

## On the Realizability of Quantum Computers

*by Subhash Kak*

Donald C. & Elaine T. Delaune Distinguished Professor of  
Electrical Engineering  
Louisiana State University  
Baton Rouge, LA 70803  
E-mail: kak@ece.lsu.edu

Quantum information science provides important insights into several aspects of the communication and computing process. Single qubits can be used in novel cryptographic protocols. Pairs of entangled qubits can, in principle, have remarkable applications: two bits of classical information may be exchanged using an existing entangled pair with the two parties while transferring only one qubit by means of the protocol of dense coding; and an unknown quantum state may be teleported to another location by use of an entangled pair of qubits and classical bits so long as the entangled qubits do not have any phase uncertainty associated between them [1].

When we go from single and entangled pairs of particles to groups of particles as in various methods of quantum computing, the question of the physical realizability of the mathematical model become a serious issue. For example, the circuit model of quantum computing [2] leaves out problems of state preparation (how to get the individual particles into a precise state using gates that may have imprecision associated with them), particle statistics (indistinguishability of quantum particles of the same quantum state), and effective error correction. It is assumed that once the qubits, each placed into a superposition of 0 and 1 by the use of an appropriate rotation operator, are loaded individually on the n-cell register, Hamiltonians for the subsequent evolution of the set of n-qubits will somehow be found. The physical implementability of the unitary matrices is not addressed. The model of computing also does not address the questions of statistics and error correction.

The quantum Turing machine and the quantum cellular automata models are equivalent to the circuit model and, therefore, face the same difficulties. These models, inspired by the philosophically extravagant many worlds interpretation of quantum mechanics [3], assign specific information to the qubits, postulating gates that

implement the unitary transformation representing the solution to the computational problem.

The quantum circuit model converts the physical problem to a circuit theoretic form but it does not map all the physical constraints required by the laws of quantum mechanics. It gives specific labels to different lines of the circuit and does not consider the question of the indistinguishability of particles in quantum mechanics. This indistinguishability may require constraints additional to the ones that are usually assumed when considering implementation. It is good to remember that "a quantum system is a useful abstraction, which frequently appears in the literature, but does not really exist in nature" [4]. Quantum computing models use selected elements of this abstraction in a manner that may preclude successful physical implementation. If a quantum computing model is not physically implementable, then it should be called a quasi-quantum model. The quantum computing model – like the billiard ball model [5] – is an example of a Hamiltonian system. Several years ago, Rolf Landauer cautioned [6] against the Hamiltonian approach to computation. In contrast to digital computers where data is reset, a Hamiltonian system cannot correct local errors. Quantum error correcting codes have been proposed but they can only correct certain large errors without correcting small errors. Even in theory these codes work only to correct bit-flips and phase-flips, which is a vanishing small fraction of all the phase errors that can occur in the quantum state. Besides successful error correction, coding requires that the error be within bounds, whereas the uncertainty with regard to phase makes that assumption invalid.

The question of decoherence of quantum states is another problem afflicting quantum computation but it does not concern us here. There is also the question of the fundamental limitations of the quantum computing paradigm. Its unitary evolution is unable to perform basic nonlinear mappings. For an unknown state  $x$ , a general unitary matrix  $U$  does not exist which will take  $x_0$  to  $xx$  or vice versa. In other words, an unknown state can neither be copied nor deleted. These operations are nonlinear and they are beyond the capacity of a unitary transformation.

By carrying the input data alongside, one can convert [7] a one-way mapping to a reversible mapping, but that would involve an exponential growth of overhead in any substantial computation and, therefore, this possibility cannot be taken seriously for real computational tasks. As unitary transformations, quantum algorithms

would still be useful in certain problems, but this usefulness would be similar to that of optical computing. Since unitary mappings are rotations on a sphere (of high dimensionality), one can only hope to compute periodicity information or properties that are related to this information.

In this note I list some interrelated issues related to the quantum circuit model. I first review the problems of creating an appropriate pure state to get the computation started and then consider the question of quantum statistics in the context of such a state. The thesis of this note is that "quantum computing" models use the mathematical apparatus of quantum theory but do not appear to incorporate all of its restrictions. If this thesis is correct then one may ask if other mathematical models of distinct computing power exist.

