Heriot-Watt University
Edinburgh

Quantum Computing

Keith J. Symington
MSc Optoelectronics and Laser Devices

Registration number: 9711710098481

Date: 28th November 1997

1 Abstract

A computer with memory that is exponentially larger than its size may sound ridiculous but it is in fact almost a reality. This report introduces the reader to the theory of *quantum computing* and proceeds to outline four implementation theories: *quantum dots*, *ion traps*, *quantum optical* and *nuclear magnetic resonance (NMR)*. But which quantum technology is the most promising for the future?

2 Contents

3 Introduction

3.1 The Information Revolution

The size of computers is constantly being reduced as lithographic processes proceed to miniaturise the transistor even further. However this trend cannot continue indefinitely because of the atomistic nature of matter; a problem recognised by Landauer ([44], [42]) in 1960. His studies suggested that a minimal limit of one hundred particles is required to represent information reliably.

Since this time, semiconductor technology has drastically improved with the size of transistors continually shrinking. As the size of a transistor is directly related to the number of particles required to store information we can gauge from this how long it will be before we start reaching the quantum regime. By examining the number of dopant impurities required to create a bipolar transistor, Keyes [39] illustrated, as shown in figure 1, that based on the past rate of development we should be reaching this limit within the next 10 years.

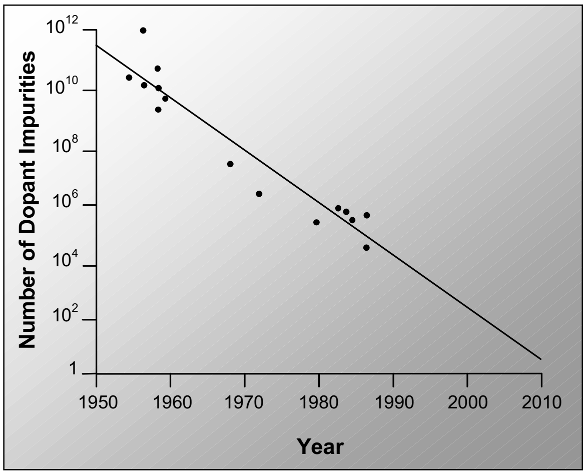

Figure 1

Decreasing number of dopant impurities in base of bipolar transistors for logic.

However, when lithographic processes reach this quantum level, quantum effects will prevent classical systems from functioning correctly - a major problem as far as the electronics industry is concerned. The only way forward then is to start making use of these effects: to represent information on the quantum scale [21].

But with size reduced to quantum levels, a new advantage becomes apparent: exponential parallelism, as theoretically proposed by Deutsch [41]. It is not, however, an incredible solution for system speed increases, simply a physical property of the system exploited in such a way that the quantum laws of superposition are taken full advantage of. Previously unsolvable problems, because of their complexity in a classical system, suddenly become solvable with quantum computation. A good example was given by Shor [29] who proposed an algorithm for the factorisation of numbers using quantum techniques (explained in more depth in [17] and section 4.2.2).

To actually make full use of this property, new ways of algorithmic programming must be considered. Therefore any 'Quantum Revolution' [7] may affect the software industry more than any other industry.

However, we have not yet managed to successfully build a quantum computer solution yet: we are currently only capable of the most rudimentary of implementations. A fully successful implementation of any quantum computer would be a twofold victory for modern technology because not only would it verify all our current quantum theory but it would also put a powerful new computational tool at our fingertips.

3.2 Objectives

This Literature Search will briefly examine the concept of quantum computation and then proceed to consider possible implementations. The advantages and disadvantages of each of four currently theorised implementations will be assessed and finally one recommended based on current theory.

This is a Literature search. It is not meant as a complete explanation of the field, but simply as an introduction to it with a large amount of references from which the reader can follow up any ideas or areas of interest.

This search was designed to try and cover the latest research and has actually focussed itself on papers published between 1995 and 1997: apart from the few obvious exceptions which are considered to be the papers that founded this field ([41] and [29]).

3.3 Report Outline

This report is divided into five major sections:

- **Introduction**: This section is designed to give an idea of why quantum computing is a desirable or perhaps even necessary evolution in computing.
- **Quantum Theory**: Examines a few of the basic concepts required to understand how quantum computing is supposed to work.
- **Implementations**: This section proceeds to look in detail at proposed implementations for quantum computer systems.
- **Conclusion**: Summarises the Literature Search and weighs up the advantages and disadvantages of each implementation.
- **Bibliography**: Contains a full listing of all the references used throughout the report in reverse chronological order of publication. Since this is a Literature Search a copy of the abstracts is provided in small type next to each reference. This allows the reader to get a better idea of what the paper is about without having to retrieve it first.

4 Quantum Theory

> *"This quantum business is so incredibly difficult and important that everyone should busy himself with it."*
>
> Einstein in a letter to his friend Laub, 1908

4.1 The Concept of Superposition

What makes quantum computing so different from classical computing? Let's take it back to the idea of bits 1 and 0.

In current computing systems this bit of information is represented by the voltage difference between two electrical plates: 1 if a charge is present, 0 otherwise.

To represent information in a quantum system we would choose, for example, an atom to represent our bit of information, as shown in figure 2. Here we could use the ground state to represent a 0, the excited state to represent a 1. This form of bit will be referred to from now on as a "quantum bit" or qubit.

However, quantum theory also states that in addition to the two distinct electronic states, an atom can also be in a coherent superposition of these two states i.e. both 0 and 1 at the same time!

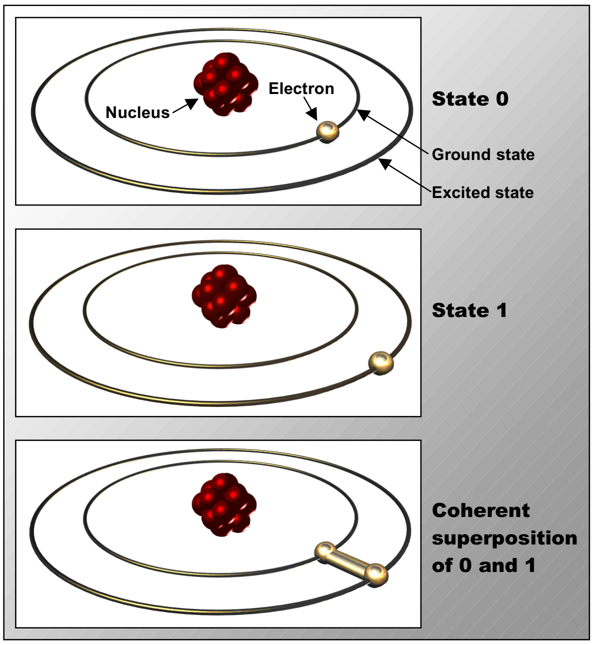

Figure 2

Atom being used to store a bit of information. According to quantum mechanics however, there is one other state that is can be in: a coherent superposition of both states 0 and 1.

To help explain the abstract concept of coherent superposition, consider the experiment shown in figure 3 overleaf. A photon enters the system and hits the half silvered mirror at point *A*. This mirror has a 50% chance that any light hitting it is reflected and indeed if we measure this probability the distribution is 0.5 for each beam. However this does not mean that the photon simply travels in either reflected or transmitted beams: the photon does in fact travel both paths at once. This can be demonstrated by re-combining the beams at point *B*, at which a very interesting phenomenon of quantum interference can be observed.

As shown in the diagram, we would expect that there is an equal probability of the photon appearing at either detector 1 or 2. Again, this is not the case: if the path lengths are equal the photon always appears at detector 1!

