Int. J. of Unconventional Computing, Vol. 2, pp. 281–290
Reprints available directly from the publisher
Photocopying permitted by license only

The Other Kind of Quantum Computing

H. John Caulfield and Lei Qian*[1]

**Fisk University, Nashville,*
TN 37208, USA.

Received: December 9, 2005, In Final Form: April 28, 2006.

Here we consider a type of quantum computing that does not involve quantum entanglement and that can be called a single (as opposed to entangled) quantum computing (SQC). Like quantum computing involving quantum entanglement (EQC in brief), SQC uses qubits, ensures "free parallelism", uses reversible operations, avoids the irreversible loss of information upon detection and can be used only for a few well-defined tasks. But there the similarities between EQC and SQC end. We discuss these similarities and differences of SQC and EQC and provide a few examples of the former's application.

Keywords: Quantum computing, Quantum entanglement, Conservative logic, Qubit, Single-quantum computer, Entangled-quantum computer.

1 INTRODUCTION

"England and America are two countries divided by a common language."

George Bernard Shaw

There are two types of quantum computing divided by a common language: quantum mechanics. One dominates the scientific and popular literature by sheer numbers of publications, but each has serious advantages and disadvantages relative to the other. The divide between them is totally unexplored in the published literature, despite the fact that there are many workers in the field that are aware to some extent that the divide exists.

[1]The work was supported by United States Missile Defense Agency contract No. HQ00604C0010.

What is new here is not a contribution to either of the two branches of quantum computing and certainly not an attempt to argue that one is superior on all counts to the other. In fact, this paper shows explicitly that there is no clear overall winner. Our purpose to explain the divide, discuss the present states and future hopes of both, and provide the tools needed to understand the differences.

Quantum computing represents a comparatively new and very rapidly developing area of research. Thus a recent Net search for "quantum computing" found 723,280 entries, and this number increases daily. If we look at the some definitions of these terms, we find that they are commonly described as follows: "A quantum computer can do an arbitrary reversible classical computation on all the numbers simultaneously, which a binary system cannot do, and also has some ability to produce interference between various different numbers. By doing a computation on many different numbers at once, then interfering the results to get a single answer, a quantum computer has the potential to be much more powerful than a classical computer of the same size. In using only a single processing unit, a quantum computer can naturally perform myriad operations in parallel". Another description reads, "A quantum computer is any device for computation that makes direct use of distinctively quantum mechanical phenomena, such as superposition and entanglement, to perform operations on data." For these two definitions there is only one thing called a "quantum computer", namely the one associated with entanglement. However there is another type of quantum computing, as which we will discuss below.

First, we need to describe quantum entanglement which plays a central role in quantum computing. It is one of the most difficult technical obstacles on the path to building a truly useful quantum computer in a sense of EQC. By itself, in simple terms, quantum entanglement is a quantum-mechanical phenomenon in which changes in a quantum object form a set of quantum objects (even if they are spatially separated) immediately results in changes of all of them. If a set of quantum objects is entangled, then change in any one of them immediately results in changes in all of them, regardless of their space-time separations.

To make it clearer, let us consider a pure quantum state (representing a quantum logical bit, a qubit)

$$|i\rangle = a|0\rangle + b|1\rangle \tag{1}$$

Here $|0\rangle$ and $|1\rangle$ are two ortho-normal states, the coefficients a and b are the normalized probabilities amplitudes (in general, complex-valued numbers) of states $|0\rangle$ or $|1\rangle$ respectively:

$$|a|^2 + |b|^2 = 1$$

For example, these two states can be polarizations in orthogonal directions, two oppositely directed spins, etc.

