QUANTUM COMPUTING: AN INTRODUCTION

Tony Hey
Department of Electronics and Computer Science, University of Southampton, Southampton, United Kingdom SO17 1BJ. Email: ajgh@ecs.soton.ac.uk

Abstract
After some remarks on the fundamental physical nature of information, Bennett and Fredkin's ideas of reversible computation are introduced. This leads on to the suggestions of Benioff and Feynman as to the possibility of a new type of essentially 'quantum computers'. If we can build such devices, Deutsch showed that 'quantum parallelism' leads to new algorithms and new complexity classes. This is dramatically illustrated by Shor's quantum algorithm for factorization which is polynomial in time in contrast to algorithms for factorization on a classical Turing computer. This discovery has potentially important implications for the security of many modern cryptographic systems. The fundamentals of quantum computing are then introduced - reversible logic gates, qubits and quantum registers. The key quantum property of 'entanglement' is described, with due homage to Einstein and Bell. As an illustration of a quantum program, Grover's database search algorithm is described in some detail. After all this theory, the status of experimental attempts to build a quantum computer is reviewed: it will become evident that we have a long way to go before we can factorize even small numbers. Finally, we end with some thoughts about the process of 'quantum compilation' - translating a quantum algorithm into actual physical operations on a quantum system - and some comments on prospects for future progress.

1. INTRODUCTION

The fundamental basis of quantum computation is Landauer's observation that all information is ultimately physical [1, 2]. Information, the 1's and 0's of classical computers, must inevitably be recorded by some physical system - be it paper or silicon. Which brings us to the key point. As far as we know today, all matter is composed of atoms - nuclei and electrons - and the interactions and time evolution of atoms are governed by the laws of quantum mechanics. Although the peculiarities of the quantum world may not seem readily apparent at first glance, a closer look reveals that applications of quantum mechanics are all around us (see for example Ref. [3]). As has been emphasized by Minsky [4], the very existence of atoms owes everything not to the chaotic uncertainties of classical mechanics, but rather to the *certainties* of quantum mechanics with the Pauli exclusion principle and well-defined and stable atomic energy levels! Indeed without our quantum understanding of the solid state and the band theory of metals, insulators and semiconductors, the whole of the semiconductor industry with its transistors and integrated circuits - and hence the computer on which I am writing this lecture - could not have developed. The same can be said about quantum optics and lasers: huge industries - from optical communications to music and video CDs - have their basis in these intrinsically quantum technologies.

At bottom then, everything is quantum mechanical and, like Feynman in his visionary 1959 ‘Plenty of Room at the Bottom’ talk [5], we can certainly envisage storing bits of information on single atoms or electrons. However, these microscopic objects do *not* obey Newton's Laws of classical mechanics: instead, they evolve and interact according to the Schroedinger equation, the ‘Newton's Law’ of quantum mechanics. In fact, we know now that even this is only a suitable approximation for everyday speeds and energies: at high speeds and energies, we must use the Dirac equation and Einstein's relativity, with its predictions of relativistic mass increase and particle-antiparticle creation, must be taken into account. However, for most of our everyday concerns, it is safe for us to ignore these complications and use the non-relativistic version of quantum mechanics embodied by Schroedinger's equation.

Information is ultimately not an abstract concept - it must be recorded and stored on media that are fundamentally quantum mechanical. We must therefore broaden our definition of information as merely a string of 1's and 0's and examine the consequences of the quantum nature of media for information. The implications of this new field of quantum information theory are still being explored and may yet deliver more surprises. However, to introduce quantum computing, we shall only need a few quantum concepts and principles. But before we turn to a discussion of qubits and the like, we must now make an apparently puzzling diversion and introduce some ideas of Ed Fredkin and Charles Bennett about reversible computing and reversible logic gates.

2. REVERSIBLE COMPUTING

In 1973, Charles Bennett of IBM Research made a remarkable discovery [6]. Classical computation can be broken down into a series of steps, each logically reversible, and this in turn allows physical reversibility of the computation. This result has implications for the energy dissipated by the computation. Rolf Landauer, Bennett's long-term colleague and mentor, had earlier shown that it is the act of discarding information that incurs an unavoidable energy loss. This is Landauer's Principle and, for example, this is now central to our current understanding of the problem of Maxwell's Demon as given by Bennett [7, 8]. Bennett's result means that we can arrange our computer to calculate reversibly, very slowly, with an energy as small as we please. In his lectures on computation in the 1980's [9], Feynman discusses a reversible computer that calculates for a few steps, then drifts back a bit, ‘uncalculating’ as it goes, before it drifts forward again to eventually complete the calculation with almost zero energy loss.