It seems that the photon must have examined both routes in some sense because if an absorbing screen is placed at point *C* there is an equal chance that either detector 1 or 2 is hit - the photon does not consider travelling down the path which is blocked by the absorber. We can therefore say that the photon took both the transmitted and reflected paths i.e. is in a coherent superposition of being in both transmitted and reflected paths.

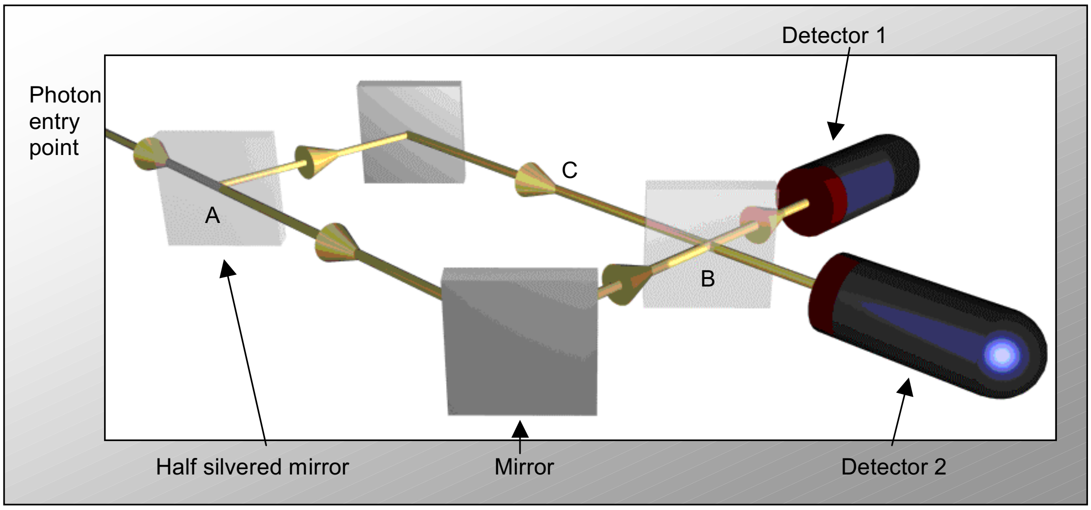

Figure 3

Diagram of beam-splitter experiment: Note that all possible paths are shown in this diagram.

It is therefore possible for a qubit to have a third state where it is both 0 and 1 at the same time. Reference [37] deals with this concept in some detail and is recommended reading.

4.1.1 The Qubit

To represent a binary value we need to consider an elementary spin-½ particle (such as an electron or proton) which will have a spin down state written $|\downarrow\rangle$ and a spin up state written $|\uparrow\rangle$. These can be considered to be binary $|0\rangle$ and $|1\rangle$ respectively. We can therefore write its wave function down as being:

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

Equation 1

where the squares of alpha and beta represent the probability that the corresponding particle is in that state.

To enhance the distinguishability of these probabilities, Hilbert space is normally used. If, however, we use a set of *k* spin-½ particles (*k*=3 in the example in equation 2):

$$|5\rangle = |101\rangle = |\uparrow\downarrow\uparrow\rangle$$

Equation 2

It becomes apparent that the dimensionality of this Hilbert space is growing proportionally to 2^k - and therefore also the number of values that may be represented by coherent superposition.

4.1.2 Reversibility

A problem in computing with miniaturisation is dissipation of heat. This problem was realised by Landauer [43] in 1961. To combat this problem, computation needs to be performed in such a way that the input can be retrieved from the output: i.e. the system is logically reversible. If we have a logically reversible system we should be in a position to create a gate that is also physically reversible. The second law of thermodynamics then states that if an operation is physically reversible it will dissipate no heat - almost a necessity when we are working at the quantum level.

4.1.3 Decoherence

Theoretically, quantum computing should work without many problems. However, there are still a few practical problems to be overcome before a solution can be implemented and one of these is decoherence [21] [45] [46]. There have already though been a few solutions to this problem proposed [5].

Quantum systems need to be perfectly isolated from their environment. If they are not then the quantum dynamics of the surrounding environment could influence a calculation's evolution in the system. Since the computation pathways are separated at the beginning and only re-combined at the end, any interference will spoil the constructive and destructive effects essential in quantum computing. It is therefore necessary that any decoherence time t_ϕ (seconds) needs to be far longer than the time required to complete computation, given switching time t_{switch} (seconds). Unruh [18] examines this problem and concludes that most present day qubits are inadequately phase coherent to perform factorisation of a 10^4 bit number using Shor's algorithm. Qubit technology is, however, continually improving.

Quantum System	t_{switch} (s)	t_ϕ (s)	Ratio
Mössbauer nucleus	10^{-19}	10^{-10}	10^{9}
Electrons: GaAs	10^{-13}	10^{-10}	10^{3}
Electrons: Au	10^{-14}	10^{-8}	10^{6}
Trapped ions: In	10^{-14}	10^{-1}	10^{13}
Optical microcavity	10^{-14}	10^{-5}	10^{9}
Electron spin	10^{-7}	10^{-3}	10^{4}
Electron quantum dot	10^{-6}	10^{-3}	10^{3}
Nuclear spin	10^{-3}	10^{4}	10^{7}

Figure 4

Important times for various two-level systems in quantum mechanics that might be used as quantum bits.

Figure 4 shows values that are unfortunately not the newest: they date from 1995.

4.2 The Advantage of Quantum Computing

Quantum computers are the same as classical computers except in one major sense: to do the same as a quantum computer, a classical computer needs exponentially more time and resources. For example, if we have a quantum register of size *k*, it can be seen to represent 2^k numbers simultaneously. Unfortunately, if we were to measure what value this quantum register held when it was in a superposition, we cause the wave function in equation 1 to collapse and suddenly we have a specific value. This problem is known as observer participation [37]. However if we do not observe this register directly we can use it to solve previously unsolvable problems…

4.2.1 Prime Factorisation of Numbers

The RSA public key cryptosystem relies on the fact that large numbers are difficult to factorise. In fact the best known algorithm on a classical computer for prime factorisation of a number *N* requires the number of steps shown in equation 3:

$$\exp\left[\left(\frac{64}{9}\right)^{1/3}(\ln N)^{1/3}(\ln \ln N)^{2/3}\right] \qquad \textbf{Equation 3}$$

the algorithm scaling exponentially with respect to log *N*.

On the other hand, the quantum implementation in Shor's [29] requires the number of steps shown in equation 4:

$$(\log N)^{2+\varepsilon} \qquad \textbf{Equation 4}$$

where ε is a very small number.

To illustrate the difference, let us consider a recent attempt at factoring a 129 digit number. 1,600 workstations throughout the world required 8 months to factor this number. Scaling this up to a 1,000 bit number, it would take classical computing methods 10^{25} years to factor such a number. On the other hand, a quantum computer using Shor's algorithm would require only a few million steps to factor a 1,000 bit number.

4.2.2 Shor's Algorithm

Classical computation follows a single, definite, pathway from beginning to end. However, quantum computation can follow several pathways which evolve in time in parallel because of the principle of superposition.

Consider figure 5. Each plane in this diagram represents the Hilbert space for both input and output registers where *k*=1000 bits. The shaded areas indicate the instantaneous state vectors throughout the 3 main phases of Shor's algorithm.

Start: The starting state is first set so that all the particles are spin down i.e. equal to zero. The number *N* to be factored is not yet needed.

Stage 1: The computation is now split up into 2^{1000} pathways. Which turns the wave function into a superposition of all possible states of input register *x*.