### **On the realizability of the circuit model**

The circuit model of quantum computing provides a schematic realization of the unitary matrix that represents the computation in terms of its sub-matrices. It is implicit that when such transformations are applied to the qubits on the register the evolution will correspond to the quantum evolution given by the Schrödinger equation. This is correct but for the fact that the circuit model takes the qubits to be unique and distinguishable from each other, a condition that maps into the uniqueness of the wires in the quantum circuit. But quantum objects cannot be distinguished amongst each other before measurement. From a practical point of view it imposes severe constraints on the labels that are ascribed to qubits. This could mean that the unitary matrices for certain gates may not be physically realizable. The circuit model may then be seen as an implementation not of quantum physics but of unitary transformations.

In the circuit model the register is loaded with data one qubit at a time where these qubits are independent of each other. Now Hadamard transformation is applied to each qubit. From a practical point of view, due to the imprecision in the implementation of the transformations, this will create a compound pure state with uncertain weights.

In several proposed implementations, the individual qubits themselves are not in a pure state. One must remember that a pure state must yield a predictable outcome in a specified maximal test [8], and no such test may be conceptualized for the qubits on the quantum register in certain practical systems [9].

## Unknown phase

The state function of a quantum system is defined on the complex plane whereas observations can only be real. This means that the state function may not be completely known even if the state is prepared because of the uncertainty associated with the state preparation process itself. In such a situation one cannot hope to characterize this reality with such precision so as to carry out a specific computation using a single quantum state.

In general there may be unknowable phase associated with the qubits [10] making it impossible to rotate this qubit through a precise angle [11].

This may also be seen from the point of view of information. A computation is a mapping from an initial sequence to the solution sequence, where both these sequences may be considered to be binary. In classical computing, small noise added to the initial sequence bits is filtered out using techniques of discretization. But in quantum computing, we face the impossibility of distinguishing between amplitudes which are phase shifted with respect to each other. If the quantum register cannot be properly initialized, the algorithms will not work as desired.

## Error correction

A realistic model of computing must address the problem of random errors. In the circuit model, small errors would creep in state preparation and in the implementation of the gate operations that constitute the unitary transformations. Error correction, intuitively and in classical theory, implies that if

$$y = x + n,$$

where  $x$  is the discrete codeword,  $n$  is analog noise, and  $y$  is the analog noisy codeword, one can recover  $x$  completely and fully so long as the analog noise function  $n$  is less than a certain threshold. If it exceeds this threshold, then also there is full correction so long this does not happen more than a certain number of times (the Hamming distance for which the code is designed) at the places the analog signal  $y$  is sampled.

The hallmark of classical error-correcting codes is the correction of all possible small analog errors and many others which exceed the thresholds associated with the code alphabet. This full correction of all

possible small analog errors is beyond the capability of the proposed quantum error-correcting codes.

This definition of error correction in classical theory is not merely a matter of convention. In the communication process the errors are analog and, therefore, all possible small errors must be corrected by error-correcting codes. To someone who looks at classical error-correction theory as an outsider, it may appear that one only needs to fix bit flips. In reality, small analog errors, occurring on all the bits, are first removed by the use of clamping and hardlimiting.

Since the definition of a qubit includes arbitrary phase, it is necessary to consider errors from the perspective of the quantum state and not just from that of final measurement. Just as in the classical theory it is implicitly accepted that all possible small analog errors have already been corrected by means of an appropriate thresholding operation, we must define correction of small analog phase errors as a requirement for quantum error correction. This is something that the proposed quantum error correction schemes are unable to do [12].

## **Statistics**

Classical particles are distinct whereas quantum particles are indistinguishable if they are part of the same quantum state. Thus it becomes impossible for us to distinguish between 01 and 10 or between 001, 010, and 100, before the measurement is made. But the circuit model considers each particle to carry unique information, albeit in a superposition. The model does not consider boson/fermion statistics [13] which prevent the identification of a qubit with any specific atom or particle within the system. This, in turn, should make it impossible to distinguish between the different wires of the circuit, but in the model each wire is uniquely labeled.