To build such a reversible computer requires us to use new types of logic gates that are reversible, i.e. from the output of the gate one can reconstruct the input. It is easy to see that a conventional AND gate is not reversible. If the output of an AND gate is 0, the signals on the two input wires could be any one of three possibilities - 00, 01 and 10. The possibility of reversible logic gates was considered by Fredkin and Toffoli nearly 20 years ago [10]. Let us consider a simple example. The truth table for a classical NOT gate is shown below (Fig. 1). It is clearly reversible: from its output we can deduce its input. For this reason Feynman prefers to use the symmetrical notation for a NOT gate shown in Fig. 2. Two NOT gates put back to back evidently bring us back to the same place and manifestly demonstrate the reversibility. Consider now the two-input gate shown in Fig.3. This is called a ‘Controlled NOT’ or CN gate, since the NOT operation on the lower input line is only operative when there is a ‘1’ on the upper input: a ‘0’ on the upper input means that the lower bit passes through unchanged. In effect, what appears on the lower output is just the XOR operation on the two input bits (Fig. 4). However, the CN gate is more than just an XOR gate since we retain information about the control bit. This is a general feature of reversible gates: the price for reversibility is that we need to carry round extra bits of information. But, because we are not discarding any information, such a gate is, in principle, more energy efficient than a classical XOR

A	NOT A
0	1
1	0

Fig. 1 Truth Table for NOT gate.

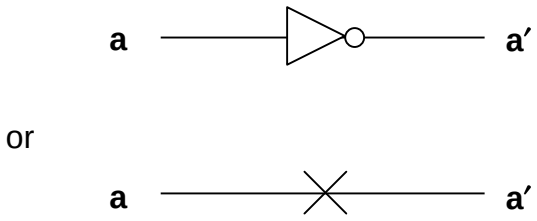


Fig. 2 Alternative symbols for NOT gate.

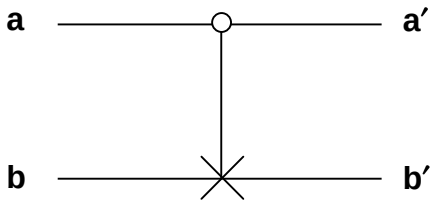


Fig. 3 Controlled NOT or CN gate.

gate. Again, as shown in Fig. 5, the CN gate can be shown to be manifestly reversible by putting two CN gates back to back. Any logical operation can be built from one of several complete sets of classical logic gates - a choice from NOT, AND, OR, XOR, NAND and so on. Similarly, one can show that there are complete sets of reversible gates that allow us to perform any logic operation. In fact, we need more than just the CN gate: we can add a Controlled Controlled NOT (CCN) or 'Toffoli' gate (Fig. 6) or a more complicated Fredkin exchange gate (Fig. 7).

Why do we care about all this? Well for one thing it is possible that use of such gates may one day be needed to reduce power consumption of microprocessors implemented in CMOS silicon technology. At present, the Intel Pentium discards something like 100,000 bits per flop with each discarded bit incurring at least the minimum Landauer energy loss [11]. In our case, however, we are interested because the laws of quantum physics are reversible in time. This guarantees that probability is conserved as a state evolves with time. Technically speaking, the Schroedinger time evolution operator is unitary and preserves the norm of quantum mechanical states (see below). To build a quantum computer with quantum states evolving according to the Schroedinger equation therefore necessarily requires us to use realisations of reversible logic gates.

a	b	a′	b′
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Fig. 4 Truth Table for Controlled NOT gate.

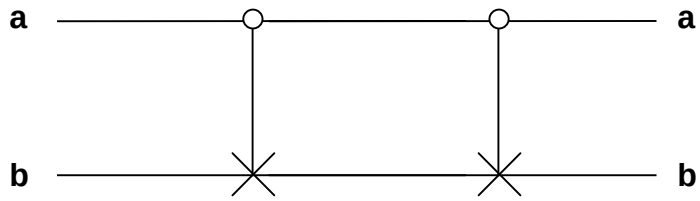


Fig. 5 CN gates are reversible.

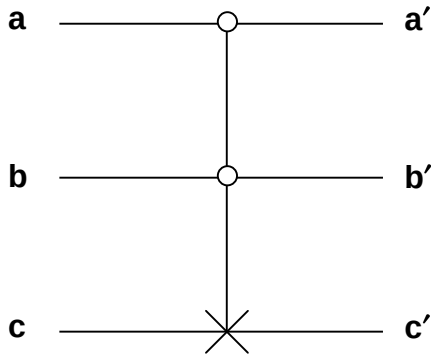


Fig. 6 Controlled Controlled NOT, CCN or Toffoli gate.

