Technical Report No. 2005-500
Quantum computing: Beyond the limits of conventional computation*

Marius Nagy and Selim G. Akl

School of Computing

Queen's University

Kingston, Ontario K7L 3N6

Canada

E-mail: {marius,akl}@cs.queensu.ca

July 22, 2005

Abstract

The quantum model of computation not only offers entirely new ways to manipulate information, but also allows information processing tasks to be formulated in unconventional, genuine quantum mechanical terms. We show that the task of distinguishing among entangled quantum states combines entanglement and non-determinism in a way that makes the quantum solution impossible to simulate on any classical machine (even one equipped with the same measurement capabilities as the quantum computational device). A new class of information processing tasks is thus uncovered whose members are readily carried out by a quantum computer, yet are impossible to perform on any classical machine (whether deterministic or probabilistic). In the broad, unconventional context created by quantum mechanics, the computational power of a quantum computer is therefore strictly greater than that of a classical computer.

*This research was supported by the Natural Sciences and Engineering Research Council of Canada.

1 Introduction

Is a quantum computer strictly more powerful than a classical one? Are there information processing tasks for which only a machine based on quantum mechanical principles is naturally suited? What are the limitations when trying to simulate a quantum process on a classical computing machine?

These questions have concerned researchers in quantum computation and quantum information theory ever since the field originated. Despite the impressive advancements made in the quantum computation and quantum information areas, the fundamental question about the relative power of a quantum computer with respect to its classical counterpart is still not fully answered. Perhaps this is partly due to the multitude of contexts (or paradigms) in which such a question might be asked. Consequently, there may not be a single answer.

In this paper, we analyze the relation between the quantum and the classical models of computation from the broad perspective offered by quantum mechanics. Non-determinism and operating on entangled quantum states can each be successfully simulated on a machine whose functioning obeys the laws of classical physics. However, we show in this paper that there are problems merging non-determinism and entanglement in such a way that a solution based on classical means is no longer possible. Distinguishing among entangled quantum states forms the basis for a whole class of problems requiring information manipulation that are only solvable by a machine endowed with the power of quantum computing. This demonstrates that the limitations of the classical model of computation are purely physical and a computer operating through quantum means is strictly more powerful than a conventional one.

In the following section we try to review and make explicit some of the contexts in which the comparison between the classical and the quantum computer took place. This will help emphasize the variety of angles under which the problem can be attacked and also put our approach (given in section 3) into perspective. The definition of the quantum distinguishability problem, its efficient quantum solution and the attempted classical solution are also presented in section 3. Two examples of information processing tasks based on the distinguishability of entangled quantum states are given in section 4. Section 5 offers some conclusions about the nature of the relation between a quantum and a classical machine, in terms of their computational powers.

2 A review of previous results

The first step towards an analytical investigation of the computational power specific to a quantum mechanical device was the elaboration of a model that should be abstracted away from any particular physical realization. The breakthrough came when David Deutsch described the operation of a universal quantum computer $\mathcal{Q}$, a model of computation inspired by the classical Turing machine, but whose functioning obeys the principles of quantum mechanics. Even in this early paper [8], several features are identified with respect to which the Quantum Turing Machine is superior to any classical device.

2.1 True randomness

The first example given is the generation of *true* random numbers. In particular, valid programs are shown to exist for $\mathcal{Q}$ that deal with arbitrary irrational probabilities, a feature that the universal Turing machine $\mathcal{T}$ could not truly match. It could only simulate such discrete finite stochastic systems with arbitrary accuracy, provided it has access to a "random oracle", which really cannot be implemented by classical means.

2.2 Entanglement

But the property of $\mathcal{Q}$ that cannot be even approximately simulated by any classical system is the generation of *entangled* (or *non-separable*) states like

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

The strong correlations exhibited by the two qubits composing state (1) are only characteristic to the quantum resource known as *entanglement*, and they are simply beyond the scope of any classical Turing machine. Bell's theorem [2] is a mathematical formulation of the fact that no classical system can reproduce the statistical results obtained by measuring these two qubits.

2.3 Quantum speed-up

As another argument intended to prove the superior computational power of the Quantum Turing Machine, Deutsch provides an example which demonstrates how *quantum parallelism* can be used to speed up computation. Quantum parallelism refers to the capability of a quantum computer to evaluate a function $f(x)$ for exponentially many different values of x in the time it takes a classical computer to evaluate the function for just one value. This is possible due to the quantum mechanical principle of the *superposition* of states. Deutsch exploited this feature and devised an example in which quantum parallelism augmented with *interference* can "beat" a classical computer. Thus, given a function $f : \{0, 1\} \rightarrow \{0, 1\}$, he presented a quantum algorithm able to compute $f(0) \oplus f(1)$ in a single evaluation of the function f.