Stage 2: First the function in equation 5 should be evaluated with the result being put in the output register *y*.

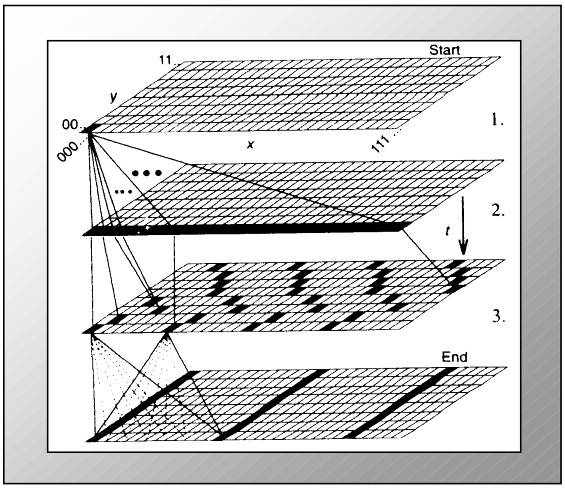

Figure 5

A schematic depiction of the time evolution pathways taken in Shor's prime factoring procedure. The top layer is the start time and the bottom layer 3 the end time. A filled rectangle indicates a computational state appearing in the wave function with a few of the pathways between sketched out. Most pathways in the final stage interfere destructively (dotted line) however some interfere constructively (solid lines). Taken from [21].

$$f(x) = c^x (\bmod N) \qquad \textbf{Equation 5}$$

Here *x* is the value being considered as a factor, *N* is the value to be factored and *c* is any integer that does not have any factors in common with *N*. We use mod here to represent modular arithmetic where the result is the remainder after division by *N*. Because of the superposition principle, evaluating equation 5 obtains every value of the output presuming that the input is a superposition of all possible values. The Importance of *f(x)* is its periodicity in relation to *x*. If *N* is a prime number then the period of *f(x)* is *N*-1. However, if *N* is composite *f(x)* has a shorter period and after a little classical computation we can extract one of the prime factors from this period.

More information on what *f(x)* is useful for the factorisation of prime numbers is give in [29] (original) and [17] (recent review).

Stage 3: Quantum computers are also very well suited to finding the periodicity of *f(x)*. This can be done by taking a DFT (Discrete Fourier Transform) of the input register *x*. The wave function in equation 6

$$\psi_t = \sum_{x=00...0}^{11...1} c_x |x\rangle \qquad \textbf{Equation 6}$$

is therefore evolved into that in equation 7 after the DFT.

$$\psi_f = \sum_{x=00...0}^{11...1} \left(2^{-k/2} \sum_{x'=00...0}^{11...1} e^{2\pi i x x' / 2^{k2}} c_{x'} \right) |x\rangle \qquad \textbf{Equation 7}$$

This proves to be a very efficient method of obtaining the periodicity of *f(x)* which is then available in the *x* register. This measure is unfortunately an unknown multiple of the fundamental period of *f(x)*; however there are some straight forward number-theory-considerations that can be used to reliably find the fundamental period.

4.2.3 A Final Word on Shor's Algorithm

The above description does not do this complicated algorithm any justice. For further information please refer to [17].

4.2.4 Error Correction in Shor's

Error detection and correction is actually not much of a problem in Shor's algorithm. This is because simple multiplication of the factors should give the number back which was being factored in the first place. This allows detection of the error, and correction ensues by simply running the algorithm again.

4.3 Gate Types

We now have a definition for quantum registers and a useful algorithm, but how is it possible perform a logical operation on something which essentially cannot be observed? Without these operations it is not possible to actually manipulate any data in the fashion we desire. There are fortunately various implementations all with a common trait: they are all reversible (see section 4.1.2).

4.3.1 The Controlled-Not Gate

This gate is the building block of most quantum computer solutions and is commonly known as the CN or CNOT gate. Considering it elementarily, if we have two qubits $|A\rangle$ and $|B\rangle$ we have:

If ($|A\rangle = 1$) then $|B\rangle$ = (NOT $|B\rangle$)

This gate system is also analogous to a XOR gate. Figure 6 shows a diagram of the gate with its associated truth table.

$\|A\rangle$ in	$\|B\rangle$ in	$\|A\rangle$ out ($\|A\rangle$)	$\|B\rangle$ out ($\|A \oplus B\rangle$)
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

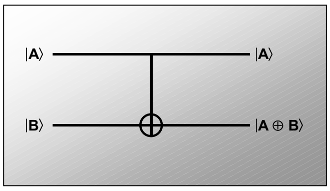

Figure 6

CNOT gate diagram and logic.

To give an example of how useful this gate can be please examine figure 7. This figure shows a sample implementation, which is reversible, that swaps both input bits.

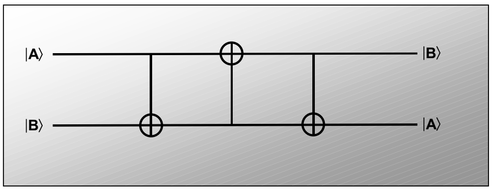

Figure 7

Sample application for CN gate which reverses the inputs.

4.3.2 CN Implementation

But how can we actually perform a logical NOT on the quantum level?

Relating back to our atomic model in 4.1, to reverse the current state at either of the energy levels we need to shine a pulse of the appropriate light intensity, duration and wavelength onto the atom. If the wavelength matches the energy difference level between both ground and excited states then the electron will change energy level: If it is in the ground state it will jump to the excited state and vice versa.

This implementation has actually been performed on atoms of rubidium (ENS experiments) and beryllium (NIST experiments)

4.3.3 The Toffoli Gate

The major problem in quantum computing is reversibility. This problem was overcome by Toffoli when he created a gate with the ability to perform all the logic functions that a computer may require. It also has the major advantage that a second application of itself will retrieve the original input. Figure 8 shows a block diagram and brief explanation of each of the functions.

$$B \oplus (A.C) \begin{cases} A.C & \mathit{for} \quad B=0 & AND \\ A \oplus B & \mathit{for} \quad C=1 & XOR \\ \overline{B} & \mathit{for} \quad A=C=1 & NOT \\ A & \mathit{for} \quad B=0, \;\; C=1 & FANOUT \end{cases}$$

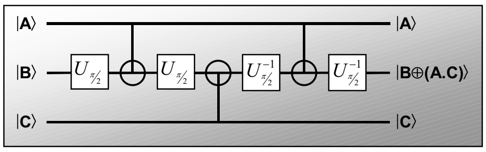

Figure 8

Toffoli gate and the logic operations it can perform.

A major problem though is that we get a lot of junk bits from the Toffoli gate. At this point we need to consider creating an erase gate to remove some of the inconsequential information. To erase information about a particle's state we must irreversibly compress phase space by a factor of 2. Landauer concluded [43] that to erase a bit of information at temperature *T* requires the dissipation of at least the amount of heat shown in equation 8

$$k_B T \ln 2$$

Equation 8

Landauer's principle

where k_B is Boltzmann's constant.

4.3.4 The Fredkin Gate

The Fredkin gate will not be examined in depth here, but for the sake of completeness its truth table is as shown overleaf in figure 9.

Input			Output		
c_i	a_l	b_i	c_o	b_o	a_o
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	1	1	1

Figure 9

For more information on the Fredkin gate see paper [36].

5 Implementations

This section examines current implementations of quantum systems paying particular attention to quantum dot and trapped ion systems.

There are still a lot of problems in this field since obtaining the correct conditions for a working quantum computing system is extremely demanding. Firstly, precise control of Hamiltonian operators on a well defined quantum system is not that simple and secondly we still have the major problem of decoherence (see section 4.1.3).