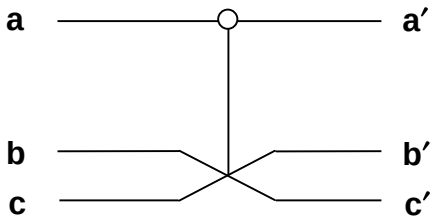


Fig. 7 Fredkin Exchange gate.

3. QUANTUM COMPLEXITY

Complexity is the study of algorithms. The ‘universality’ of Turing Machines makes it possible for computer scientists to classify algorithms into different ‘complexity classes’. For example, multiplication of two N x N matrices requires an operation count that grows like N^3 with the size of the matrix. This can be analysed in detail for a simple Turing machine implementation of the algorithm. However, the important point about ‘universality’ is that although you may be able to multiply matrices somewhat faster than on a Turing machine, you cannot change from an N^3 growth of operations no matter what Pentium chip or special purpose matrix multiply hardware you choose to use. Thus algorithms, such as matrix multiply, for which execution time and resources grow polynomially with problem size, are said to be ‘tractable’ and in the complexity class ‘P’. Algorithms for which time and resources are found to grow exponentially with problem size are said to be ‘intractable’. There are many subtleties to this classification scheme: the famous ‘Travelling Salesperson Problem’, for example, is in the rather mysterious complexity class ‘NP’. The book by David Harel [12] contains an excellent introduction to this subject.

What has this to do with quantum information and quantum computers? In 1985 David Deutsch pointed out that since a quantum computer was not a Turing machine there was the possibility of new complexity classification of algorithms [13]. As we will see, quantum computers evolve a coherent superposition of quantum states so that each of these states could follow a distinct computational path until a final measurement is made at the output. It is therefore certainly conceptually possible that at least for some problems, quantum computers could surpass the power of classical Turing computers. The first speculation that this might be so is probably due to Feynman in 1981 [14]. However, it was not until 1994 that interest in this subject exploded after Peter Shor's discovery of a new quantum algorithm for factorizing large numbers [15].

Mathematicians believe (although it has yet to be proved) that the number of steps required on a classical computer to factorize a number with N decimal digits grows exponentially with N. Since the computational work required grows very rapidly, the difficulty of factorizing very large numbers has been made the basis of the security of the RSA encryption method (see Ref. [13] for a good review of encryption techniques). This system is widely used to protect electronic bank accounts, for example. The significance of Shor's result was that his algorithm, running on a quantum computer, could solve the factorization problem in polynomial time. What this could mean for the RSA cryptographic system may be illustrated by the time required to factorize a 129 digit number known as RSA129 [16]. In 1994 this required 5000 MIPS-years of computer time to factorize into its 64 and 65 bit prime factors, using over 1000 workstations over a period of 8 months. A quantum computer using Shor's algorithm with a clock speed of 100 MHz could factor RSA129 in a few seconds. This explains the interest of various ‘secret’ government agencies around the world in the feasibility of building quantum computers!

4. QUBITS AND QUANTUM GATES

Instead of using high and low voltages to represent the 1's and 0's of binary data, there is no reason in principle for us not to be able to any two state quantum system. Two commonly discussed possibilities are the two spin states of an electron:

$$|1\rangle \text{ and } |0\rangle \qquad \text{as} \qquad \uparrow \text{ and } \downarrow$$

or two polarization states of a photon:

$$|1\rangle \quad \text{and} \quad |0\rangle \qquad \text{as} \qquad H \quad \text{and} \quad V$$

The time evolution of a quantum system is usually well approximated by the Schroedinger equation. In a coordinate space representation, for example, the Schroedinger equation is a linear partial differential equation with the property that any linear superposition of eigenfunctions is also a solution. This superposition property of quantum mechanics means that the general state may be written as a superposition of eigenstates. In the case of our 2-state quantum system the general state may be written as:

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

According to the standard interpretation of quantum mechanics, any measurement (of spin or polarization) made on this state will always yield one of the two eigenvalues with no way of knowing which one. If we prepare an 'ensemble' of identical systems then quantum mechanics assures us that we will observe result '1' with probability $|\alpha|^2$ and result '0' with probability $|\beta|^2$. Normalization of the state to unity guarantees:

$$|\alpha|^2 + |\beta|^2 = 1$$

and this normalization and hence the probability interpretation is maintained by any unitary operator U defined by the property:

$$U^+ U = 1$$

Information stored in a 2-state quantum system is called a quantum bit or 'qubit': besides storing classical '1' and '0' information there is also the possibility of storing information as a superposition of '1' and '0' states.

