The promise of quantum computing*

E. C. G. Sudarshan

I present an overview of the paradigm of quantum computing that is emerging as a result of recent advances in a variety of fields, including fundamentals of quantum mechanics, information theory, quantum optics and atomic physics. The essentials of a practical quantum computer are discussed and a few algorithms that may be implemented on such a computer are presented. The advantages of quantum computers over classical ones are touched upon. A brief discussion on quantum teleportation and entanglement is also included in this article.

THE past half century has seen the digital computer which used to be only a scientific aid, develop into a consumer appliance; today almost all commercial and even personal activities are dominated by the computer and computer-aided gadgets. Thus the Y2K was a matter of great concern for everyone. It appears that we have transcended all those troubles.

Digital calculating aids have been known for a long time. When the numbers used exceeded the number of digits of the hand it became necessary to use other aids. Some of them, particularly cowrie shells are used even today by astrologers computing the data for the *panchanga*, the five-limbed calendar-ephemeris. Other countries have used the abacus. Some of us were taught how to do operations on large numbers mentally. In addition to digital computation, analogue computation was also done mainly using the versatile slide rule.

Today 'computation' refers not only to arithmetical operations on numbers but any process in which an 'input' and a 'program' will yield an 'output'. This could be data retrieval, algebraic calculations or producing a word processed document. We can now also use the computer to transmit, edit and modify text as well as graphics. At the same time elaborate computer programs like *Mathematica* seem almost human in their ability to calculate and display the solutions of complicated problems.

The progress in the computing power of computers has been phenomenal. When I was a graduate student in the late fifties, the most powerful computer in our university was the IBM650 with its inevitable bunch of punched cards. Today hand-held calculators can do far more. The supercomputers like the Cray can do the incredible amount of number crunching needed for problems like weather prediction in meteorology or computer-aided design of airframes and other complicated machines. One of the methods of speeding up these computations is to use 'parallel processing' where a number of different but similar calculations are carried out simultaneously.

Underlying our success in vastly improving the variety and the allowed complexity of the problems that can be tackled using modern digital computers is the question: are all problems computable? This question has received considerable attention over the past century leading up to the Church–Turing hypothesis. There are two aspects to the Church–Turing hypothesis. One is the definition of problems that can be regarded as 'computable', the other is a sweeping statement about the means by which a 'computable' problem can indeed be 'computed'.

The answer to the question whether all problems that we can imagine are computable is in the negative as demonstrated by Gödel[1]. He showed that in every arithmetizable framework there are propositions which cannot be either proved or disproved from within the framework. In other words the truth (or falsehood) of certain propositions cannot be verified through a computation. So we must be modest in our attempts to compute: only the class of computable problems must be attempted. Apart from problems that are in principle not computable we must identify those that are not computable due to the sheer complexity of the computation involved. For instance, there are some physical processes displaying such a degree of complexity that the system is its best computer in the sense that no simulation can predict or even keep track of the complex evolution for any reasonable amount of time.

Even if we are modest and consider only computable problems we have to keep in mind the practical question of how much time (or how many computational steps) are needed to carry out the computation. For a problem with N input elements the time may grow exponentially with N making the very complex computation practically impossible. For simple problems one expects that the time need grows only as some power of N; these problems belong to a class of problems called **P**-computable[2]. Even

*Based on the Millennium lecture presented at the Indian Science Congress, Pune, India in December 2000.

E. C. G. Sudarshan is in the Department of Physics, University of Texas, Austin, TX 78712, USA
e-mail: sudarshan@physics.utexas.edu

for some of the problems in the class **P**, the time required might be too long as anyone looking up a particular phone number in a city telephone directory would know. One could have a $\sqrt{N}$ or a $\log(N)$ dependence. Such methods (algorithms) of computation are more desirable. There are a class of problems that are not **P**-computable. They are broadly referred to as **NP**-problems. For **NP** problems the time required for the computation scales exponentially (or faster) with the number of inputs N. Note that even with modest amounts of parallel computing power it is not possible to reduce an **NP** problem to a **P** problem.

The Church–Turing hypothesis states that any problem that is computable (in the sense that it belongs to the class **P**) can be computed using a very rudimentary computational device called a Turing Machine[3,4]. The basic Turing Machine consists of a long ticker tape filled with a long sequence made up of a limited variety of symbols, a read–write head that runs over the tape and a device with a fixed number of internal configurations connected to the read–write head. The hypothesis states that any computable problem can be reduced to a form in which the ticker tape machine with the limited number of internal states and a set of instructions that decides what the state is and what the read–write head should do next as the ticker tape moves through can perform the computation. The instruction set in the Turing Machine is the analogue of the software in modern-day computers. Turing's thesis suggests that the complexity of the computation is independent of the means using which it is performed. The modern digital computer which uses nothing more than just two symbols, 0 and 1, to perform a wide variety of computational tasks is in itself an excellent validation of the hypothesis. The Turing machine can always be made reversible by construction leading to the conclusion that any computable problem can always be computed in a *reversible* fashion. There are further refinements and extensions of Turing's idea for classical computers which include probabilistic computation and so on which I will omit in this discussion[5].