There are 5 important rules laid down [8] which can be used to define a quantum computer's operation:

1) Well defined qubits should be identified.
2) Reliable state preparation should be possible.
3) The system should have low decoherence.
4) Accurate quantum gate operations must be possible.
5) There must be strong quantum measurements.

These points need to be adhered to if a satisfactory quantum computer is to be designed.

5.1 Quantum Dot Systems

Quantum dots have one big advantage over other quantum computing methods: ease of implementation. Unlike all other systems mentioned here,

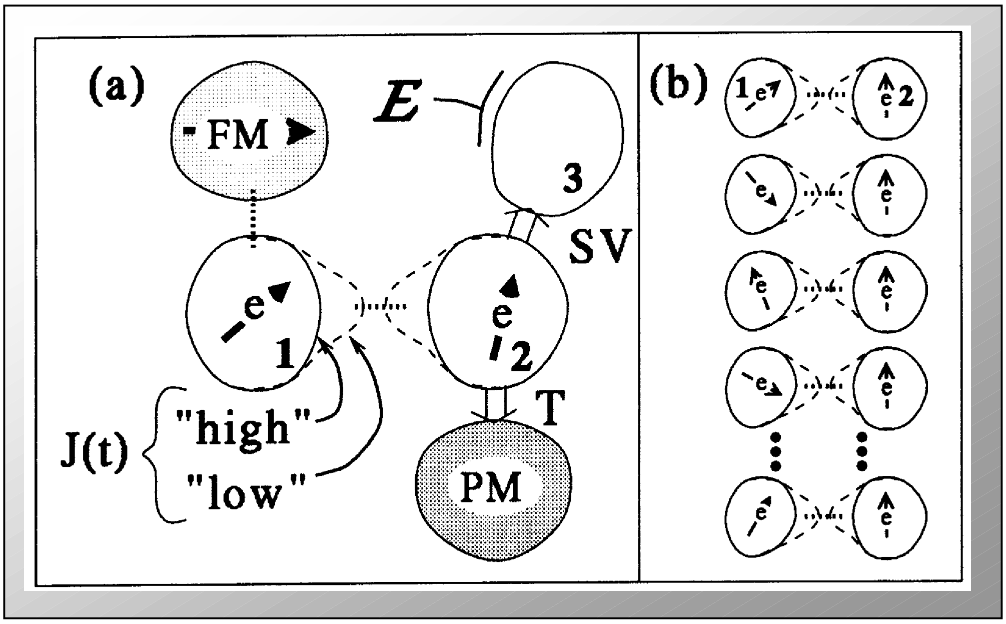

Figure 10

Sample quantum dot implementation. Please refer to text for details. Taken from [8].

the quantum dot does not actually work with quantum sized particles. Instead it is a magnetic nano-system within which the non-equilibrium spin dynamics can be controlled. The sheer fact that it is a nano-system puts us in a position to fabricate it far easier than any of the other choices.

The model qubit in a quantum dot system is realised as the spin of the excess electron on a single electron quantum dot. Interaction between qubits is performed using controlled gating of the tunnelling barrier between neighbouring quantum electron dots. When the dots are set to interact, the spins in a quantum dot system become subject to a transient Hysenberg coupling. Please examine figure 10 carefully.

Section (a) in figure 10 shows two quantum dots labelled 1 and 2 each with one excess electron *e* with spin-½. The tunnel barrier can be raised or lowered by setting a gate voltage high (solid equipotential contour) or low (dashed equipotential contour). If the tunnel barrier is lowered then virtual tunnelling will produce a Heisenberg exchange *J(t)* with respect to time. One method of performing single qubit operations is by hopping to an auxiliary ferromagnetic dot FM. Another method is tunnelling (T) to a paramagnetic (PM) dot which may be used as a positive operator valued (POV) [34] readout with 75% reliability. The final method is spin dependent tunnelling through 'spin valve' SV into dot 3 which allows spin measurement via an electrometer.

Section (b) in figure 10 describes a proposed experimental setup for initial test of swap-gate operation in an array of non-interacting quantum dot pairs. The left column here is unpolarised while the right one is polarised.

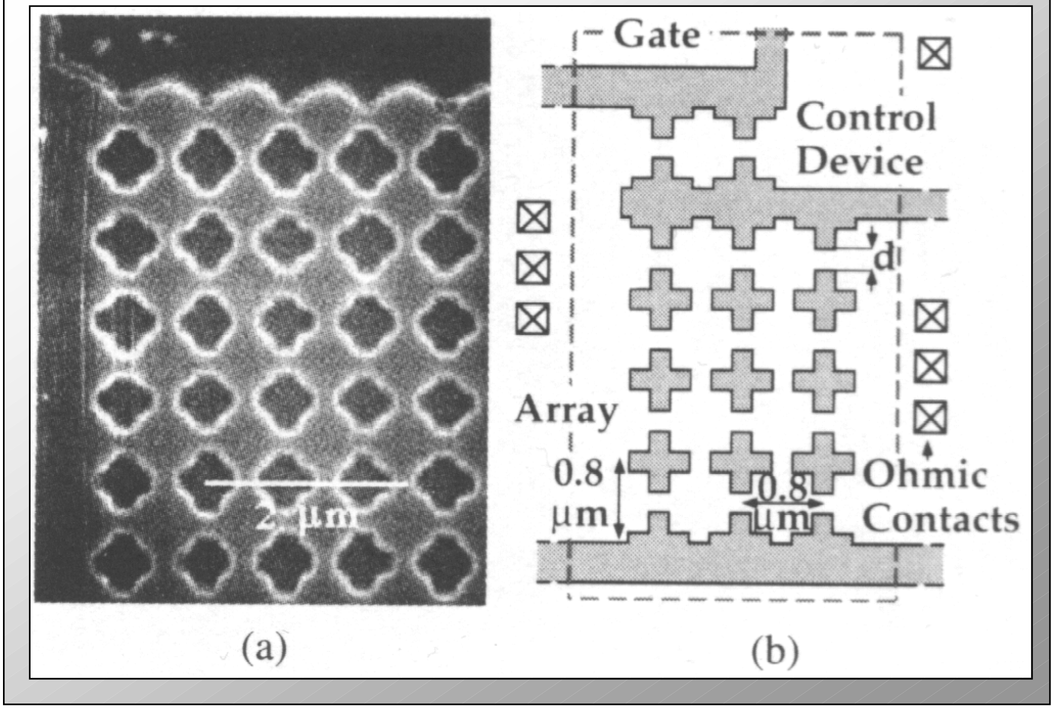

Figure 11

(a) shows a picture of the fabricated array while (b) shows a schematic layout of the array, control device and ohmic contacts. Taken from [27].

State preparation is possible by cooling the system sufficiently in a uniform magnetic field: acceptable spin polarisation will eventually be reached at cryogenic temperatures. An example of this is shown in (b) in figure 10.

A normal quantum dot system can be made using today's lithographic techniques [27]. Figure 11 shows an electron micrograph of such a system made from standard modulation doped GaAl/$Al_{0.34}Ga_{0.66}As$.

One method of non-invasive measurement of the quantum dot is called ballistic point contact measurement [3], however decoherence from point contact was recently observed by Buks [2]. For further discussion on coherence in quantum dots please refer to [26].

Of all the implementations of quantum computers, quantum dots seem to be one of the fastest growing. Whether or not it will become the first working implementation of quantum computing remains to be seen.