We can define quantum analogues of classical reversible gates by means of unitary operators acting on the qubit basis states. For example, a quantum version of the NOT operator may be defined as follows:

$$U_{NOT}|1\rangle = |0\rangle$$

$$U_{NOT}|0\rangle = -|1\rangle$$

The phase is chosen for consistency of interpretation in terms of rotations of a spin half particle. The NOT gate corresponds to a 180 degree spin rotation. An overall phase makes no

difference to the probability of measuring the particular basis state although any relative phase difference does affect measurements which depend on the interference between the two basis states.

We now see two possible quantum generalisations compared to computation with classical bits. First, we can perform unitary operations on coherent linear combinations of the two basis states:

$$U_{NOT}\frac{1}{\sqrt{2}}\left(|1\rangle+|0\rangle\right)=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$$

Second, we can consider operations on qubits that have no classical analogue. For example, Deutsch introduces the 'Square Root of NOT' operator defined by:

$$\left(U_{SRN}\right)^2=U_{NOT}$$

$$U_{SRN}|1\rangle=\frac{1}{\sqrt{2}}\left(|1\rangle+|0\rangle\right)$$

$$U_{SRN}|0\rangle=\frac{1}{\sqrt{2}}\left(-|1\rangle+|0\rangle\right)$$

In physical terms, such an operation merely corresponds to a 90 degree spin rotation[1]. Generalizing away from this specific spin interpretation, a transformation that takes a basis state and transforms it into a linear combination of the two basis states is very useful in the construction of quantum algorithms and is called a 'Hadamard' transformation.

We have considered a single electron system for storing a single qubit. By considering multiparticle systems we can construct quantum registers. Thus an n-bit register may be written as:

$$|\psi_n\rangle=|1\rangle\otimes|1\rangle\ldots\otimes|1\rangle\equiv|11\ldots1\rangle$$

[1] The extra minus signs floating around arise from the fact that spin half systems are double-valued representations of the rotation group. A 360 rotation yields the original state apart from an overall minus sign: a 720 rotation is required to return to where we started.

If we now apply our SRN or Hadamard transformation to this state we now generate a superposition of all 2^n states:

$$\left|\psi_n\right\rangle' = U_{SRN} \otimes U_{SRN} \ldots \otimes U_{SRN} |11\ldots1\rangle$$

$$= \frac{1}{2^{n/2}} \left(|1\rangle + |0\rangle \right) \otimes \left(|1\rangle + |0\rangle \right) \ldots \otimes \left(|1\rangle + |0\rangle \right)$$

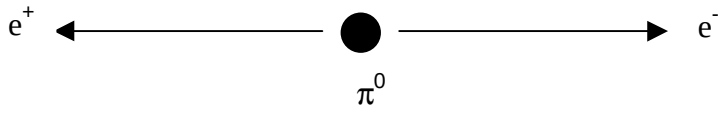
$$= \frac{1}{2^{n/2}} \left\{ |11\ldots1\rangle + |11\ldots0\rangle + \ldots + |00\ldots0\rangle \right\}$$

In other words, by applying a linear number of operations to the quantum register we are able to generate a register state with an exponential (2^n) number of terms. The ability to create such superpositions is one of the key properties that gives quantum parallel processing its power.

We now seem to have all the ingredients - logic gates and registers - to construct a quantum computer. However, neither reversible gates nor superpositions are specifically quantum mechanical. Quantum algorithms derive their remarkable power from one intrinsically quantum phenomenon that we have not so far considered. This is the property called quantum entanglement and, as we shall see, takes us to the very heart of the peculiarities of quantum mechanics.

5. THE 'EPR' PARADOX AND QUANTUM ENTANGLEMENT

As is well known, Einstein was suspicious of the probabilities inherent in quantum mechanics. In the famous 'Bohr-Einstein debate' he tried unsuccessfully to pinpoint an intrinsic contradiction in quantum theory. The climax of this debate was his formulation, with Podolsky and Rosen, of a situation in which one of the essential peculiarities of quantum mechanics was exposed [17]. A modern variant (due to Bohm) of the argument of Einstein, Podolsky and Rosen goes as follows [18]. Imagine we have an elementary particle with zero charge and spin - such as a neutral pion - at rest, which then disintegrates into a spin 1/2 electron and a spin 1/2 positron (Fig. 8). Since angular momentum is conserved in this decay, the two spin half particles must together combine to form a spin zero state. Thus if we measure the electron spin to be up, for example, we know that the positron spin must be down - and vice versa.