Later, Deutsch's algorithm was generalized by Deutsch and Jozsa [9], who addressed the n-bit case by allowing the domain of f to be the set of all integers in the interval $[0, 2^n - 1]$. In just one evaluation of the function f, the Deutsch-Jozsa algorithm is able to determine whether f is constant or perfectly balanced (the latter property meaning that f maps exactly half of the input values in the domain to the image 0, and the other half to 1). Although the problem seems somewhat contrived, with no immediate practical applications, this was the first example in which the quantum computer achieved an exponential speed-up over the classical one (note that a classical Turing machine needs an exponential number of evaluations of f in order to make the decision between constant and perfectly balanced).

The same superiority of the quantum computer was proved by Shor's factorization algorithm [16], only this time for a problem of huge practical importance. Factoring large integers and computing discrete logarithms in quantum polynomial time threatens the security of a large class of public-key cryptographic systems in use today. For a classical computer these tasks remain intractable, despite remarkable advances that could only bring their running time to a sub-exponential level [12]. So, in the context of essentially speeding up the computation for some problems, we can affirm that a quantum computer is definitely more powerful than a classical one. However, we should keep in mind that these problems can also be solved by the universal Turing Machine, given enough time (even if this time is more than the age of the Universe).

2.4 Quantum simulations

Another class of tasks at which quantum computers could naturally outperform any classical machine is simulating quantum mechanical systems occurring in Nature. As the size (number of constituents) of a quantum system increases, the number of variables required to describe the state of the system grows exponentially. So, in order to store the quantum state of a system with n distinct components, a classical computer would need some c^n bits of memory, with the constant c depending upon the system being simulated and the desired accuracy of the simulation. Furthermore, calculating its evolution over time would require the manipulation of a huge matrix, involving $c^n \times c^n$ bits. As Feynman noted in 1982 [10], this is prohibitively inefficient for a simulator observing the laws of classical physics. On the other hand, a machine that worked by quantum means would intrinsically make a much more efficient simulator, requiring only a linear number of qubits.

Following the same logic, it is not difficult to envisage a classical Turing machine that simulates an arbitrary quantum circuit, if one does not care about efficiency. The simulation in [3] requires space, and therefore time, exponential in the number of qubits in the quantum circuit. Bernstein and Vazirani [5] have given a simulation that takes polynomial space, but exponential time. The lack of an efficient classical simulation of a quantum computer induced the idea that a quantum computing machine may be inherently faster and therefore strictly more powerful. However, any computation a quantum computer can perform, by applying a series of unitary evolutions to its quantum register, can be replicated (even if highly inefficiently) by a Deterministic Turing Machine (DTM). Similarly, a Probabilistic Turing Machine (PTM) can simulate the inherent probabilistic nature of a quantum measurement operation.

For the unacquainted reader, we state that when measuring a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with respect to the standard basis for quantum computation $\{|0\rangle, |1\rangle\}$, we get either the result 0 with probability $|\alpha|^2$, or the result 1 with probability $|\beta|^2$. Furthermore, measurement alters the state of a qubit, collapsing it from its superposition of $|0\rangle$ and $|1\rangle$ to the specific state consistent with the result of the measurement. For example, if we observe $|\psi\rangle$ to be in state $|0\rangle$ through measurement, then the post-measurement state of the qubit will be $|0\rangle$, and any subsequent measurements (in the same basis) will yield 0 with probability 1.

2.5 QTM versus DTM and PTM

The contest between the quantum and the classical computer can also be judged from these two points of view: comparing the Quantum Turing Machine (QTM) with a DTM or a PTM. The Deutsch-Jozsa algorithm, for instance, achieves an impressive speed-up over a DTM, but the problem is also easy for a PTM, which can solve it very quickly with high probability.

The first hint that QTMs might be more powerful than PTMs was given by Bernstein and Vazirani, who showed how to sample from the Fourier spectrum of any Boolean function on n bits in polynomial time on a QTM [5]. No algorithm was known to replicate this result on a PTM. Then, Berthiaume and Brassard were able to construct an oracle, relative to which a decision problem exists that could be solved with certainty in polynomial time in the worst case on a quantum computer, but could not be solved classically in probabilistic expected polynomial time, if errors were not tolerated [6]. In the same paper, they also show that there is a decision problem solvable in exponential time on a QTM and in double exponential time on all but finitely many instances on any DTM. These two results, besides being a victory of quantum computers over classical machines (deterministic or probabilistic) also prove that the power of quantum computation cannot simply be ascribed to the indeterminism inherent in quantum theory.