5.2 Trapped Ion Systems

Trapped Ion systems [22] are realised by trapping a single ion in a chosen quantum state of the centre-of-mass vibrational motion (for a complete analytical description of the motion of a trapped ion in either an even or odd state, please refer to [10]). The two states of the *n*-th qubit are characterised by the two internal states of the corresponding ion. If we consider the ground state to have an approximate value of 0 and the excited state a value of 1 we can define a state of the quantum computer to be a macroscopic superposition, as shown in equation 9, of quantum registers $|\underline{x}\rangle = |x_{N-1}\rangle_{N-1}\ldots|x_0\rangle_0$

$$\left|\psi\right\rangle = \sum_{x=0}^{2^N-1} c_x \left|x\right\rangle \equiv \sum_{\underline{x}=\{0,1\}^N} c_{\underline{x}} \left|\underline{x}\right\rangle$$ **Equation 9**

$$x = \sum_{n=0}^{N-1} x_n 2^n$$ **Equation 10**

where *x* equals equation 10, the binary decomposition of *x*.

It is possible to trap a set of *N* cold ions in a linear trap [30] [35] and use laser light as a means of interaction - as shown in figure 12. This system is characterised by:

- It allows the implementation of *n*-bit quantum gates between any set of (not necessarily neighbouring) ions.
- Decoherence can be made negligible during the whole computation.
- The final readout can be performed with unit efficiency.

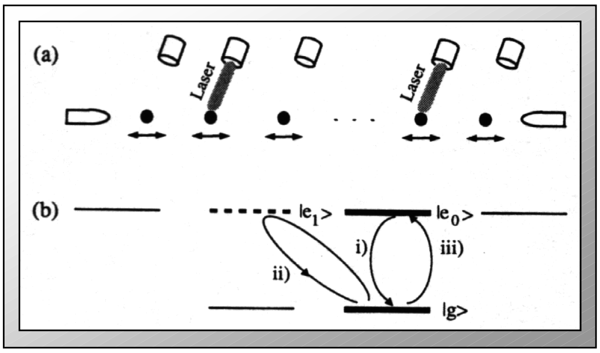

Figure 12

(a) N ions in a linear trap interacting with N different laser beams; (b) atomic level scheme. Taken from reference [22].

Individual manipulation of a qubit can be easily performed by directing different laser beams onto each of the ions.

However, decoherence in the system is still a problem and is caused by spontaneous decay of the internal atomic states and damping of the motion of the ion [15]. Another more obscure source is decoherence due to intensity and phase fluctuations in the exciting laser pulses [4]. Both of these limit the size of computation ion trap systems can perform: for example, figure 13 shows the size of number that can be factorised dependant on how quickly an ion type becomes decoherent.

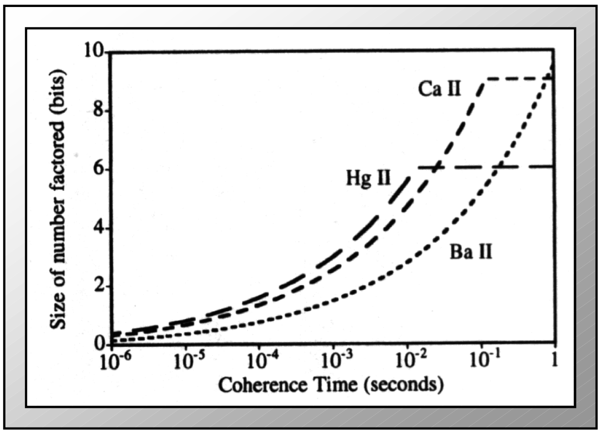

Figure 13

The variation of the number of bits l in the largest integer that may be factored depending on ion type. Maximum values are determined by spontaneous emission. Figure taken from [15].

The problem of spontaneous emissions can fortunately be suppressed by the use of metastable transitions as described in [28]. In addition, given sufficiently low pressures, the chance of collisions with background atoms, and their couplings that affect the moving charges, can be reduced to give stability for very long times [31].

Finally, the readout of the quantum register at the end of a calculation can be accomplished using the quantum jumps technique [16] [40] with unit efficiency.

Linear ion traps are well suited to implement a quantum computer, however, scaling them up to do large scale quantum computing is a problem. The reason they are so suited is because of negligible decoherence in the system [31] and unit efficient readout techniques.

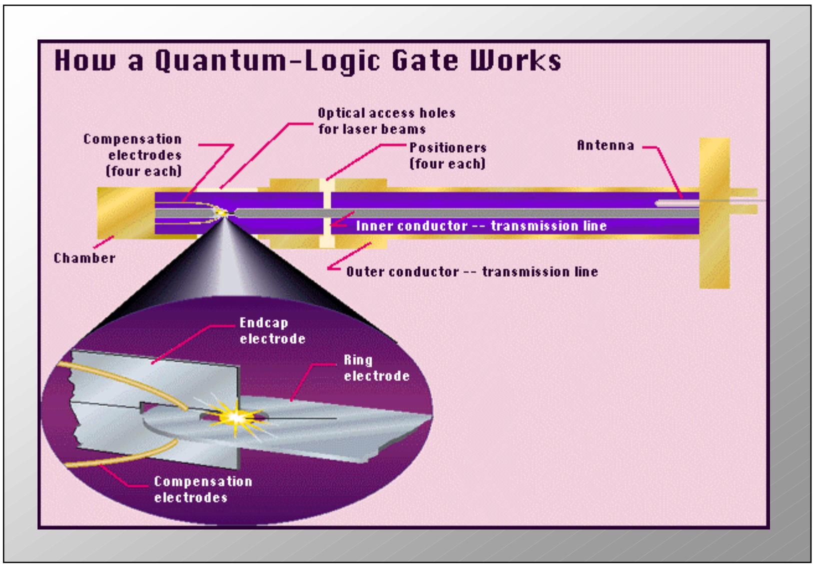
How a Quantum-Logic Gate Works
Optical access holes for laser beams
Compensation electrodes (four each)
Positioners (four each)
Antenna
Inner conductor -- transmission line
Chamber
Outer conductor -- transmission line
Endcap electrode
Ring electrode
Compensation electrodes

Figure 14

Possible design for an Ion trap quantum computing system. Internet source unknown.

5.3 Quantum Optical

Quantum Optical systems make use of the superposition of single photons to perform optical computations. The major advantage of using optical frequencies is that they are essentially isolated from thermal noise and thus ideal for analysing the ultimate quantum limits to reversible quantum computation.

However this very advantage is also its drawback: There is no such thing as a lossless symmetric beam splitter, polarising media or Kerr media. This means that regardless of what happens there is always a chance that a photon in the middle of a computation will be lost with disastrous effects. Without error detection or correction there is no way of knowing whether the computation was correctly performed or not.

An important development in quantum optics was the development of the quantum optical Fredkin gate (see section 4.3.4 for more information) by Milburn [36] in 1989. As time progressed, so did the theory and in 1996, Chuang and Yamamoto [14] proposed a full implementation for a simple quantum computer - with only one problem: we still do not have the technology to implement it. Since this point, technology has not progressed particularly far, but the requirements from it have changed.

In June of 1997, Cerf, Adami and Kwiat [9] published a paper that outlined a system which they believe can be implemented using present technology. One major advantage in their system was that it uses purely linear optical components: in other words avoiding recourse to non-linear Kerr media. It does unfortunately also have its disadvantages: the system has an exponential need for resources as it is scaled up. They therefore recommended that the system is only useful for creating small scale quantum circuits.