$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2\right]$$

Fig. 8 EPR pair created by $\pi^0 \bullet e^+ e^-$ decay.

So what is the problem? Well, the electron and positron are separating rapidly in opposite directions (conservation of linear momentum). If we make the first spin measurement on the electron, we could in principle measure the positron spin before even a light signal had time to communicate to the positron whether its spin has to be up or down! In fact, no matter what we do, we always find perfect anti-correlation between the spins, even though there could have been no physical communication between the two particles. Einstein thought that this demonstrated that the spins of the two particles are therefore not indeterminate before measurement but are actually 'elements of physical reality'. According to Bohr's 'Copenhagen' interpretation of quantum mechanics, it is meaningless to talk of the spin direction of the particles until you make a measurement. This is the truly startling point about quantum mechanics: orthodoxy has it that there is no objective reality (a reality independent of an 'observer') for the electrons and their spins! Einstein would have none of this and thought that things must really be predetermined in advance of the measurement. In other words, although our present formulation of quantum mechanics has the spins as only having a probabilistic value, and since 'spooky, faster than light' signaling is out of the question, there must be some 'hidden variables' that make the directions of the spins predetermined from the outset. After several months of frantic activity devising a response to Einstein's challenge, Bohr declared the EPR paradox not to be a paradox at all and argued essentially that quantum mechanics demands that you are only allowed to treat the electron-positron system as a single quantum system. And there the matter rested, as a rather abstract and philosophical debate about hidden variables and objective reality - since neither side denied that quantum mechanics worked as a predictive framework. Until John Bell entered the debate.

John Bell's great contribution was to devise a way of putting these two views - hidden variables/objective reality and quantum mechanics/no objective reality - to an experimental test. In our discussion above, we only discussed measuring spins in the 'up' and 'down' direction. What happens if we measure 'up/down' for the electron but 'left/right' for the positron. This is easy to calculate according to quantum mechanics. If the electron is found to be 'up', the positron state must be 'down' for our zero spin initial state, and by standard quantum mechanics a down state may be written as an equal superposition of 'left' and 'right' eigenstates. Thus a measurement of the 'right/left' kind on the positron would yield right or left with equal probabilities[2]. John Bell's contribution, as he was proud of saying, was to consider the correlations predicted for spin measurements not at right angles but at an angle of 37 degrees, say. In this case, the probabilities for 'up' and 'down' along this new direction are now not equal and are not purely random. What Bell was able to prove was that the correlations predicted by quantum mechanics are greater than could be

[2] It is just this property of quantum mechanics that is used as the basis for provably secure key distribution in quantum cryptographic systems[19].

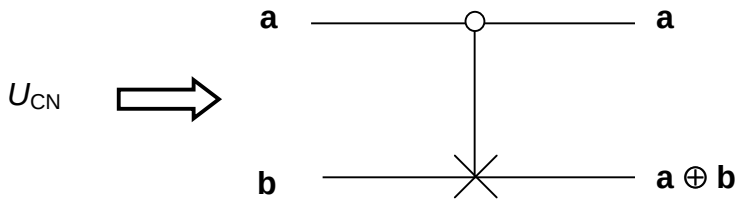
obtained from any *local* hidden variable theory - where local means there is no faster than light signaling or any other peculiar, acausal behaviour [20]. Unfortunately for Einstein, Alain Aspect and co-workers, in a famous series of experiments, demonstrated (to most people's satisfaction) that Bell's hidden variable inequalities are violated and Nature appears to obey quantum mechanics [20].

Why have we made this apparent diversion to discuss the EPR paradox? The reason is that the EPR state of the electron and positron is an example of an 'entangled state'. If we write the spin zero spin state in terms of the spin states of particles 1 and 2 we have:

$$|S=0\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2\right)$$

In the EPR case these two particles are rapidly flying apart. The key point about an entangled state is that it is not possible to write such a state as a simple product state of particle 1 and particle 2. Particle 1 is not in a definite spin state - the spin information is shared between the two particles. This is an example of what is sometimes called an 'entangled qubit' or just an 'e-bit'. The important thing to remember is that it is with such states that quantum mechanics shows its bizarre non-local power.