Quantum mechanics and quantum computation

From the discussion on Turing machines we recognize that in the end all classical computers deal with only binary bits, a two level register with 0 and 1 as the possible states. As mentioned before, problems can be reduced to strings of zeroes and ones. We map all the data and all the instructions in the computer into such strings. There is the possibility of going from using integers as the basic units on which the computation is done to complex numbers by using as elements quantum bits or *qubits*[6]. A qubit is the state of a two-level quantum system. These are represented by complex vectors of unit norm. We write

$$\psi = \begin{pmatrix} a \\ b \end{pmatrix}; \qquad |a|^2 + |b|^2 = 1.$$

If we write $a/b = z$ then $|b|^2(|z|^2 + 1) = 1$ or $|b|^2 = 1/(1 + |z|^2)$ so that the vector becomes

$$\psi = \frac{e^{if}}{\sqrt{1+|z|^2}} \begin{pmatrix} z \\ 1 \end{pmatrix},$$

so that ϕ is indeterminate. We could equally write

$$\psi = \psi^0 . e^{if}; \qquad \psi^0 = \frac{1}{\sqrt{1+|z|^2}} \begin{pmatrix} z \\ 1 \end{pmatrix}.$$

The pair (z, ϕ) defines the vector $(a, b)^T$ with three $(3 = 2 \times 2 - 1)$ parameters. Since only scalar products

$$(\psi, \psi') = (a^*, b^*) \begin{pmatrix} a' \\ b' \end{pmatrix},$$

are relevant physically, it follows that only *differences* of ϕ are relevant.

Since a complex number z is needed to define a quantum state, and hence a qubit, we have infinitely more variability than the state for a classical system with 0, 1 (or in the more general stochastic computer, a number p, $0 \le p \le 1$). This is one of the advantages of quantum elements, but not the most important. They are the possibility of *amplitude division* and of *entanglement*, both absent for classical particle systems.

If we have two qubits each having the states $|0\rangle$ and $|1\rangle$ then the state $|0\rangle.|1\rangle$ in which the first qubit is excited and the second qubit is not excited can be transformed by a reversible unitary transformation to

$$\frac{1}{\sqrt{2}}(|1\rangle|0\rangle + |0\rangle|1\rangle),$$

dividing the amplitude of the first qubit and delivering to the second. We could do it for N qubits to obtain

$$\frac{1}{\sqrt{N}}\{|1\rangle|0\rangle|0\rangle...|0\rangle + |0\rangle|1\rangle|0\rangle...|0\rangle + ... + |0\rangle|0\rangle|0\rangle...|1\rangle\}.$$

This is amplitude division.

We can also deal with two qubits and we have a product state like the one above, i.e.

$$\frac{1}{\sqrt{2}}(|1\rangle|0\rangle \pm |0\rangle|1\rangle).$$

This state is *entangled* since both the + and the – states have the same individual qubit states that are correlated and superposed but the phases of the superpositions are different. This information of the two qubit system is not contained in the state of either one separately.

The qubit may be realized by a spin 1/2 particle, or by a two level atom. If it is a spin 1/2 particle the natural method is to have a liquid in which the spin 1/2 objects are suspended. This liquid NMR[7] is a convenient method when one is only interested in the states of a spin 1/2 ensemble; and it may be used as an adaptation of classical parallel processing (See below for an application to encrypting very large numbers). The two level atom may be in a cold atomic trap to preserve the phase relations and to reduce external noise. The technique of handling one or more cold atoms in a trap (even to the extent of realizing Bose–Einstein condensation) are now available in many laboratories.

Quantum algorithms

Deutsch and Jozsa

There are problems that take exponential time to do using classical computers but which can be **P**-computable on a quantum computer; two such problems were described by Deutsch and Josza[8] in 1992. For a function f from Z_{2^N} (the integers from 0 to 2^N–1) to Z_2 (yes, no) for a large N the problem is to establish the truth value of the following two alternatives allowed for the function f: (A) f is not a constant (at 0 or 1); (B) $f(0)$, $f(1)$,…, $f(2N)$ does not contain exactly N zeroes.

For any f, at least one of (A) or (B) has to be true. It may be that both of them are true. We require that the computation (quantum or otherwise) return an answer with certainty if only one of them is true.