Quantum optic computing was one of the foundations of quantum computing but it is also probably the most problematic to implement. We should not however write it off as photonic systems are one of the most resilient to noise.

5.4 NMR Quantum Computing

NMR (Nuclear Magnetic Resonance) systems [6] (when working in a liquid state) perform computation on a large number of identical quantum systems. Each quantum system consists of the interacting nuclear spins of a molecule in a high magnetic field. There are three stages to NMR computation:

- Preparation: Performed by allowing the system to relax to thermal equilibrium.
- Computation: The nuclear spins within the system are manipulated by applying radio frequency (RF) pulses tuned to the Larmor frequencies. Spins can be selectively excited by exploiting differences in these frequencies.
- Readout: Performed by observing the signal induced in RF coils by the precession of the nuclear spins.

Figure 15 showns an example of a trichloroethylene molecule representing a 3 qubit system.

The main problem with NMR is using it for the observation of multi-particle entanglements and quantum computation is that the sample is initially in a highly mixed state. This can fortunately be overcome without cooling by transforming the initial mixed state so that we have a psuedo-pure state.

Room temperature NMR proves to be useful for computations involving small numbers of qubits. There is one interesting point though: NMR is the only technology where we can systematically entangle more than two qubits.

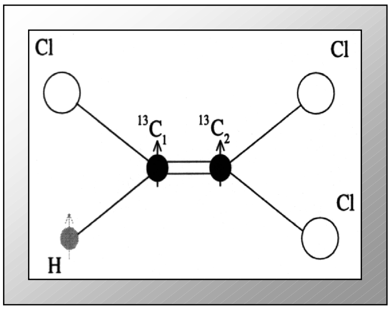

Figure 15

Trichloroethylene molecule being used for NMR: 3 qubits are Hydrogen and both Chlorine molecules. Diagram taken from [6].

5.5 Further Reading

There are a number of papers which relate to the quantum computing field but did not fit nicely under any of the headings in the report. These papers are detailed in the references section and have the following numbers: [1], [11], [13], [23] and [25].

6 Conclusion

The main problem for any practical realisation is the existence of decoherence processes due to the interaction of the system with the environment. These problems are beginning to dwindle as are not only better technologies becoming available, but so are better theoretical versions of a quantum computer.

From the information available, it seems that in the short term quantum dots seem to be the most promising technology for quantum computers. They are nano-scale systems which makes them easier to build than quantum systems, but yet they represent a quantum system. Scalability to large quantum dot systems is also not so much of a problem when compared to scaling up a quantum optical or trapped ion system. This is not to say that the other two don't have their advantages. In the long term it seems that trapped ion quantum computers will become more and more interesting due to the long time it takes for them to become decoherent.

When a working quantum computer is created it will be a great breakthrough and I believe that this day is not far off. Quantum computing is still in its infancy, but its growing up very fast.

6.1 Future Work

This examination was very much high level: the hard-core maths being left to the referenced papers.

An interesting extension to this report would be the consideration of method of implementation for a quantum dot system as this area of research seems very promising.

7 Bibliography

This section has been put in reverse chronological order. Some of the following references also have a copy of their abstract accompanying them in small type - this is to give the reader a good idea of what the papers are about in advance.

[1] A. Chi-Chih Yao, *"Quantum Circuit Complexity"*, Department of Computer Science, Princeton University, not known to be published.

We study a complexity model of quantum circuits analogous to the standard (acyclic) Boolean circuit model. It is shown that any function computable in polynomial time by a quantum Turing machine has a polynomial-size quantum circuit. This result also enables us to construct a universal quantum computer which can simulate, with a polynomial factor slowdown, a broader class of quantum machines than that considered by Bernstein and Vazirani [32], thus answering an open question raised in [32]. We also develop a theory of quantum communication complexity, and use it as a tool to prove that the majority function does not have a linear-size quantum formula.

[2] E. Buks, R. Shuster, M. Heiblum, D. Mahalu, V. Umansky and H. Shtrikman, Bulletin of the American Physical Society, volume 42, number 1, 1997, page 769.

[3] S. A. Gurvitz, *"Measurements with a noninvasive detector and dephasing mechanism"*, Los Alamos archives cond-mat/9706074 v2, October 1997.

We study dynamics of the measurement process in quantum dot systems, where a particular state out of coherent superposition is observed. The ballistic point-contact placed near one of the dots is taken as a noninvasive detector. We demonstrate that the measurement process is fully described by the Bloch-type equations applied to the whole system. These equations clearly reproduce the collapse of the density-matrix into the statistical mixture in the course of the measurement process. The corresponding dephasing width is uniquely defined. We show that the continuous observation of one of the states in a coherent superposition may accelerate decay from this state - in contradiction with rapidly repeated observations, which slow down the transitions between quantum states (the quantum Zeno effect).

[4] S. Schneider and G. J. Milburn, *"Decoherence in ion traps due to laser intensity and phase fluctuations"*, Los Alamos archives quant-ph/9710044, October 1997.

We consider one source of decoherence for a single trapped ion due to intensity and phase fluctuations in the exciting laser pulses. For simplicity we assume that the stochastic processes involved are white noise processes, which enables us to give a simple master equation description of this source of decoherence. This master equation is averaged over the noise, and is sufficient to describe the results of experiments that probe the oscillations in the electronic populations as energy is exchanged between the internal and electronic motion. Our results are in good qualitative agreement with recent experiments and predict that the decoherence rate will depend on vibrational quantum number in different ways depending on which vibrational excitation sideband is used.

[5] Lu-Ming Duan and Guang-Can Guo, *"Preserving Coherence in Quantum Computation by Pairing Quantum Bits"*, Phys. Rev. Lett., volume 79, number 10, September 1997, page 1953

A scheme for protecting quantum states from both independent and cooperative decoherence is proposed. The scheme operates by pairing each qubit (two-state quantum system) with an ancilla qubit and by encoding the states of the qubits into corresponding coherence-preserving states of qubit pairs. In this scheme, amplitude damping (loss of energy) as well as phase damping (dephasing) is prevented by a strategy called "free-Hamiltonian elimination." We further extend the scheme to include quantum gate operations and show that loss and decoherence during such operations can also be prevented.

[6] R. Laflamme, E. Knill, W. H. Zurek, P. Catasti and S. V. S. Marippan, *"NMR GHZ"*, Los Alamos archives quant-ph/9709025 v1, September 1997.

We describe the creation of a Greenherger-Horne-Zeihnger (GHZ) state of the form $(|000\rangle + |111\rangle)/\sqrt{2}$ (three maximally entangled quantum bits) using Nuclear Magnetic Resonance (NMR). We have successfully carried out the experiment using the proton and carbon spins of trichloroethylene, and confirmed the result using state tomography. We have thus extended the space of entangled quantum states explored systematically to three quantum bits, an essential step for quantum computation.

[7] A. Zeilinger, *"Get set for the quantum revolution"*, Physics World, September 1997, page 54.

[8] D. Loss and P. DiVincenzo, "Quantum Computation with Quantum Dots", Los Alamos archives cond-mat/9701055 v3, July 1997.

A completely analytic description is given of the motion of a trapped ion which is in either an even or an odd coherent state. Comparison to recent theoretical and experimental work is made.

[9] N. J. Cerf, C. Adami and P. G. Kwiat, *"Optical Simulation of Quantum Logic"*, Los Alamos archives quant-ph/9706022, June 1997.

A systematic method for simulating small-scale quantum circuits by use of linear optical devices is presented. It relies on the representation of several quantum bits by a single photon, and on the implementation of universal quantum gates using simple optical components (beam splitters, phase shifters, etc.). This suggests that the optical realization of small quantum networks is reasonable given the present technology in quantum optics, and could be a useful technique for testing simple quantum algorithms or error-correction schemes. The optical circuit for quantum teleportation is presented as an illustration.