Why are entangled states of relevance to quantum computing? Consider the action of a quantum CN gate:



If we apply this transformation to the following product state we generate precisely a state of the EPR form:

$$U_{CN}\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle+|1\rangle|1\rangle\right)$$

It is the sharing of two halves of an entangled pair that makes possible such things as 'quantum teleportation' [21]. In this case, interacting with one half of an EPR pair affects the other half in a non-local way. This remarkable non-local nature of quantum mechanics is also an essential ingredient of quantum algorithms on quantum computers.

6. GROVER'S SEARCH ALGORITHM: AN EXAMPLE OF A QUANTUM ALGORITHM

Consider the problem of searching a database with N names in a random order for the telephone number of a friend. Classically this would require on average N/2 steps to find the required entry since there is no smarter way than a brute force O(N) search. Lov Grover was able to devise a quantum algorithm to search an analogous quantum database with N items in $O(\sqrt{N})$ steps [22]. Although this quantum algorithm does not change the complexity class it still provides significant speed-up for large N. The problem may be formulated as follows. We have a system with $N = 2^L$ states. Each state can therefore be labeled as an L-bit string $S_1, S_2, \ldots S_N$. The state we want is S_m which satisfies the condition:

$$C(S_m) = 1 \text{ for } n = m$$
$$C(S_n) = 0 \text{ for } n \neq m$$

The problem is to identify the state S_m.

Grover's algorithm specifies the following steps:

1. Start with L qubit register in state

$$|0\rangle = |00\ldots0\rangle$$

2. Apply Hadamard transformation to generate a superposition of all possible states

$$U_H |00\ldots\rangle = \frac{1}{2^{L/2}} \left(|0\rangle + |1\rangle\right)^L = \frac{1}{2^{L/2}} \sum_{n=0}^{2^L-1} |n\rangle$$

3. DO FOR SQRT N TIMES

4. Apply the operator U_m defined by

$$U_m |n\rangle = |n\rangle \quad for \quad n \neq m$$

$$U_m |n\rangle = -|n\rangle \quad for \quad n = m$$

5. Apply Grover's 'Diffusion' operator

$$U_D = U_H U_0 U_H$$

6. END DO

7. Measurement yields state S_m with high probability

Although this algorithm may appear rather cryptic, the effect of these operations is in fact rather simple. The diffusion operator corresponds to a reflection of all the amplitudes about their mean. Because the sign of the amplitude we want has been reversed, this operation amplifies this amplitude at the expense of the others. This is illustrated below for the case N = 8, L = 3 (Fig. 9).

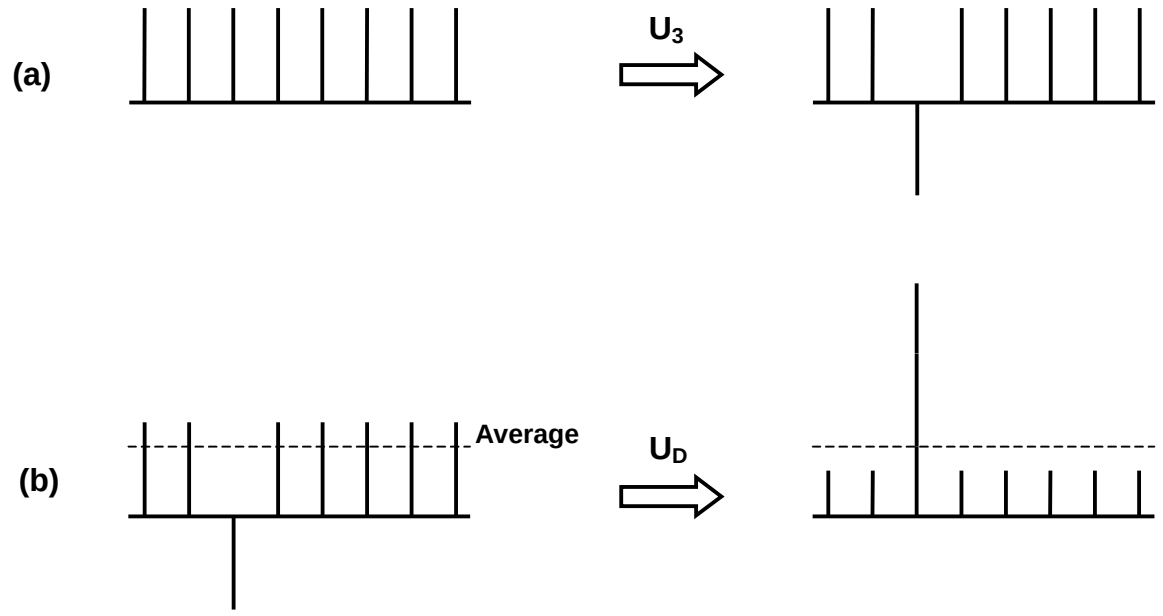


Fig. 9 Representation of amplitudes and operators for N=8 L=3 Grover Search.