The method of solution makes use of quantum parallelism. We start a state of the form $|0\ 0\rangle$ where the two zeroes denote two registers of qubits in which all the qubits are set to the zero state. The first register should be big enough to accommodate all the numbers from 0 to $2N$–1 while the second register, for this problem, has to have only one qubit. We use a transformation called the Hadamard–Walsh transformation to take this initial state to a superposition of states of the form

$$|\boldsymbol{j}\rangle = \frac{1}{\sqrt{2N}}\{|0,0\rangle + |1,0\rangle + |2,0\rangle + ... |2N-1,0\rangle\}.$$

If $2N$ is a power of two, this operation can be done in $(\log N)$ steps. In matrix form, the Hadamard transformation is given by

$$M = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix};\quad M\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix};\quad M\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{pmatrix}. \tag{1}$$

The states $|0\rangle$, $|1\rangle$, $|2\rangle$… (or equivalently $|000\ldots0\rangle$, $|000\ldots1\rangle$, $|000\ldots10\rangle$… in binary) to which the first register $|x\rangle$ is set to is called the *computational basis*.

We now identify a unitary transformation U_f, called the 'Oracle' for the function f such that

$$U_f\,|i, 0\rangle = |i, f(i)\rangle.$$

U_f acting on the linear superposition of states $\boldsymbol{j}$ obtained from the initial state gives

$$U_f\,|\boldsymbol{j}\rangle = \frac{1}{\sqrt{2N}}\{|0, f(0)\rangle + |1, f(1)\rangle + |2, f(2)\rangle + ... |2N-1, f(2N-1)\rangle\}.$$

Next, we need an element S which changes the phases of the individual state vectors so that

$$\boldsymbol{S}|j, f(j)\rangle = (-1)^{f(j)}\,|j, f(j)\rangle.$$

Then

$$\boldsymbol{S}U_f\,|\boldsymbol{j}\rangle = \frac{1}{\sqrt{2N}}\sum_{j=0}^{2N-1}(-1)^{f(j)}\,|j, f(j)\rangle.$$

Using $U_f^2\,|j, 0\rangle = |j, 0\rangle$ we get

$$U_f\boldsymbol{S}U_f\,|\boldsymbol{j}\rangle = \frac{1}{\sqrt{2N}}\sum_{j=0}^{2N-1}(-1)^{f(j)}\,|j, 0\rangle = |\boldsymbol{y}\rangle.$$

Then compute

$$c = |\langle \boldsymbol{j}\,|\,\boldsymbol{y}\rangle| = \frac{1}{2N}\sum_{j=0}^{2N-1}(-1)^{f(j)}.$$

$c = 1$ only when $f(j)$ is a constant, i.e. (A) is false and $c = 0$ only when one $f(0)$, $f(1)$ …, $f(2N-1)$ has exactly N zeroes, i.e. (B) is false. This means that the projection operator $|\boldsymbol{j}\rangle\langle\boldsymbol{j}|$ in the state $|\boldsymbol{y}\rangle$ returning the values 0 and 1 are the determining cases. So each computation gives one or the other conclusion. The measurement of $|\boldsymbol{j}\rangle\langle\boldsymbol{j}|$ in the state $|\boldsymbol{y}\rangle$ can be done in $(\log N)$ steps. This is to be compared with the possibly $N + 1$ trials required in the worst case if we were to compute $f(j)$ using a classical computation to establish the truth values of (A) and (B). What is important to note is that in the quantum case the oracle U_f is invoked precisely two times while in the classical case it may have to be invoked up to $N + 1$ times. It follows that if the oracle U_f has size $p(\log N)$ then the classical computer requires (e^N) steps while the quantum computer requires only polynomial $p(N)$ steps.

One can object that these are artificial, 'manufactured' problems. This is true, but it illustrates the power of quantum computing. To make more converts to quantum computing we need the solution to some more realistic problems. These are provided by three 'classic' problems and their quantum algorithms. (1) The Grover algorithm for *searching a large database* for a specific element (like a phone number or a name in the phone book). (2) The Shor algorithm for *factorizing very large numbers* and (3) The Chinese remainder theorem for encrypting very large numbers *beyond the word size* in the memory. We outline these briefly.

Grover's algorithm

Grover's algorithm[9] searches a large database for a particular element. It is a reversible computation that gradually builds up the probability for the element that we are searching for. The database search problem is very much like trying to find her name and address from the phone book if all that she has given you is her phone number.

The database that we want to search is of size N. Out of the N elements we have to find the element w. Classically if we pick one element from the database at random, the probability of it being w is $1/N$. We have to query the database at least $N/2$ times to get a fifty fifty chance of obtaining the element we want. Using a quantum algorithm we can reduce the number of queries that are needed to a certain extent. Unlike in the previous case the speedup provided by using quantum algorithms is not exponential.

In the case of Grover's algorithm also we assume that we have at hand an *oracle* or a unitary operator $U_w(x)$ which computes the characteristic function $c(x)$ for any input x: $c(x) = 1$ if $x = w$ and $c(x) = 0$ otherwise. We start off with the state $|0, 0\rangle$ again with the first register big enough to represent the largest element, N–1 in our database. The second register contains only one qubit. This initial state is transformed by Hadamard transformations (1) on the individual qubits to

$$|f\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}} \right), \tag{2}$$

in (log N) steps. Note that the second register in this case is initialized to a different (singlet) state rather than to $|0\rangle$.