[10] M. M. Nieto, *"Analytical Description of the Motion of a Trapped Ion in an Even or Odd Coherent State"*, Los Alamos archives quant-ph/9605010 v2, February 1997.

A completely analytic description is given of the motion of a trapped ion which is in either an even or an odd coherent state. Comparison to recent theoretical and experimental work is made.

[11] N. A. Gershenfeld and I. L. Chuang, *"Bulk Spin Resonance Quantum Computing"*, Cambridge MA and Santa Barbara CA respectively, December 1996.

Quantum computation remains an enormously appealing but elusive goal, appealing because of the ability to perform superfast algorithms such as finding prime factors in polynomial time, but elusive because of the difficulty of simultaneously manipulating quantum degrees of freedom while preventing environmentally induced decoherence. We introduce a new approach to quantum computing based on using multiple phase resonance techniques to manipulate the small deviation from equilibrium of the density matrix of a macroscopic ensemble so that it appears to be the density matrix of a much lower-dimensional pure state. A complete prescription for quantum computing is given for such a system.

[12] A. Barenco, A. Ekert, A. Sanpera and C. Machiavello, *"A short introduction to quantum computation"* from *"Un saut d'echelle pour les calculateurs"*, La Recherche, November 1996

[13] J. F. Poyatos, J. I. Cirac and P. Zoller, *"Complete Characterisation of a Quantum Process: the Two-Bit Quantum Gate"*, Los Alamos archives quant-ph/9611013, November 1996.

We show how to fully characterize a quantum process in an open quantum system. We particularize the procedure to the case of a universal two-qubit gate in a quantum computer. We illustrate the method with a numerical simulation of a quantum gate in the ion trap quantum computer.

[14] I. L. Chuang and Y. Yamamoto, *"A Simple Quantum Computer"*, Los Alamos archives quant-ph/9505011, October 1996.

We propose a implementation of a quantum computer to solve Deutsch's problem, which requires exponential time on a classical computer but only linear time with quantum parallelism. By using a dual-rail qubit representation as a simple form of error correction, our machine can tolerate some amount of decoherence and still give the correct result with high probability. The design which we employ also demonstrates a signature for quantum parallelism which unambiguously delineates the desired quantum behaviour from the merely classical. The experimental demonstration of our proposal using quantum optical components calls for the development of several key technologies common to single photonics.

[15] R. J. Hughes, D. F. V. James, E. H. Knill, R. Laflamme and A. G. Petschek, *"Decoherence Bounds on Quantum Computation with Trapped Ions"*, Phys. Rev. Lett., volume 77, number 15, October 1996.

Using simple physical arguments we investigate the capabilities of a quantum computer based on cold trapped ions. From the limitations imposed on such a device by spontaneous decay, laser phase coherence, ion heating, and other sources of error, we derive a bound between the number of laser interactions and the number of ions that may be used. The largest number which may be factored using a variety of species of ion is determined.

[16] S. A. Gardiner, J. I. Cirac and P. Zoller, *"Measurement of Arbitary Observables of a Trapped Ion"*, Los Alamos archives quant-ph/9606026, June 1996.

We describe a method to perform a single quantum measurement of an arbitrary observable of a single ion moving in a harmonic potential. We illustrate the measurement procedure with explicit examples namely the position and phase observables.

[17] A. Ekert and R. Jozsa, *"Shor's Quantum Algorithm for Factorising Numbers"*, Rev. Mod. Phys., 1995, issue unknown.

There is no known efficient method for factorising large whole numbers on a classical computer. Recently Peter Shor discovered an efficient algorithm for factoring which uses characteristically quantum effects. We give an exposition of Shor's algorithm for factoring on a quantum computer, together with some relevant background in number theory, computational complexity theory and quantum computation including remarks about possible experimental realisations.

[18] W. G. Unruh, Phys. Rev. A, volume 51, 1995, page 992.

[19] A. Fritze *"Quantum Cryptography & Quantum Computing"*, Heriot-Watt University, December 1995.

A review of the basic theoretical concepts of quantum cryptography and quantum computing is given. Different implementations of quantum cryptographic systems are discussed.

[20] Samuel A. Braunstein, *"Quantum Computation: A Tutorial"*, Not known to be published, November 1995.

Imagine a computer whose memory is exponentially larger than its apparent physical size; a computer that can manipulate an exponential set of inputs simultaneously; a computer that computes in the twilight zone of Hilbert space. You would be thinking of a quantum computer. Relatively few and simple concepts from quantum mechanics are needed to make quantum computers a possibility. The subtlety has been in learning to manipulate these concepts. Is such a computer an inevitability or will it be too difficult to build?

[21] D. P. DiVincenzo, *"Quantum Computation"*, Science, volume 270, 13 October 1995, page 255.

If the bits of computers are someday scaled down to the size of individual atoms, quantum mechanical effects may profoundly change the nature of computation itself. The wave function of such a quantum computer could consist of a superposition of many computations carried out simultaneously; this kind of parallelism could be exploited to make some important computational problems, like the prime factoring of large integers, tractable. However, building such a quantum computer would place undreamed of demands on the experimental realization of highly quantum-coherent systems; present-day experimental capabilities in atomic physics and other fields permit only the most rudimentary implementation of quantum computation.

[22] J. I. Cirac and P. Zoller, *"Quantum Computation with Cold Trapped Ions"*, Phys. Rev. Lett., volume 74, number 20, May 1995, page 4091.

A quantum computer can he implemented with cold ions confined in a linear trap and interacting with laser beams. Quantum gates involving any pair, triplet, or subset of ions can be realized by coupling the ions through the collective quantized motion. In this system decoherence is negligible, and the measurement (readout of the quantum register) can be carried out with a high efficiency.

[23] A. Barenco, D. Deutsch, A. Ekert, R. Jozsa, *"Conditional Quantum Dynamics and Logic Gates"*, Phys. Rev. Lett., volume 74, number 20, May 1995, page 4083.

Quantum logic gates provide fundamental examples of conditional quantum dynamics. They could form the building blocks of general quantum information processing systems which have recently been shown to have many interesting non-classical properties. We describe a simple quantum logic gate the quantum controlled-NOT, and analyze some of its applications. We discuss two possible physical realizations of the gate, one based on Ramsey atomic interferometry and the other on the selective driving of optical resonances of two subsystems undergoing a dipole-dipole interaction.

[24] G. M. Palma, K. A. Suominen and A. K. Ekert, *"Quantum Computers and Dissipation"*, Clarendon Laboratory, University of Oxford, May 1995.

We analyse dissipation in quantum computation and its destructive impact on efficiency of quantum algorithms. We discuss relations between decoherence and computational complexity and show that quantum factorisation algorithm must be modified in order to be regarded as efficient and realistic. Our model of decoherence is quite general and incorporates reservoirs with a large coherence length.

[25] T. Sleator and H. Weinfurter, *"Realizable Quantum Logic Gates"*, Phys. Rev. Lett., volume 74, number 20, May 1995, page 4087.

We identify a 2-bit quantum gate that is sufficient to build any quantum logic network. The existence of such a 2-bit universal gate considerably simplifies the search for physical realizations of quantum computational networks. We propose an explicit construction of this gate, which is based on cavity QED techniques and may be realizable with current technology.

