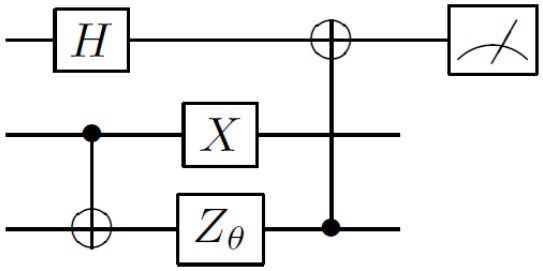


**FIGURE 2**
**A QUANTUM CIRCUIT SHOWING THE MANIPULATION OF THREE QUBITS THROUGH SEVERAL QUANTUM GATES, TERMINATING WITH A MEASUREMENT. NOTE THE RIGHT-MOST CONTROLLED-NOT GATE DOES NOT INTERACT WITH THE MIDDLE WIRE.**

One-qubit gates represent unitary operations that either transform the qubit's state by changing the orientation of the basis, effectively rotating the Bloch sphere, or by shifting the state's phase. These transformations are reversible, so no information is lost, and can be represented by square matrices which act on a column vector representing the input state of the qubit. The state $|0\rangle$ is represented by the column vector:

$$\begin{pmatrix}1\\0\end{pmatrix}$$

While the state $|1\rangle$ corresponds to:

$$\begin{pmatrix}0\\1\end{pmatrix}$$

A common one-qubit quantum logic gate is the Hadamard gate (the top-left gate in Figure 2) which performs a rotation of $\pi$ radians about the axis $(\hat{\boldsymbol{x}} + \hat{\boldsymbol{z}})/\sqrt{2}$ and can be expressed as the matrix[3]:

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$$

A common two-qubit gate is the controlled-NOT gate. Considering its appearance on the bottom-left of Figure 2, the bottom qubit is the target qubit, indicated by the circular outline, while the upper qubit is the control qubit, designated by the filled circle. The line between them represents the transfer of information. The state of the target qubit is flipped if the state of the control qubit is set to $|1\rangle$, otherwise it is unchanged[3].

There are many more possible quantum gates, not necessarily bound to involving a maximum of two qubits, however it is not essential to consider them in this model. Universal sets of these gates can be taken such that any operation may be performed using only gates within that set. This is found to be true, for example, in the case that at least one two-qubit gate along with all the one-qubit gates are taken[3].

Furthermore, the quantum circuit model is universal, so any computation that can be performed by any computer can be described using this model. Conversely, this also means that there is no problem that quantum computers can answer which classical computers cannot already solve. The advantage of quantum computers is the ability to perform certain computations in significantly less time.

## CLUSTER STATES

Perhaps the most distinct phenomenon separating the quantum and classical worlds is entanglement. Two qubits are entangled if the wave function of the pair cannot be expressed individually, but only as an inseparable wave function. This effect is independent of choice of basis.

An entangled pair of qubits could be formed, for example, as the pair of photons produced in the decay of an excited Calcium atom[4]. The initial system has zero angular momentum. To conserve angular momentum, the new system containing the Calcium atom and the two new photons must also have total angular momentum of zero. Thus if one of our photons is clockwise circularly polarised, the other must be anticlockwise circularly polarised: an entangled pair of photons has been created.

Cluster states are a particular form of graph state, which refers to a multi-qubit state which can be represented by a graph[3] as in Figure 3. Each vertex, or node, of the graph (represented by the circles) denotes a qubit, while the joining lines represent interaction between joined qubits. In the cluster

state case, the lines indicate entanglement; the cluster state's defining characteristic is that it is highly entangled[5]. Although cluster states could be considered on any geometry, the state constructed on a two-dimensional lattice is sufficient for the application of quantum computation.