More complicated states can be constructed out of the pure states, for example their products. Let's consider a simple case of a product of states 1 and 2:

$$|f\rangle = (|i\rangle)_1 \times (|j\rangle)_2 = (a|0\rangle_1 + b|1\rangle_1) \times (c|0\rangle_2 + d|1\rangle_2)$$
$$= ac|0\rangle_1|0\rangle_2 + bc|1\rangle_1|0\rangle_2 + ad|0\rangle_1|1\rangle_2 + bd|1\rangle_1|1\rangle_2 \quad (2)$$

In this case a measurement carried out on state 1(2) does not affect state 2(1). Let's say that by measuring state 1 we find that it yields $|0\rangle_1$. In formal terms this means that projecting (1) onto $|0\rangle_1$ and taking into account the ortho-normality of $|0\rangle_1$ and $|1\rangle_1$ we get the following:

$$|0\rangle_1|f\rangle = |0\rangle_1\langle 0|_1(a|0\rangle_1 + b|1\rangle_1) \times (c|0\rangle_2 + d|1\rangle_2)$$
$$= a|0\rangle_1(c|0\rangle_2 + d|1\rangle_2) \quad (3)$$

which is what we have stated: state 2 has not been affected by this measurement.

The above construction is not the only one possible. It has turned out that out of two (or more, however we consider only 2 states for simplicity sake) pure states (1 and 2) one can construct a state which *cannot* be decomposed into the product of 2 pure states, which implies that any measurement carried out on either state immediately changes the other part of the combination.

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2) \quad (4)$$

Let measurement of state 1 yield $|0\rangle_1$. According to Eq.(4) we obtain (by projecting it onto $|0\rangle_1$)

$$|0\rangle_1\langle 0|_1|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle_1\langle 0|_1(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2) = \frac{1}{\sqrt{2}}|0\rangle_1|1\rangle_2 \quad (5)$$

This measurement immediately reduces pure state $2([|0\rangle + |1\rangle]_2/\sqrt{2})$ into a state $|1\rangle_2$. If we find that measurement of state 1 yields the result $|0\rangle_1$, then state 2 will be reduced to $|0\rangle_2$. In other words, states of two subsystems are not independent, but rather mutually bound, entangled. Therefore such states are called the *entangled states*.

Many multi-qubit quantum gates can (but not necessarily do) transform a non-entangled state (in general, a pure state or its products) to an entangled state. One of the examples is a $CNOT$ (control not) gate, whose action on a state is

$$CNOT(|ij\rangle) \rightarrow |ik = j \eqcirc i\rangle$$

(here the logical operation $\eqcirc$ means "not equivalent"). In other words, $CNOT(|ij\rangle) = |ij\rangle$ if $i = 0$; $CNOT(|ij\rangle) = |i(1-j)\rangle$ otherwise.

For example, its action on the product of two pure states (2) yields

$$\begin{aligned} &CNOT(a|00\rangle + b|01\rangle + c|10\rangle + d|11) \\ &\quad = a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle \end{aligned} \tag{6}$$

that is, it transforms a pure state (2) into the pure state (6). However, if CNOT acts on a pure state $(|01\rangle - |11\rangle)/\sqrt{2} \equiv 1/\sqrt{2}(|0\rangle - |1\rangle) \times |1\rangle$ the result is

$$CNOT\frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{7}$$

that is an entangled state.

Alongside with Entanglement based Quantum Computing (EQC)(for example, see [1, 2, 3]) using the remarkable properties of quantum entanglement, there is (and was for a long time) another way to perform quantum computing. It has many of the remarkable properties, some of which it shares with EQC. On the other hand, it has some of the properties which it does not share with the latter. We called the kind of quantum computing which does not use entanglement as SQC (Single-Quantum Computing). Both EQC and SQC have some advantages over classical computation. For example, logical gates in SQC (as in EQC) systems are reversible. On the other hand, they do not use entanglement, which is one of the greatest obstacles to constructing EQC computers.

More concretely, the generation of a useful number of entangled qubits is an extremely difficult task. The best result achieved in an experiment is just seven[4] (to the best of knowledge of present authors). However, a working quantum computer would need many more, perhaps hundreds of entangled qubits. But this is not the only difficulty, since to perform meaningful calculation the entangled state must remain such for a long enough time. Unfortunately, the entanglement is very easily destroyed by the particles' interactions with their environment. Because of these difficulties, it seems that a working model of EQC with a useful number of entangled qubits will not be realized in the near future.