The oracle U_w has the action

$$U_w|i, j\rangle = |i, j \oplus c(i)\rangle,$$

where $\oplus$ denotes the *exclusive or* operation ($0 + 0 = 1 + 1 = 0$ and $1 + 0 = 0 + 1 = 1$). Then

$$U_w |f\rangle = \frac{1}{\sqrt{N}} \left\{ \sum_{i \neq w} |i\rangle \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}} \right) - |w\rangle \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}} \right) \right\}. \tag{3}$$

This follows from

$$\frac{|1 \oplus 1\rangle - |0 \oplus 1\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = -\frac{|1\rangle - |0\rangle}{\sqrt{2}}.$$

The action of U_w on the vector $|f\rangle$ is to flip the sign of only the component along the direction of the desired element $|w\rangle$. This amounts to reflecting the vector $|f\rangle$ in the N dimensional Hilbert space about the hyperplane that is orthogonal to the vector $|w\rangle$. All we know at this stage is that the oracle performs such a reflection for some value of $|w\rangle$. The value of w itself is unknown to us and that is what we have to find out by consulting the oracle a minimum number of times.

We now construct another operator U_s that does a reflection in which the component of the vector $|f\rangle$ along $|s\rangle$ is preserved while the signs of the component in the hyperplane perpendicular to $|s\rangle$ is flipped. One iteration of the Grover's algorithm is the unitary transformation

$$\mathbf{R}_{\text{grov}} = U_s U_w, \tag{4}$$

one query to the oracle followed by our reflection. The action of one iteration of the algorithm on the state $|f\rangle$ is to rotate its component along $|s\rangle$ by an angle 2θ away from the hyperplane perpendicular to $|w$ where θ is the angle between the vectors $|s\rangle$ and $|w\rangle$. Successive iterations with various choices of $|s\rangle$ brings the vector $|f\rangle$ progressively closer to $|w\rangle$ and away from the hyperplane perpendicular to $|w\rangle$.

We can estimate that the number of queries of this sort required to get the correct value of $|w\rangle$ with high probability when $|f\rangle$ is measured after the iterations is about $\frac{\pi}{4}\sqrt{N}$. This is a quadratic speedup relative to the classical computation.

Shor's algorithm

Shor's algorithm[10,11] uses a period finding routine to find a method of factorizing large numbers in polynomial time. Given a large number N which can be factorized into exactly two large prime numbers, classically we might have to exhaustively test out all the numbers from 1 to $\sqrt{N}$ to find the factors.

The factorization problem is reduced to a period finding problem by the following observation. We randomly pick a number $a < N$ such that $a^r = 1 (\text{mod } N)$ for some even integer value of r. It can then be shown that N shares a common factor with $a^{r/2} + 1$ or $a^{r/2} - 1$ for most choices of a. Once we find r (which is usually an even number) then using the classical Euclid's algorithm it is

easy to find the common factor of N and $a^{r/2} \pm 1$ which solves the problem of factorizing N.

To reduce the problem of finding r to period finding problem we do the following. We choose as the function that we want to evaluate,

$$f_{N,a}(x) = a^x \pmod N. \tag{5}$$

Since $a^r = 1 \pmod N$ the period of the function $f_{N,a}(x)$ is r.

We can evaluate the function $f_{N,a}$ on a state $|f\rangle$ initialized as in the case of Grover's algorithm to

$$|f\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i, 0\rangle.$$

The only difference here is that the second register is big enough to hold $f_{N,a}(i)$. We can now construct a unitary operation (oracle) $U_{f_{N,a}}$ such that

$$U_{f_{N,a}} |f\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i, a^x \pmod N\rangle = |y\rangle.$$

The second register contains a function with period r so if we make a measurement on the second register and obtain a value $|u\rangle$ then that will collapse the first register to a linear combination of all the values of x that give $f(x) = u$. Because of the periodicity of the function these values of x have the form $x_0 + jr$, where $j = 0, 2 \ldots x_{\max}/r$ and $f(x_0) = u$. $x_{\max}$ is the biggest number that can be contained in the first register. For simplicity we assume here that $t = x_{\max}/r$ is an integer. The measurement reduces the state $|y\rangle$ to

$$|j\rangle = \frac{1}{\sqrt{x_{\max}/r}} \sum_{j=0}^{x_{\max}-1} |x_0 + jr\rangle |u\rangle. \tag{6}$$

We can now implement a quantum Fourier transform on the first register of the state $|j\rangle$ to obtain the value of r. The quantum Fourier transform can be implemented efficiently and it has the following effect on $|j\rangle$

$$U_{FT} |j\rangle \rightarrow \sum_k \tilde{f}(k) |k\rangle |u\rangle, \tag{7}$$

where $\tilde{f}(k) = 1$ if k is a multiple of $x_{\max}/r$ and zero otherwise. If we measure the first register then the value of k obtained has the form $k = l \frac{x_{\max}}{r}$. Both l and r are unknown but in the cases where l and r have no common factor we can reduce $k/x_{\max} = l/r$ to an irreducible fraction to read off the values of r and l. If l and r do share a common factor then the algorithm fails and we will have to repeat it with a different value of a to start off with. Even with the possibility of having to repeat the algorithm to get to the correct factor it is possible to show that it takes only $(\log N)$ steps to run the algorithm enough number of times to get the right answer with certainty. This is still *exponential speedup* compared to the classical algorithm.