[26] A. Yacoby, M. Heiblum, D. Mahalu and H. Shtrikman, *"Coherence and Phase Sensitive Measurements in Quantum Dots"*, Phys. Rev. Lett., volume 74, number 20, May 1995, page 4047.

Via a novel interference experiment, which measures magnitude and phase of the transmission coefficient through a quantum dot in the Coulomb regime, we prove directly, for the first time, that transport through the dot has a coherent component. We find the same phase of the transmission coefficient at successive Coulomb peaks, each representing a different number of electrons in the dot; however, as we scan through a single Coulomb peak we find an abrupt phase change of π. The observed behaviour of the phase cannot be understood in the single particle framework.

[27] C. I. Duruöz, R. M. Clarke, C. M. Marcus and J. S. Harris Jr., *"Conduction Threshold, Switching and Hysteresis in Quantum Dot Arrays"*, Phys. Rev. Lett., volume 74, number 16, April 1995, page 3237.

We investigate low temperature transport in 200 x 200 arrays of GaAs quantum dots in which coupling between dots and electron density is controlled by a single gate. Current-voltage curves obey a power law above a threshold voltage with exponent ~1.5, and show discontinuous and hysteretic jumps in the current, or "switching events." Multiple switching events result in a hierarchy of hysteresis loops. Switching and hysteresis decrease with increasing temperature and disappear above 1K. A possible mechanism for the hysteresis involving gate-to-dot tunnelling is discussed.

[28] R. Blatt, Proceedings ICAP, 1994.

[29] P. W. Shor in *Proc. 35th Annual Symposium on the Foundations of Computer Science*, IEEE press, USA, 1994.

[30] H. Walther, Adv. At. Mol. Opt. Phys., volume 32, 1994, page 379.

[31] D. J. Wineland et al., Phys. Rev. A, volume 50, 1994, page 67.

[32] E. Bernstein and U. Vazirani, *"Quantum Complexity Theory"*, Proceedings of the 1993 ACM Symposium on Theory of Computing, 1993.

[33] A. K. Ekert, *"Quantum Computation"*, Clarendon Laboratory, University of Oxford, 1993.

As computers become faster they must become smaller because of the finiteness of the speed of light. The history of computer technology has involved a sequence of changes from one type of physical realisation to another - from gears to relays to valves to transistors to integrated circuits and so on. Quantum mechanics is already important in the design of microelectronic components. Soon it will be necessary to harness quantum mechanics rather than simply take it into account, and at that point it will he possible to give data processing devices new functionality.

[34] A. Peres, *"Quantum Theory: Concepts and Methods"*, Kluwer and Dordrecht, 1993.

[35] M. G. Raizen et al., Phys. Rev. A, volume 45, 1992, page 6493.

[36] G. J. Milburn, *"Quantum Optical Fredkin Gate"*, Phys. Rev. Lett., volume 62, number 15, May 1989, page 2124.

A simple optical model to realize a reversible, potentially error-free logic gate -a Fredkin gate - is discussed. The device dissipates no energy and makes use of the Kerr nonlinearity to produce intensity-dependent phase shifts. The analysis shows that quantum mechanics permits the operation of error-free logic gates which dissipate no energy. However, even though the device is nondissipative, error-free performance only occurs under particular operating conditions.

[37] J. A. Wheeler, *"World as system self-synthesised by quantum networking"*, IBM J. Res. Develop., volume 32, January 1988, page 4.

The quantum, strangest feature of this strange universe, cracks the armour that conceals the secret of existence. In contrast to the view that the universe is a machine governed by some magic equation, we explore here the view that the world is a self-synthesizing system of existences, built on observer-participancy via a network of elementary quantum phenomena. The elementary quantum phenomenon in the sense of Bohr, the elementary act of observer-participancy, develops definiteness out of indeterminism, secures a communicable reply in response to a well-defined question. The rate of carrying out such yes-no determinations, and their accumulated number, are both minuscule today when compared to the rate and number to be anticipated in the billions of years yet to come. The coming explosion of life opens the door, however, to an all-encompassing role for observer-participancy: to build, in time to come, no minor part of what we call its past-our past, present, and future-but this whole vast world.

[38] C. H. Bennet, *"Notes on the history of reversible computation"*, IBM J. Res. Develop., volume 32, January 1988, page 16.

We review the history of the thermodynamics of information processing, beginning with the paradox of Maxwell's demon; continuing through the efforts of Szilard, Brilloum, and others to demonstrate a thermodynamic cost of information acquisition; the discovery by Landauer of the thermodynamic cost of information destruction; the development of the theory of and classical models for reversible computation; and ending with a brief survey of recent work on quantum reversible computation.

[39] R. W. Keyes, *"Miniaturisation of electronics and its limits"*, IBM J. Res. Develop., volume 32, January 1988, page 24.

Abstract: The long-continued advance of the performance of information processing technologies has been based on miniaturisation of components. The history of miniaturisation is presented through examples. They suggest that limits proposed by Landauer in the 1960s will be reached in two or three decades.

[40] W. Nagourney et al., Phys. Rev. Lett., volume 56, 1986, page 2797.

[41] D. Deutsch, *"Quantum theory, the Church-Turing principle and the universal quantum computer"*, Proc. R. Soc. Lond., A 400, 1985, page 97.

It is argued that underlying the Church-Turing hypothesis there is an implicit physical assertion. Here, this assertion is presented explicitly as a physical principle: 'every finitely realisable physical system can be perfectly simulated by a universal model computing machine operating by finite means'. Classical physics and the universal Turing machine, because the former is continuous and the latter discrete, do not obey the principle, at least in the strong form above. A class of model computing machines that is the quantum generalization of the class of Turing machines is described, and it is shown that quantum theory and the 'universal quantum computer' are compatible with the principle. Computing machines resembling the universal quantum computer could, in principle, be built and would have many remarkable properties not reproducible by any Turing machine. These do not include the computation of non-recursive functions, but they do include 'quantum parallelism', a method by which certain probabilistic tasks can be performed faster by a universal quantum computer than by any classical restriction of it. The intuitive explanation of these properties places an intolerable strain on all interpretations of quantum theory other than Everett's. Some of the numerous connections between the quantum theory of computation and the rest of physics are explored. Quantum complexity theory allows a physically more reasonable definition of the 'complexity' or 'knowledge' in a physical system than does classical complexity theory.

[42] R. Landauer, *"Fluctuations in Bistable Tunnel Diode Circuits"*, J. Appl. Phys., volume 33, 1962, page 2209.

In a series of preceding papers connection has been made between the physics of the activated jump over a static potential barrier and related computing devices. This paper treats a more complicated system, namely, the tunnel diode, which stores information in one of two possible dissipative states. The activated jump between dissipative states is analyzed. An idealised physical model is used to find which of the two states is the really preferred one, and to also evaluate the rate at which fluctuations bring about an approach to this preferred distribution. To simplify the analysis, the case where the tunnel diode is in series with a vacuum diode, rather than a resistor, is emphasised. For typical germanium Esaki diodes, activated jumps are improbable if the junction cross section exceeds 10^{-11} cm^{2}.

[43] R. Landauer, *The seminal paper in reversible computation*, IBM J. Res. Develop., volume 3, 1961, page 183.

[44] R. Landauer, *"Irreversibility and Heat Generation in the Computing Process"*, IBM J. Res. Develop., volume 5, 1961, page 183.

[45] R. Landauer, Proceedings of the Drexel-4 Symposium on Quantum nonitegrability - Quantum Classical Correspondence, D. H. Feng and B. L. Hu Eds., International Press, in press.

[46] R. Landauer, Philos. Trans. R. Soc. London Ser. A., in press.