2 SINGLE-QUANTUM COMPUTER

Technically, if we just use one-qubit quantum gates, the computer will be SQC. Multi-qubit quantum gates of the type given in (7) are not used in SQC. However, not all multi-qubit gates are excluded. For example, the gate whose action (operator $\hat{G}$) on a pure state $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ results in a pure state as follows

$$\hat{G}(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle) = a|00\rangle + c|01\rangle + b|10\rangle + d|11\rangle$$

Of course, without using entanglement, we lose many of the most far reaching and promising applications of quantum computation. In particular, it will not be possible to perform teleportation, do dense coding, and solve certain NP and even exponential problems in polynomial time. However, some problems, like the quantum key distribution proposed by Bennett and Brassard [4], still can be solved by SQC.

Let us consider in details similarities and differences between two types of quantum computing concepts.

3 SIMILARITIES BETWEEN SQC AND EQC

3.1 Qubits

Both EQC and SQC use qubits to manipulate data. They both work with superposed states.

3.2 Limited Applicability

Neither EQC nor SQC is ever likely to be used for bookkeeping, email composition, drawing, word processing, etc, despite the fact that they can be used as such. At the present, each has only a few algorithms for which it is either more powerful than a conventional computer or the only possible device to solve problems a conventional computer cannot solve in polynomial time. Whether the number of such algorithms will be greater in the future remains to be seen.

Quantum computers seem most suitable for problems designed to utilize their parallelism. It is clear that to use them for such tasks as, say word processing, does not make sense.

3.3 Reliance on Reversible Pre-Detection Computations

Quantum-mechanical gates are represented by quantum operators, which are Hermitian. This means that all the operations performed on such a computer (excluding detection) are reversible. This also means that means that both information and energy (before detection, i.e., measurement) are conserved-hence the term “conservative logic.”

3.4 Reducing the Irreversible Loss of Information on Detection

To get information out of either an EQC or a SQC, we have to measure that information. However, any measurement results in an irreversible loss of information. In both types of quantum computers, the goal is to extract only the relevant information, while the lost information is to bee one which we do not want, the so-called “garbage”. For example, in the two-slit diffraction experiment one measures only the photons hitting the output plane without probing which slit the photon passes through. In this way the

information which we are not interested in (which slit the photon passes through) represents "garbage" which is not measured, and as such does not lead to an additional irreversible loss of information.

3.5 "Free" Parallelism

Parallelism can be found in both conventional computers and quantum computers. However it is quite different in both types of computers. While classical parallelism requires physical operators to perform each step in parallel, quantum computers use the global properties of the wave function to achieve parallelism without any multi-step operations. As a result, there is no cost in hardware, or bandwidth, or energy to accomplish those parallel operations. They are, in that sense, free.

4 DIFFERENCES BETWEEN SQC AND EQC

4.1 Entanglement

As we have already stated, EQC uses multiple entangled states to achieve quantum parallelism. On the other hand, SQC uses particles that have single unentangled wave functions. It is possible to use them with entangled photons, but we see no reason to do so.

4.2 Computational Complexity of Problems

EQC can solve combinatorial problems with high computational complexity (NP and even exponential) such as sorting or factoring in polynomial time. On the other hand, SQC solves problems of polynomial complexity by using coherent light: that include a wide range of problems varying from Fourier filtering to Boolean logic.

4.3 Dimensions of Vector Spaces

If there are n qubits, the possible states for n unentangled particles form a $2n$- dimensional vector space in SQC, while in EQC the resulting space of state vectors has 2^n dimensions due to the entanglement.

4.4 Practicality

At the present it is not clear whether EQC with a significant number of entangled particles will ever be made to work. To our knowledge, no one is even attempting that incredibly difficult task now. Existing experiments concentrate on demonstrating that gates constructed with two or three entangled states can perform reliably. On the other hand, SQC is already working.