## **Hierarchy of computation models**

There may be a hierarchy of models of varying computational power that lie between classical and quantum paradigms.

We know that the quantum circuit model and others that are equivalent to it have computational power greater than that of classical computers. But can we find other models, still not fully quantum, that will be even more powerful? Knill and Laflamme have argued that if the initial state were highly mixed one could under certain conditions obtain efficient solutions to some problems

compared to classical techniques [14]. This suggests that a hierarchy might very well exist.

Imposing further constraints such as indistinguishability of the particles may lead to computing power less than that of the quantum circuit model. This question should be of interest to computer science theorists.

### **Do useful quantum computing models exist?**

Although the common quantum circuit model is not realistic, we should not be pessimistic about the plan to devise quantum computers. Physical processes in the microworld unfold according to quantum mechanics and this is enough for us to seek a paradigm for computation that satisfies all the rules of quantum mechanics. One would expect that in this paradigm some problems will be solved faster than by the fastest classical computer by virtue of the parallelism of quantum states.

For example, it is believed that the protein-folding problem is NP-complete [15], yet nature performs the folding in a second or so, and it is plausible that this is due to the quantum basis of the underlying chemical process. Furthermore, the use of quantum apparatus offers an exponential edge over classical apparatus [16], providing us with more assurance that useful models of quantum computing do exist.

A realistic model of quantum computing must ensure that the questions of preparation of pure states and that of boson/fermion statistics for a quantum state are not ignored. It would also require a realistic method of error correction.

### **Conclusion**

There remains the question of practical implementation of the circuit framework without even considering the issues raised in this note. The requirements are so stringent so as to make the computer physically unrealizable.

As a mathematical construct, the idea of the quantum computer will continue to provide useful insights into the nature of the information process.

## References

1. See A.M. Steane, "Quantum computing," Rept.Prog.Phys. 61, 117 (1998), quant-ph/9708022, for an account of cryptography, dense coding and teleportation.
2. For example, see P. Shor, "Introduction to quantum algorithms." quantph/0005003. Shor acknowledges the unrealizability of the model on page 3.
3. D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer." Proc. Roy. Soc. London Ser. A, 400, 97-117 (1985).
4. A. Peres, Quantum Theory: Concepts and Methods. Kluwer Academic, Dordrecht, 1995, page 24.
5. E. Fredkin and T. Toffoli, "Conservative logic." Int. J. Theor. Phys., 21, 219-253 (1982).
6. R. Landauer, "Information is physical." Phys. Today, 44, 23-29 (1991);  
R. Landauer, "The physical nature of information." Phys. Lett. A, 217, 188 (1996).
7. E. Fredkin and T. Toffoli, op cit.
8. A. Peres, op cit., page 30.
9. R. Laflamme et al, "Introduction to NMR quantum information processing." quant-ph/0207172.
10. S. Kak, "The initialization problem in quantum computing." Foundations of Physics, 29, 267-279 (1999); quant-ph/9805002.
11. S. Kak, "Rotating a qubit." Information Sciences, 128, 149-154 (2000);  
quant-ph/9910107.
12. S. Kak, "General qubit errors cannot be corrected." Information Sciences, 152, 195-202 (2003); quant-ph/0206144.
13. S. Kak, "Statistical constraints on state preparation for a quantum

computer." *Pramana*, 57, 683-688 (2001) ; quant-ph/0010109.

14. E. Knill and R. Laflamme, "On the power of one bit of quantum information."

*Phys. Rev. Lett.*, 81, 5672 (1998).

15. A. Fraenkel, "Complexity of protein folding." *Bulletin of Mathematical*

*Biology*, 55, 1199 (1993);

R. Unger and J. Moult, "Finding the lowest free energy conformation of a protein is an NP-hard problem: proof and implications." *Bulletin of Mathematical Biology*, 55, 1183-1198, 1993;

B. Berger and T. Leighton, "Protein folding in the hydrophilic-hydrophobic (HP) model is NP-complete." *Journal of Computational Biology*, 5, 27 (1998).

16. S. Kak, "Speed of computation and simulation." *Foundations of Physics*,

26, 1375-1386 (1996); quant-ph/9804047.

<<http://www.acm.org/ubiquity/>>