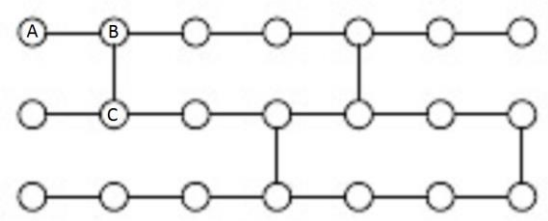


**FIGURE 3**
**A CLUSTER STATE GENERATED ON A TWO-DIMENSIONAL LATTICE OF 21 QUBITS, WITH LINES INDICATING ENTANGLEMENT. THREE ARBITRARY QUBITS A,B AND C HAVE BEEN LABELLED.**

Note that if a qubit A is entangled with a qubit B, and qubit B is entangled with a qubit C, as shown in Figure 3, then A must also be entangled with C. Thus, through a chain of this effect, each qubit is entangled with every other qubit in the system. It is therefore possible to achieve this state without explicit entanglement between every qubit.

There is no reason to confine qubit entanglement to one physical quantity in a quantum computer. Indeed, if *n* different entangled physical quantities are measured from a pair of physical entities, *n* entangled qubits pairs are formed. For example, two photons may be used to produce two entangled qubit pairs using the quantities of both angular momentum and polarisation direction[6].

## ONE-WAY QUANTUM COMPUTERS

An alternative theoretical model for quantum computation is the one-way quantum computer, or measurement-based quantum computer, proposed by Raussendorf and Briegel in 2001[5].

This machine operates by making a sequence of irreversible (hence one-way) single-qubit measurements on a cluster state[3]. Although qubit states are entangled, individual measurement outcomes are random because the states are non-deterministic. However each measurement outcome affects the following measurement, influencing the next measurement basis choice. This information is transferred forward classically; known as feed-forward[3].

The sequence of measurements made on the cluster state form the algorithm that solves the problem. A quantum circuit performs a calculation by using quantum gates to process qubits; with the one-way quantum computer, the measurements perform the same task. The two models are computationally equivalent[5]. Thus, any measurement-based computation performed on a cluster state can be reproduced using a quantum circuit, and conversely, any computation performed by a quantum circuit can be reproduced with the one-way quantum computer by taking appropriate measurements of the cluster state.

The way in which the cluster state is initially prepared defines the limits of possible computations. For specific operations, it would only be necessary to have some sufficient number of entanglements in relevant places. To achieve a universal cluster state, one that could be used to perform any quantum computation, it is necessary for the cluster state to be maximally entangled. This is achieved if each qubit is entangled with each of its closest neighbouring qubits (ie. vertically and horizontally)[5].

Furthermore, one-way quantum computers are universal[3]: they must be if they are computationally equivalent to quantum circuits. Thus a one-way computer built using a universal cluster state can perform any possible computation.

With quantum circuits, it is necessary to prepare relevant circuits for each calculation: effectively, a different quantum computer is required for each computation. This is a primary motivation of one-way quantum computation over other models: producing a single quantum computer which can solve any problem. Once the universal cluster state has been constructed, it can be used to perform any operation depending on how measurements are made on the qubits of the system.

## DECOHERENCE

A major issue with both discussed models of quantum computation is decoherence. Although

measured qubit states are ideally stationary, external interactions cause the states to change with time. Equally, entanglement is not conserved under time evolution. In a system where each qubit is perfectly isolated from its environment, this would not be an issue; however, in reality this is impossible, and would make performing operations and measurements rather difficult regardless. Environmental interactions with the qubit's physical entity alters its wave functions: in other words, decoherence occurs. Efforts are made to isolate the system from external influences, as well as performing quantum error correction[7].

Decoherence effects are closely related to the physical system used to implement the qubit. Photons are good candidates because they do not interact very much with their environment, and thus they decohere slowly. On the other hand, for the same reason, it is more difficult to entangle them. Electrons can be entangled by simply bringing two close together, so would provide an easily entangled qubit system. However, this relatively high interaction with surrounding environment leads to high decoherence. Thus, most current experimental one-way quantum computers use photons as the qubits to minimise decoherence.

## APPLICATIONS

Currently, there are two primary algorithms which have useful application and which can be performed on quantum computers with considerably increased performance[8]. The time complexity of an algorithm quantifies the running time as a function of the input size and is used to measure their performance; for example, a linear time algorithm would have running time scaling linearly with input string length.