2.6 Quantum vs. classical complexity

The great hope for quantum computers at the inception of the quantum paradigm of computation was that they would be able to make NP-complete problems tractable. Relative to this criterion, we still don't know whether a quantum machine is more powerful than a classical one, in spite of Shor's results concerning factorization and computing discrete logarithms. The trouble is that neither of these two problems is known to be NP-complete, despite the general belief that they are not in P. Furthermore, the current belief is that a quadratic improvement in the running time may be the best we can get out of a quantum computer in these kinds of tasks [15].

The relative power of quantum computers with respect to classical ones can also be couched in the relationships between classical and quantum complexity classes. In this sense, the complexity classes BPP (Bounded error Probability in Polynomial time) and its quantum analogue BQP have attracted a lot of interest. Proving that $BPP \subset BQP$ is regarded as proving that quantum computers are strictly more powerful than classical computers. This may be quite non-trivial to demonstrate, since $BPP \subset BQP$ implies that P is not equal to $PSPACE$, a result that many researchers have unsuccessfully attempted to prove. However, if we adopt a non-classical approach and allow the input to be described in non-classical terms (genuine quantum mechanical terms, in our case) then we can show that the set of problems solvable efficiently by a classical computer (deterministic or probabilistic) is strictly included in the set of problems having an efficient quantum solution.

2.7 Super-Turing computations

We end this exposition of working hypotheses, when comparing quantum and classical computers, with the most "exotic" cases. Some researchers have shown that there are quantum processes which can be used to compute the solution to Turing uncomputable (or undecidable) problems. Calude and Pavlov [7] describe a mathematical quantum device that is able to determine with a pre-established precision whether an arbitrary program halts or not. Kieu [11] uses quantum adiabatic processes to provide a single, universal procedure, taking the form of a quantum algorithm that solves Hilbert's tenth problem (which has been shown to be equivalent to Turing's halting problem). The essence of these results is that there exist mathematical constructions, built within the framework provided by the physical theory of quantum mechanics, which are powerful enough to tackle with success problems that have been proved to be out of the capabilities of the Turing machine.

A few observations have to be made with respect to the features empowering these quantum "hypercomputers". They manage to compute the "uncomputable" by eluding in one way or another the *finiteness condition* [1]. The method employed by Calude and Pavlov (a quadratic form of an iterated map acting on randomly chosen vectors, the latter viewed as special trajectories of two Markov processes working in two different scales of time) encodes the whole data into an infinite superposition. Kieu too works with a dimensionally infinite Hilbert space in his quantum adiabatic algorithm. However, he argues that the number of dimensions is only required to be sufficiently large, but finite.

Furthermore, an important common characteristic of both algorithms is their probabilistic nature. The answer they give to a problem has only a certain probability to be the correct one. This probability can be made arbitrarily close to 1, but it can never reach 1 as long as the quantum procedure is only allowed to run for a finite amount of time. Finally, we note that the models of computation capable of such performances are mathematical objects with no constructive indications being offered to attempt the experimental realization of such a machine (assuming this thing is possible). From this point of view, they can rather be characterized as quantum "hypercomputers", as opposed to a "standard" quantum computer, capable of running Shor's algorithm, for example.

3 Our approach

Let us now describe the terms under which we compare, in this paper, the quantum computer with the classical computer. The quantum machine is assumed to have a set of quantum gates that is universal for quantum computation (although for our purposes the controlled-NOT and Hadamard gates will suffice), together with the ability to perform single-qubit measurements in the standard computational basis $\{|0\rangle, |1\rangle\}$. This description corresponds to a standard quantum computer that can have various physical realizations.

On the other hand, the classical computer in consideration is a conventional computing device whose capabilities match those of the Universal Turing Machine. Due to the nature of the problems addressed in this paper, the classical computing machine is augmented with the same measurement capabilities as the quantum computer. After all, quantum measurements in the standard computational basis are just a means of acquiring classical information (about quantum states).

In the context delimited by these specifications, we can identify a whole class of information processing tasks which clearly separate the quantum computer from its classical counterpart in terms of computability.