We summarize the above properties of both types of computers in the following table

Property	Entanglement Quantum Computer (EQC)	Single Quantum Computer(SQC)
Use of qubits	Yes	Yes
Algorithms	Very few	Very few
Qubits	Yes	Yes
Reversible operators	Yes	Yes
Not measuring "garbage"	Yes	Yes
Entanglement	Yes	No
Complexity capability	NP and EXP	P
State space dimension	2^n	$2n$
Implementation	problems requiring a few steps and may work for larger ones in the future	worked for a long time on real problems

5 CLASSICAL COMPUTING AND SQC

Comparing to classical computing, SQC and EQC have the same working flaws. The only difference between SQC and EQC is that only certain kinds of quantum gates are available to be used. However, quantum computing has totally different working flow than classical computing. The following table shows the comparison between them

Classical computing	SQC	EQC
Insert data and instructions	Prepare quantum states and apparatus	Prepare quantum states and apparatus
Carry out the intermediate calculations	Propagate the wave function	Propagate the wave function
Read the result	Read the result	Read the result

6 EXAMPLES OF SQC

6.1 Massively Parallel Free Space Interconnection Based SQC's

These are what Caulfield, Shamir, and others [5, 6, 7] called Wave -Particle Duality (WPD) processors. While conventional computers must implement $O(n^4)$ components to connect each of an $n \times n$ input array with each of an $n \times n$ output array having different weights or strengths, there are optical systems that accomplish that automatically. One way of thinking of this is that those $O(n^4)$ computational steps are virtual, performed "free" in the wave domain. When we make a detection, however, there is an irreversible loss of information in entering into the "real" world of particles (electrons in this case).

The goal in designing a suitable algorithm-architecture ("algotecture") is to arrange it so that what is detected is the sought-after information and what is lost is the "garbage". WPD computers generate the inevitable garbage virtually and destroy it upon detection. WPD processors have been implemented for linear algebra problems and for Fourier transform systems.

6.2 Conservative Optical Logic Devices

Boolean logic devices destroy one bit of information with each operation, so they are inherently irreversible. Consider, for example, the AND gate.

A	B	A $\wedge$ B
0	0	0
0	1	0
1	0	0
1	1	1

This operation (gate) is clearly not reversible. Suppose, you know that $A \wedge B = 0$. You have no idea which of three input pairs was present to give that result. As a result this operation "dissipate" information. This means that it requires energy of at least $kTln2$ to destroy one bit of information at temperature T. Modern digital computers operate at much greater energy per operation than this theoretical minimum. And that is a good thing in some regards. For a quantum computer the uncertainty principle would dictate that a smaller change in energy would increase the operation time of the gate.

Bennett and Landauer [8] explored the possibility that logic gates might be able to operate without loss of information. Such "conservative" logic gates would have no minimum energy expenditure per bit of information. But, to be useful, such conservative optical logic gates would have to generate the same information as the familiar dissipative gate. How can we create a dissipative operation (yielding the necessary information) within a conservative operation? That is the key question of conservative logic gates. The only solution until recently was to increase the numbers of input and output signals for a gate, so some can give the desired results while others conserve information by producing garbage [9].

Recently, we have been exploring another solution. The numbers of inputs and outputs to a gate remain two, but they become qubits not bits. When a detection occurs, what is measured is the desired Boolean function. In the pre-detection, the operation on wave domain is reversible. Indeed, in our cases, the optical systems that perform the SQC operations are passive. Because they are passive, they require no energy and do not reduce the bandwidth of signals incident upon them. There is no energy loss and no bandwidth loss. The only published work [10] describes the pair of Boolean functions $XOR(A, B)$ (which is nothing more than a CNOT, that is $A\widetilde{\vee}B$) and its complement *COINC (A, B)*, i.e., $A \sim B$. In a work

submitted elsewhere for publication [11], we show that any operation can be performed passively in this way, but results cannot be cascaded without losses.

RELATED WORK

A recent report [12] showed that more powerful Single-Quantum computers are being studied. D-Wave Systems Company in Vancouver, Canada is doing a project to build a different kind of quantum computer. Instead of relying on quantum entanglement, this kind of quantum computer exploits the more robust property of quantum mechanics, namely quantum tunneling. By our definition, it is an SQC since no entanglement states involve. According to the report, it can solve some NP complete problems such as traveling-salesman problem.