The first is Shor's Algorithm, which defines a method of prime factorisation of integers. Classical computers perform this task in exponential time, while Shor's algorithm on a quantum computer can achieve polynomial time[9] (Figure 4), a significant improvement. This application is of particular interest to cryptanalysis as it could break many cryptosystems, including the widely used public-key cryptosystem RSA[9]. RSA depends on the computational difficulty of prime factorisation, so although it is possible to break the encryption, it would take a prohibitively long time. A quantum computer running Shor's Algorithm, however, could break RSA in a practical time scale.

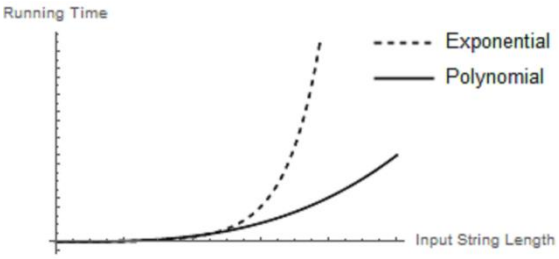


**FIGURE 4**
**EXPONENTIAL TIME COMPARED TO POLYNOMIAL TIME. THE PLOTTED POLYNOMIAL IS CUBIC; HOWEVER, EXPONENTIALS ALWAYS GROW FASTER THAN POLYNOMIALS.**

The other algorithm performs database searching. Classically, each element of the database must be examined systematically until the solution is identified, leading to linear time complexity. A quantum computer can cut this down to square root time (Figure 5) using Grover's Algorithm[9].

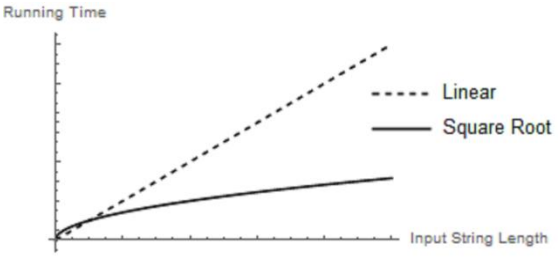


**FIGURE 5**
**LINEAR COMPARED TO SQUARE ROOT TIME COMPLEXITY.**

The key element to these algorithms that allow quantum computers to be so much more efficient at running them is the ability to run the calculation in parallel, that is, the operation can be divided into smaller ones which can be solved concurrently. Using superposition, the multiple operations can effectively be performed simultaneously.

This advantage has led to speculation that simulation of quantum mechanical processes in, for example, chemistry or condensed matter physics, could be performed more efficiently on quantum computers than would be possible with classical

computers[2]. Some mathematical applications that would considerably benefit from quantum computation have also been recognised, like the approximation of Jones polynomials[10] and the solving of Pell's equation[9].

Although the computations currently identified to be significantly improved in performance by quantum computers are very few, the application of quantum computers is a field still in its infancy and it is expected to grow in the future. Regardless, the challenge remains in the physical implementation of the device.

## IMPLEMENTATION

Basic principles of one-way quantum computers have been well demonstrated in laboratories, however only with small numbers of qubits. For example, a four-qubit cluster state was generated using the polarisation states of four photons in 2005[11]. Moreover, Grover's Algorithm was implemented on it, the first quantum algorithm demonstration on a one-way quantum computer[12].

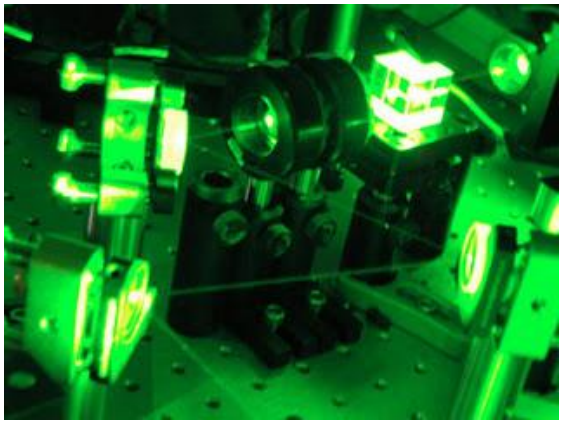

**FIGURE 6**
**AN IMPLEMENTATION OF PHOTONIC QUANTUM COMPUTING. GENERALLY, OPTICAL REALISATIONS LIKE THE EXAMPLE ABOVE USE SIMILAR APPARATUS.**