Chinese remainder theorem

Suppose we are given the remainders $r_0, r_1 \ldots, r_{n-1}$ when a number N is divided by $m_0, m_1 \ldots, m_{n-1}$ where all m_i are pairwise relatively prime (no two share a common factor). The Chinese remainder theorem[12] tells us that modulo the product $m = m_0 \times m_1 \times \ldots \times m_{n-1}$ we can reconstruct N from the knowledge of the divisors and the remainders. If sufficient number of m_i are given so that $N \leq m$ then N is determined uniquely.

For example if we have a number x such that

$$x = 2 \bmod 3, \quad x = 3 \bmod 5, \quad x = 2 \bmod 7,$$

then to find x we do the following. Find three numbers s_0, s_1 and s_2 such that each of them give a remainder of 1 when divided by exactly one of the divisors of x while giving a remainder 0 when divided by all the other divisors. In this example

$$s_0 = 70 = 1 \bmod 3 = 0 \bmod 5 = 0 \bmod 7,$$

$$s_1 = 21 = 0 \bmod 3 = 1 \bmod 5 = 0 \bmod 7,$$

$$s_0 = 15 = 0 \bmod 3 = 0 \bmod 5 = 1 \bmod 7.$$

Multiply each s_i by r_i (r_i is the remainder when x is divided by that divisor which has remainder 1 with s_i). So we get $140 = 2 \times 70$, $63 = 3 \times 21$ and $30 = 2 \times 15$. Then the Chinese remainder theorem tells us that $140 + 63 + 30 = 233$ is x modulo $105 = 3 \times 5 \times 7$. In this example, $x = 233 \bmod 105 = 23$.

The application of the remainder theorem is in quantum cryptography more than in computing. Large number can be encoded into small registers (smaller word size) by recording only the divisors and the remainders rather than the large number itself and then reconstructing the number from this knowledge. These smaller registers of qubits are easier to transmit through some sort of quantum communication channel. Truly quantum communication channels, in turn, can provide absolute security in the transmission of confidential data because the very nature of quantum systems makes sure that they cannot be observed without disturbing them. So any eavesdropping on the communication channel can, in principle, be always detected.

Quantum gates

The effectiveness and usefulness of the quantum algorithms that we have seen lies not only in the exponential speedup of the computation but also in the fact that they can be implemented using a sequence of operations on a few qubits at a time. Controlled operations on entire registers of qubits at one shot is not only near impossible but also not in line with the spirit of Turing's ticker tape machine that does operations on only one individual cell in the tape at a time. Going a step further it can be shown that not even all possible one qubit and two qubit operations are required to build a network that implements quantum algorithms. The few one, two and sometimes three qubit operations using which all the algorithms can be implemented are called *universal quantum gates*.

We have already encountered one such universal gate: the Hadamard transformation given in eq. (1). The Hadamard gate acts on a single qubit and its effect is to rotate the state about the *y* axis. (It is rotation about the *y* axis only if we follow the usual convention and choose to represent our qubit in terms of the eigenstates of the spin operator oriented about the *z* axis.) In symbolic form we can represent the Hadamard gate as shown in Figure 1.

Another useful gate is the controlled not (CNOT) gate. This is a two qubit gate that modifies the state of one of the qubits depending on the state of the other (control) qubit. The CNOT gate is shown in Figure 2. The action of the CNOT gate on the two qubits is the same as the classical XOR (exclusive OR) gate. Depending on the values of the inputs A and B we get the following outputs: $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$ and $1 \oplus 1 = 0$. Since the state of the second qubit is now dependant on the state of the first qubit, the two qubits become entangled on passing through the CNOT gate. By using a combination of the CNOT gate and the Hadamard gate we can achieve both quantum superposition and entanglement.

The *Toffoli* gate is an extension of a CNOT gate which acts on three qubits, modifying the state of the third qubit based on the states of the first two. Sometimes it is called the C^2NOT gate. The Toffoli gate is shown in Figure 3.

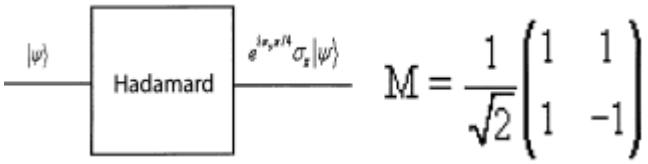

Figure 1. The Hadamard gate.