(Assumed marked bit is m=3.)

Boyer et al. [23] have pointed out that Grover's algorithm is one of a general class of ‘amplitude enhancement’ quantum algorithms.

What uses could there be for Grover's algorithm? It will not be very useful for searching a conventional database since it would first be necessary to transfer all the data into a quantum database and this in itself is an O(N) operation. However, it could be effective in cryptoanalysis. In the DES encryption system, the security is ensured by the time required to search a large array of keys. Using Grover's algorithm, a quantum computer could reduce the search time from thousands of years to minutes.

7. EXPERIMENTAL QUANTUM COMPUTING: STATE OF THE ART

This is fast moving field and several different physical realisations of quantum logic gates are being explored by groups in many different countries. The front-runners at the moment are ion traps, cavity QED and NMR ‘ensemble’ quantum computing. The group of David Wineland in Boulder have recently demonstrated a realisation of a CN gate using the two lowest energy levels of two Be ions to realise the two qubit states [24]. The ions are confined in a linear array in an ion trap and cooled to very low temperature using laser cooling techniques. The coupling between the two ions is provided by the vibrational modes of the two ions and Wineland and his group have successfully cooled the system to its vibrational ground state to implement a CN gate. The Caltech group have used an atom interacting with photons in a cavity to demonstrate conditional phase rotations for a two qubit system [25]. Both these approaches attempt to manipulate individual qubits directly. By contrast, an approach using conventional NMR machines manipulates many molecules in bulk. There is no direct control of the qubits of individual molecules but clever manipulation of the NMR operations allows one to effectively isolate pure qubit states. Several groups have investigated quantum systems containing two or three qubits [26-28]. More recently, Jones and co-workers in Oxford have successfully implemented both Grover's and Deutsch's algorithms on a two qubit system [29, 30]. Although it seems clear that it will be possible to build and implement quantum algorithms on small numbers of qubits using these technologies, it is by no means clear that any of these will scale to the sort of numbers required for factorizing large numbers.

Most recently Paul Kwiat and co-workers at Los Alamos National Laboratory have implemented Grover's search algorithm using conventional optical interferometers [31]. In this realisation the two qubits are the two photon polarizations and the two directions through the interferometer. Thus although one can demonstrate quantum gates and algorithms using this technique, no multi-particle entanglement is involved. It is therefore no surprise that increasing the number of qubits using this approach requires exponentially increasing resources.

Several authors have speculated about using solid state devices such as quantum dots or SQUIDs but there seem to be great difficulties in both the control and readout of individual qubits and also in isolating the quantum ‘system’ from the ‘environment’. This last problem is the ‘decoherence’ problem. The coupling to the environment sets bounds to the length of time one can allow the quantum computer to calculate and keep meaningful phase relations between the different states. An exciting futuristic but potentially feasible scheme using carefully positioned phosphorus impurity nuclei in isotopically pure silicon semiconductor has been proposed by Kane [32]. It will be some years, if ever, before such an approach delivers a working quantum computer.

8. CONCLUSIONS

There are many exciting avenues to be explored involving computer scientists, quantum physicists and electronic and photonic engineers. One example has been provided by Butler and Hartel at Southampton [33]. They have shown how Grover's search algorithm can be expressed in terms of a probabilistic version of Djikstra's wp calculus and derived closed forms for its convergence. Another example is the new field of ‘quantum compilers’! Quantum compilation is the business of translating an abstract quantum algorithm down to operations in a given implementation technology. For NMR, for example, a Hadamard transformation must be translated into a specific set of NMR magnetic field pulses.

As we have seen, the extraordinary power of quantum algorithms seems to be derived from the properties of multiparticle entangled states. This is where the peculiar non-local behaviour of

quantum mechanics enters the game. In addition, for a practical quantum computation to survive interactions with the environment and tolerate slightly inaccurate quantum gate operations, the question of error correction must be addressed. Surprisingly, Shor [34] and Steane [35] have independently proposed schemes that show that quantum error correction is indeed possible in principle - something that had hitherto been doubted. Again, entanglement is at the heart of these error correction schemes.