The foremost problem, however, remains in scaling the system up to include many qubits. In the case of optics-based quantum computers (Figure 6), the photonic qubits are operated on as they travel through optical apparatus, so the equipment must have very low latency and high accurate to compute with particles travelling at light speed. Combined with the resulting prohibitively large apparatus arrangements, the scalability limitations arise from the equipment involved.

The alternative lies with solid-state quantum computers, which concern quantities like nuclear spin. Such a device should be more easily scalable considering the well-developed silicon-based semiconductor manufacturing industry in place using related techniques to produce transistor-based computers. However, the effects of decoherence limit the size of quantum computer possible using this method. Thus, there exists a trade-off between the low-decoherence of optical systems and the scalability of solid-state systems[13]. A possible route forward may lie in using aspects of both systems in the implementation of a quantum computer, as proposed by C. Wu et al. [12]

## REFERENCES


1. R. Feynman, *Simulating Physics with Comptuers*, International Journal of Theoretical Physics **21** 467 (1982)
2. M. Nielson & I. Chuang, *Quantum Computation and Quantum Information,* 10th Ed. (University Press, Cambridge, 2010)
3. M. Nielson, *Cluster State Quantum Computation,* arXiv:quant-ph/0504097v2 (2005)
4. B. Clegg, *The God Effect: Quantum Entanglement, Science's Strangest Phenomenon,* 1st Ed. (St. Martin's Press, Griffin, 2009)
5. R. Raussendorf & H. Briegel, *A One-Way Quantum Computer*, Physical Review Letters **86** (22) 5188 (2001)
6. G. Vallone, E. Pomarico, P. Mataloni, F. De Martini & V. Berardi, *Realization and characterization of a 2-photon 4-qubit linear cluster state,* Physical Review Letters **98** (18) 180502 (2007)
7. B. Bell, D. Herrera-Marti, M. Tame, D. Markham, W. Wadsworth & J. Rarity, *Experimental demonstration of a graph state quantum error-correction code*, Nature Communications **5** 3658 (2014)
8. P. Walther, K. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer & A. Zeilinger, *Experimental one-way quantum computing*, Nature **434** 169 (2005)
9. E. Rieffel & W. Polak, *Quantum Computing - A Gentle Indroduction,* 1st Ed. (MIT Press, Massachusetts, 2011)
10. D. Aharonov, V. Jones & Z. Landau, *A Polynomial Quantum Algorithm for Approximating the Jones Polynomial,* arXiv:quant-ph/0511096v2 (2006)

11. Nature Highlights, *One way to quantum computing*, http://www.nature.com/nature/links/050310/050310-2.html (accessed 23 Nov 2014)
12. C. Wu, M. Gao, H. Li, Z. Deng, H. Dai, P. Chen & C. Li, *Scalable one-way quantum computer using on-chip resonator qubits*, Physical Review A **85** 042301 (2012)
13. E. Martin-Lopez, *Experimental realization of Shor's quantum factoring algorithm using qubit recycling*, Nature Photonics **6** 773 (2012)

## SOURCES OF FIGURES

1. Wikimedia, *Bloch Sphere*, http://upload.wikimedia.org/wikipedia/commons/thumb/f/f4/Bloch_Sphere.svg/163px-Bloch_Sphere.svg.png
2. M. Nielson, *Cluster State Quantum Computation,* arXiv:quant-ph/0504097v2 (2005)
3. P. Kok, *Cluster State Quantum Computing*, http://www.pieter-kok.staff.shef.ac.uk/index.php?nav=research&sub=cluster
4. Produced using Mathematica
5. Produced using Mathematica
6. Next Big Future, *A new scheme for photonic quantum computing,* http://nextbigfuture.com/2011/10/new-scheme-for-photonic-quantum.html (accessed 23 Nov 2014)