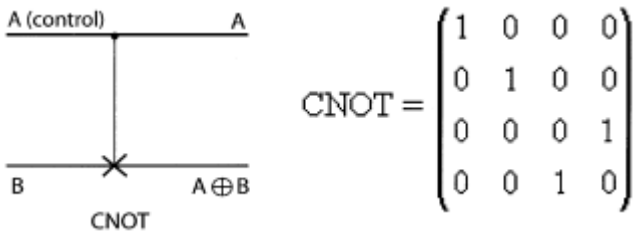

Figure 2. The CNOT gate ($A \oplus B$ stands for B XOR A).

Building a working quantum computer

Since the superposition of amplitudes with their phases is involved in any quantum computation, it is important to deal with any *phase decoherence* by external perturbation. So to maintain the integrity of the computation we need to make use of error correcting codes. Such a program has been experimentally realized last year with a 3 qubit code[13].

It is in principle possible for any system with superposition of linear complex amplitude to be appropriate for implementing a quantum computer. In particular, wave optics[14,15] is a natural choice. We may then recognize that we have *already carried* out simple *quantum computations with light*: like in X-ray diffraction of crystals, Michaelson interferometry, the Zernike phase contrast microscopy and in optical holography. With its two polarization states, *a thin pencil of light is a qubit*. When monochromatic light of wavelength λ propagates through an aperture of area A, approximately A/λ^2 pencils pass through and all of them maintain constant relative phases. So we automatically get a coherent register of A/λ^2 optical qubits. In trying to locate and study a thin transparent microbe using phase contrast microscopy, we make use of only the independent pencils and superposition of the signal beam with a phase shifted reference beam. This maybe thought of as a search of a large database, the field of illumination, for the specific small set 'the microbe occupied patch'.

Quantum gates can be constructed using optical elements; so also the processes corresponding to quantum computing can in principle be done using wave optics. This includes the error-correcting codes[16] so necessary for reliably serial quantum computing.

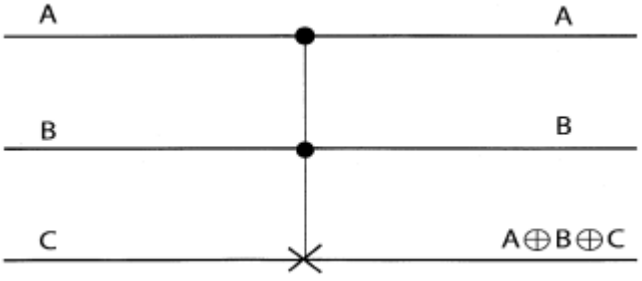

Figure 3. The Toffoli gate.

Quantum teleportation

Another area closely related to quantum computing is quantum teleportation[17]. This makes use of quantum entanglement in which a pure state of a composite system differs from the product of pure states of the components of the system. These days we call them EPR states[18]. Using such a state shared by two experimenters Appu and Ammu, they can do non-classical transmission of quantum states. If Ammu receives a signal not known to her (she does not 'measure' it) she can superpose this on her half of a EPR state. Since the EPR state is shared by the two of them, when Ammu does the superposition that modifies the whole state including the half that Appu has with him. Ammu can now measure the combined state of the signal and her half of the EPR pair without actually ever measuring the signal itself. If this information is then provided to Appu through a classical channel like a telephone line, Appu can combine his half of the EPR state with a blank register and then modify this combined state to one in which the blank register becomes the input state that Ammu originally received.

The input state is thus effectively teleported via a combination of quantum (EPR) communication channels and a classical channel. The transmission is done without either person knowing what exactly the (perhaps secret) input signal was. This process of transferring a quantum state from one place to another without any actual transportation of matter is called *quantum teleportation*. It is the 'quantum configuration' that is transported from Ammu to Appu. Note that Ammu does transmit non-quantum information to Appu (in that sense it is not *Star Trek* where people are beamed aboard the starship *Enterprise*).

The property of quantum states that are used in teleportation (and computation) is their ability to form superpositions and thus for a composite system to be entangled. The quantum state can be subdivided by *amplitude division* (beam splitting), both copies being the same state. Superposition, entanglement and beam splitting are non classical (non-corpuscular) properties. These properties are reminiscent of the couplet:

भिन्ने कुम्भे यत्याकाशं ।
ततास्मिे परमात्मानी ॥

(*As the sky is reflected in many pots, so does the individuated awareness in the Absolute awareness*) and:

वागर्थविव संप्रक्तौ वागर्थ प्रतिपत्तये ।
जगत पितरौ वन्दे पार्वती परमेस्वरौ ॥

(*Let word and meaning be so joined indivisibly so as to present the meaning of the words, so do I pay homage to Parvati and Parameswara, the progenitors of all the world*.)

Concluding remarks

This is the transition period between two millennia – *yugaparivarthanam*. Tradition has it that at such transition times the *sandhyas* are ideal for new insights (*sandyavandanam*). Rsí Patanjali says that we must seek to attain the intellect undisturbed by noise and chaos to get greater insights. It is therefore appropriate that we invoke quantum computing at this time.