In his 1981 talk [14] in which he first proposed the idea of a quantum computer, Feynman confessed that he was "not sure if there is a real problem with quantum mechanics." He was also not clear whether quantum computers could be made or would ever do anything useful. But he thought that quantum computation was a wonderful problem to "squeeze the difficulty of quantum mechanics into a smaller and smaller place." Since quantum computation relies so heavily on the non-local aspect of quantum theory we can extend and stress the theory in new and exciting ways. We may have the foundations of a new multibillion industry or we may find the first clues towards a theory that may eventually supplant quantum mechanics! Both possibilities are exciting.

REFERENCES

[1] R.Landauer, 'Information is Inevitably Physical', published in 'Feynman and Computation' edited by Anthony J.G.Hey (Addison Wesley Longman, Reading MA 1998).

[2] J.A.Wheeler, 'Information, Physics, Quantum: The Search for Links', reprinted in 'Feynman and Computation', ibid.; originally published in Proceedings of 3rd Int. Symp. Foundations of Quantum Mechanics, Tokyo, p. 354 (1989).

[3] A.J.G. Hey and P. Walters, 'The Quantum Universe' (CUP, Cambridge 1987).

[4] M. Minsky, 'Richard Feynman and Cellular Vacuum' published in 'Feynman and Computation' ibid.

[5] R.P. Feynman, 'There's Plenty of Room at the Bottom', reprinted in 'Feynman and Computation', ibid.; originally published in February 1960 issue of Caltech's Engineering and Science.

[6] C.H. Bennett, 'Logical Reversibility of Computation', IBM J. Res. Dev. 17 (1973) 525.

[7] R. Landauer, 'Irreversibility and Heat Generation in the Computing Process', IBM J. Res. Dev. 5 (1961) 183.

[8] C.H. Bennett, Int. J. Theor. Phys. 21 (1982) 905.

[9] A.J.G. Hey and R.W. Allen, eds., 'The Feynman Lectures on Computation', (Addison Wesley Longman, Reading MA 1996).

[10] E. Fredkin and T. Toffoli, Int. J. Theor. Phys. 21 (1982) 219.

[11] E. Fredkin, unpublished lecture given at Southampton in September 1997.

[12] D. Harel, 'Algorithmics', Addison-Wesley, Reading MA, 2nd edition (1992).

[13] D. Deutsch, Proc. Roy. Soc. A400 (1985) 97.

[14] R. P. Feynman, 'Simulating Physics with Computers', reprinted in 'Feynman and Computation', ibid.; originally published in Int. J. of Theor. Phys. 21 (1982).

[15] P.W. Shor, 'Algorithms for quantum computation: discrete logarithm and factoring', in Proc. 35th A. Symp. on the Foundations of Computer Science, p124, edited by S.Goldwasser (IEEE, Los Alamitos, CA.), 1994.

[16] R.J. Hughes, ‘Cryptography, quantum computation and trapped ions’, Phil. Trans. Roy. Soc. 356 (1998) 1713.

[17] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. 47 (1935) 777.

[18] D. Bohm, Phys. Rev. 85 (1952) 166.

[19] J.S. Bell, Physics 1 (1964) 195.

[20] A. Aspect, J. Dalibard and G. Roger, Phys. Rev. Lett. 49 (1982) 1804.

[21] C.H. Bennett et al., Phys. Rev. Lett. 70 (1993) 1895.

[22] L.K. Grover, Phys. Rev. Lett. 79 (1997) 325.

[23] M. Boyer et al., Los Alamos e-Print xxx.lanl.gov (1998).

[24] D.J. Wineland et al., Phys. Rev. A50 (1994) 67.

[25] Q.A. Turchette et al., Phys. Rev. Lett. 75 (1994) 4710.

[26] D.G. Cory, A.F. Fahmy and T.F. Havel, Proc. Natl. Acad. Sci. USA 94 (1995) 1634.

[27] N.A. Gershenfeld and I.L. Chuang, Science 275 (1997) 350.

[28] R. Laflamme et al., Los Alamos National Lab. e-Print xxx.lanl.gov (1998).

[29] J.A. Jones and M. Mosca, J. Chem. Phys. 109 (1998) 1.

[30] J.A. Jones, M. Mosca and R.H. Hansen, Oxford e-Print xxx.lanl.gov (1998).

[31] P.G. Kwiat et al, Los Alamos e-Print xxx.lanl.gov (1998).

[32] B. Kane, Nature 393 (1998).

[33] M. Butler and P. Hartel, Southampton e-Print xxx.lanl.gov (1998).

[34] P.W. Shor, Phys. Rev. A52 R2493 (1995).

[35] A. Steane, Proc. Roy. Soc. London A452 (1996) 2551.