As this manuscript was being revised, we found that another paper with the same general theme had just been published [13]. That paper emphasized the ability of SQC (the authors named them as QCWE, Quantum Computation Without Entanglement, in their paper) in algorithm point of view. They proved that certain subproblems of some well-known algorithms, such as Deutsch-Jozsa, Simon and Grover's algorithms, can be solved with quantum computer without entanglement and still have advantage over classical computer. Our approach differs somewhat from theirs in that we have not sought ways to avoid the use of entanglement for established quantum computing algorithms. Rather, we have emphasized the development of hardware systems specifically designed for quantum computing without entanglement. In other words, we focus on the advantages of SQC over classical electronic computers in hardware point of view. Our paper and theirs share the belief that entanglement is key to the most powerful quantum computer operations but unnecessary and undesirable for some important simpler operations. In other words, SQC still has advantages over classical computation.

It is also worth to mention the work of Knill, Laflamme and Milburn [14, 15]. They showed that it is in principle possible to construct a (full power) quantum computer with linear optics, single-photon sources and photon detection alone. *Single-photon source* has a similar name with our *Single Quantum Computer*. However, the construction of quantum gates proposed by Knill, Laflamme and Milburn uses entangled ancilla photons. So they are actual EQC by our definition.

CONCLUSION

In this paper, we discussed another kind of quantum computing, SQC. Unlike quantum computing that most people refer to (that we call it EQC), this kind of quantum computing does not rely on quantum entanglement,

one of the biggest technical difficulties of building quantum computers. Some of SQCs already work today. We compare SQC to EQC side by side. We also gave a couple of examples of SQC.

ACKNOWLEDGMENTS

The authors thank Prof. A. Granik for the help rendered in preparation of this paper.

REFERENCES

[1] Bennett, C. H. and Wiesner, S. J., (1992). Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states, *Phys. Rev. Lett., 69,* 2881.

[2] Bennett, C. H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A. and Wootters, W. K., (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, *Phys. Rev. Letter., 70,* 1895.

[3] Shor, P., (1994). Algorithms for quantum computation: Discrete logarithms and factoring, Proc. of 35th Annual Symposium on the Foundations of Computer Science, 124.

[4] Vandersypen, L. M., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H. and Chuang, I. L., (2001). Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature. 414,* 883.

[5] John, H., (1989). Caulfield and Joseph Shamir. Wave particle Duality Considerations in Optical Computing. *Applied Optics 28,* 2184.

[6] John, H., (1990). Caulfield and Joseph Shamir. Wave-Particle-Duality Processors: Characteristics, Requirements, and Applications. *Journal of the Optical Society of America A7,* 1314.

[7] Caulfield, H. J., Joseph Shamir, Ludman J. E. and Greguss, P., (1990). Reversibility and Energetics in Optical Computing. *Opt. Lett. 15,* 912.

[8] Bennett, C. H. and Landaur, R., (1985). Fundamental physical limits of computation, *Scientific American 253,* 48.

[9] Fredkin, E. and Toffoli, T., (1982). Conservative logic, *International Journal of Theoretical Physics 21,* 3.

[10] Caulfield, H. J. and Westphal, J., (2004). The logic of optics and the optics of logic, *Information Sciences 162,* 21.

[11] Qian, L. and Caulfield, H. J., (2006). What we can do with a linear optical logic gate? To appear in Information Sciences.

[12] MacCormack, A., Agrawal, A. and Henderson, R., (2004). D-Wave Systems: Building a Quantum Computer, Harvard Business Online.

[13] Kenigsberg, D., Mor, T. and Ratsaby, G., (2006). Quantum advantage without entanglement. *Quantum Information & Computation Online, 4.*

[14] Knill, E., Laflamme, R. and Milburn, G. J., (2001). A scheme for efficient quantum computation with linear optics. *Nature, 409,* 46–52.

[15] Kok, P., Munro, W. J., Nemoto, K., Ralph, T. C., Dowling, J. P. and Milburn, G. J., (2005). Linear Optical Quantum Computing. quant-ph/0512071.