The coming together of the most prosaic, most orderly notion of computation and the most pure discipline of quantum mechanics is seen in the paradigm of quantum computation. The practical applications of quantum computing brings a most esoteric and pure research topic into the information technology arena. Since many of these techniques are adaptable to quantum optics in place of spin assemblies, it may be of particular interest in India.

It has been often said that when we make decisions or learn, we act like a computer; so much so that many people are willing to equate the mind to the brain and then to a complex digital network. But my own observation is that creative processes or moments of insight can rarely be adequately described thus. Insight or creativity is the abstract discipline (and sometimes in the not so abstract discipline – Nobel Prize winner Woodward's doodling) involves a period of apparent gloom when many alternative views are superimposed in thinking. It is in this *domain of superposition* of pictures that *sudden insight illuminates*.

निरस्थ सर्वसंदेहं एकीकृत्य सुदर्शनं ।
रहस्यं यो दर्शयति भजामि गुरुमीदवरं ॥

(*I pay homage to that entity (the guru) which banishes all doubts, joins all perspectives and thus enables secret knowledge to be accessible.*)

It is not only in such profound situations but also in routine activities that such superpositions occur: when you are just about to go to the university you hesitate between two neck ties: like Buridan's ass one could pass a long time without being able to decide. Similarly very reminiscent of Grover's algorithm (which involves spreading your awareness on a multitude of 'sites') is the 'computation' that you have to perform when you meet a person whom you know and you are trying to make the precise identification. I usually misplace things and look for them classically. My wife, does her searching using the analogous quantum protocol and she usually finds it.

If the 21st century is the century of the science of the mind, it may well be that the lessons learnt from quantum computing may enable us to use the proper protocol for analysing our data and formulating the problems. We may or may not be quantum computers, but we are definitely *not* classical computers.

So to the promise of quantum computing:

1. More powerful computing protocols converting some of the **NP**-computable problems to **P**-computable problems.
2. Faster data search.
3. Quantum teleportation and secure information transport.
4. Merging of the disciplines of quantum mechanics and computer sciences.
5. Possible basis for a beginning of a science of the mind.

Then maybe Mashelkar's dream of the revival of an Indian leadership in science becomes realized.

Appendix: Quantum entanglement

Anil Shaji
University of Texas, Department of Physics, Austin TX 78712, USA

Interactions of any sort between two quantum systems leaves a mark on both of them that persists even if the two systems are prevented from having any further contact with each other. This, of course, is not something unique to quantum systems. Two classical systems that interact with each other; say, through a collision can end up bearing signatures of the interaction for quite a long time. A fende-bender collision between two cars bears the signs of the accident until one spends a bit of money at the mechanics!

The persistent effects of the interaction between two (or more) quantum systems that show up in measurements made on each system even after they are isolated from each other is entanglement. The prototypical system that illustrates the various, often counter-intuitive, aspects of the phenomenon of quantum entanglement is the following:

Imagine that a quantum particle of total angular momentum zero breaks up into two pieces, each carrying spin 1/2. Conservation of angular momentum requires that the state of the system after the original particle has dissociated must be of the form

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle).$$

Here the up and the down arrows represent the components of the spin of the first and the second particle measured along a particular direction (we choose the z-direction).

Even if we assume that the two particles have no further interaction with each other after they are created the two still seem to be inseparably connected by just being in the combined quantum state $|\psi\rangle$. The state $|\psi\rangle$ is a coherent superposition of the two particle states $|\uparrow\downarrow\rangle$ and $|\downarrow\uparrow\rangle$. Consequently, if a measurement on the first particle yields the result that it is in the $|\uparrow\rangle$ state then that means that we have picked up the $|\uparrow\downarrow\rangle$ component of the superposition and therefore the second particle must be in the state $|\downarrow\rangle$. Yet, one could argue that in the original state $|\psi\rangle$ the second particle by itself is in a superposition of $|\uparrow\rangle$ and $|\downarrow\rangle$ states. It is then as if the measurement on the first particle transforms the second particle automatically from a superposed state to a definite spin state. This transformation seems inevitable even if we assume that the second particle is totally isolated from the first particle at all times except at the instant of their creation from the original particle. Without any interaction between the two particles, how is it then possible for the measurement on the first particle to affect the state of the second? Questions like this has been the source of a large amount of discussion[18,19] and endless confusion. We do not discuss these aspects of entanglement here but refer the reader to ref. 20 for details.

Viewed as a single two-particle state, the effects of the quantum entanglement in $|\psi\rangle$ presents no particular conceptual difficulties. Observing the first particle in the $|\uparrow\rangle$ state simply means that we have observed the $|\uparrow\downarrow\rangle$ component of the original superposition. The difficulties come in when we stipulate that a consequence of the fact that the two particles do not interact with each other once they are created is that the result of a measurement on each of them should be understandable in terms of their individual quantum states rather than in terms of the combined state $|\psi\rangle$. Deliberately avoiding such treacherous discussions on the connection between entanglement, causality and the nature of physical reality we merely state that there is sufficient experimental evidence to substantiate the reality of the phenomena of quantum entanglement[21].

From the point of view of quantum computation, entanglement is a potent physical resource that is used in almost all quantum algorithms that we know of. For instance, in Grover's algorithm and Shor's algorithm there is an 'oracle' U_f that has the following action on a specially prepared initial state $|\phi\rangle$:

$$U_f\,|\phi\rangle = U_f \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\,|0\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\,|f(i)\rangle.$$

U_f evaluates the function f onto the second register in $|\phi\rangle$ depending on the state $|i\rangle$ of the first register. In doing so U_f is *entangling* the first and second registers.

In the algorithm, the final measurement is always on one of the registers which in turn 'collapses' the other register of qubits to a desired state. This step depends crucially on the entanglement between the two registers.

Quantum entanglement is of considerable interest in information theory also. It is recognized that the infor-

mation content of an array of qubits depends not only on the states of the individual qubits but also on whether or not the qubits are entangled among themselves. It can be shown that a maximally entangled array of qubits has a greater information content than an equivalent array in which the qubits are not entangled. The problem of characterizing and detecting the degree of entanglement of an array of qubits is still an open one with only a few partial solutions available[22,23].

1. Godel, K., *Monatsh. Math. Phys.*, 1931, **38**, 173–198. For English translation see Godel, K., *On Formally Undecidable Propositions of Principia Mathematica and Related Systems*, Dover Publications, New York, 1992.
2. Papadimitriou, C. H., *Computational Complexity*, Addison-Wesley, Reading, Mass, 1994.
3. Turing, A. M., *Proc. London Math. Soc. Ser.*, 1936, **42**, 230 (see also *Proc. London Math. Soc. Ser.*, 1936, **43**, 544).
4. Penrose, R., *The Emperor's New Mind: Concerning Computers, Minds, and the Laws of Physics*, Oxford University Press, New York, 1989.
5. Hirvensalo, M., *Quantum Computing*, Springer-Verlag, Berlin, 2001.
6. Schumacher, B., *Phys. Rev.*, 1995, **A51**, 2738–2747. For an introduction to qubits and other aspects of quantum computing see Preskill, J., Lecture notes on Quantum Computation available at http://www.theory.caltech.edu/people/preskill/ph229/\#lecture.
7. Ernst, R. R., Bodenhausen, G. and Wokaun, A., *Principles of Nuclear Magnetic Resonance in One and Two Dimensions*, Oxford University Press, Oxford, 1994.
8. Deutsch, D. and Jozsa, R., *Proc. R. Soc. London*, 1992, **A439**, 553–558.
9. Grover, L. K., *Phys. Rev. Lett.*, 1997, **79**, 325–328.
10. Shor, P. W., Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Santa Fe, 1994, pp. 124–134.
11. Steane, A., *Rep. Prog. Phys.*, 1998, **61**, 117–173.
12. Ding, C., Pei, D. and Salomaa, A., *Chinese Remainder Theorem*, World Scientific, Singapore, 1996.
13. Steane, A., *Appl. Phys.*, 1997, **B64**, 623–642. Also available at http://www.arxiv.org/abs/quant-ph/9608011. For recent developments in ion-trap computing see http://www.qubit.org/research/IonTrap/index.html.
14. Born, M. and Wolf, E., *Principles of Optics*, Pergamon Press, New York, 1993.
15. Klauder, J. R. and Sudarshan, E. C. G., *Fundamentals of Quantum Optics*, W. A. Benjamin, New York, 1968.
16. Shor, P. W., *Phys. Rev.*, 1995, **A52**, R2493–R2496. Also see Calderbank, A. R. and Shor, P. W., *Phys. Rev.*, 1996, **A54**, 1098–1105.
17. Nielsen, M. A., Knill, E. and Laflamme, R., *Nature*, 1998, **396**, 52–55.
18. Einstein, A., Podolsky, B. and Rosen, N., *Phys. Rev.* 1935, **47**, 777–780.
19. Bohr, N., *Phys. Rev.*, 1935, **48**, 696–702.
20. Bell, J. S., *Speakable and Unspeakable in Quantum Mechanics: Collected Papers in Quantum Mechanics*, Cambridge University Press, Cambridge, 1987.
21. Baggot, J., *The Meaning of Quantum Theory*, Oxford University Press, Oxford, 1992.
22. Peres, A., *Phys. Rev. Lett.*, 1996, **77**, 1413–1415.
23. Horodecki, M., Horodecki, P. and Horodecki, R., *Phys. Lett.*, 1996, **A223**. Also available at http://xxx.lanl.gov/quant-ph/9605038.

ACKNOWLEDGEMENTS. Substantial assistance by Anil Shaji in the preparation of this paper is acknowledged. I also thank him for the appendix that he has provided.

Received 30 December 2002; accepted 18 January 2003