3.1 Quantum distinguishability

At the heart of this class of problems is the task of distinguishing among entangled quantum states. The general formulation of the problem is given in the following. Suppose we have a quantum system composed of n qubits whose state is not known exactly. What we know with certainty is that the system can be described by one of the following 2^n entangled states:

$$\begin{aligned} \frac{1}{\sqrt{2}}(|000\cdots0\rangle &\pm |111\cdots1\rangle), \\ \frac{1}{\sqrt{2}}(|000\cdots1\rangle &\pm |111\cdots0\rangle), \end{aligned}$$

$$\vdots \tag{2}$$

$$\frac{1}{\sqrt{2}}(|011\cdots 1\rangle \quad \pm \quad |100\cdots 0\rangle).$$

The challenge for the two candidate computers is to correctly identify the state of the system resorting to all their measurement and computational abilities. Alternatively, the problem can also be formulated as a function computation (evaluation), with the unknown quantum state as the input and the corresponding index (between 0 and $2^n - 1$) as the output. We have to say from the very beginning that this function is computable. The 2^n states in (2) are perfectly distinguishable since they form an orthonormal basis for the state space corresponding to the n-qubit system. Note, in particular, that the case $n = 2$ corresponds to the distinguishability of the four Bell (or EPR) states, which is the key feature in achieving superdense coding [4].

The immediate, theoretical solution to this problem is to perform a single joint measurement of the whole system by defining each of the 2^n states that are to be distinguished to be a projector associated with the measurement operation. Although mathematically this is a perfectly valid solution, it is very difficult in practice to perform such a joint measurement, even for the simplest case involving only two qubits [13]. Furthermore, as it was shown in [14], if a joint measurement of all qubits in the system is not feasible, then no solution is better than measuring each qubit individually, one after the other. Of course, in this way we will not be able to distinguish between quantum states that differ only through a relative phase factor, like $\frac{1}{\sqrt{2}}(|000\cdots 0\rangle + |111\cdots 1\rangle)$ and $\frac{1}{\sqrt{2}}(|000\cdots 0\rangle - |111\cdots 1\rangle)$, for example. But note that this is the best that can be achieved, given the measurement capabilities of both the classical and quantum computer.

However, if we resort to their processing capabilities, the situation changes. Unitary operators preserve inner products, so any unitary evolution of the system described by (2) will necessarily transform it into another orthonormal basis set. Therefore, a unitary transformation must exist that will allow a subsequent measurement in the standard computational basis without any loss of information. The following result shows that such a transformation not only exists, but that in fact it can be implemented efficiently.

Theorem 1 *The transformation between the following two orthonormal basis sets for the state space spanned by n qubits:*

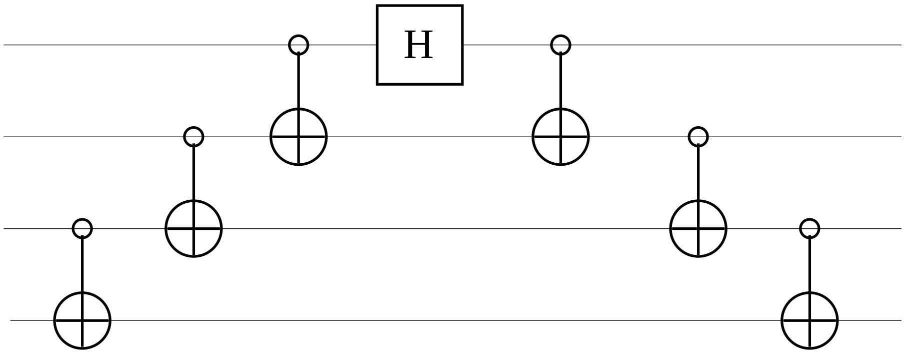

Figure 1: Quantum circuit for Theorem 1.

$$
\begin{aligned}
\frac{1}{\sqrt{2}}(|000\cdots 0\rangle + |111\cdots 1\rangle) &\longleftrightarrow |000\cdots 0\rangle, \\
\frac{1}{\sqrt{2}}(|000\cdots 0\rangle - |111\cdots 1\rangle) &\longleftrightarrow |111\cdots 1\rangle, \\
\frac{1}{\sqrt{2}}(|000\cdots 1\rangle + |111\cdots 0\rangle) &\longleftrightarrow |000\cdots 1\rangle, \\
\frac{1}{\sqrt{2}}(|000\cdots 1\rangle - |111\cdots 0\rangle) &\longleftrightarrow |111\cdots 0\rangle, \\
&\vdots \\
\frac{1}{\sqrt{2}}(|011\cdots 1\rangle + |100\cdots 0\rangle) &\longleftrightarrow |011\cdots 1\rangle, \\
\frac{1}{\sqrt{2}}(|011\cdots 1\rangle - |100\cdots 0\rangle) &\longleftrightarrow |100\cdots 0\rangle.
\end{aligned} \tag{3}
$$

can be realized by a quantum circuit comprising only a linear number of controlled-NOT and Hadamard gates.

Proof

It is easy to check that the circuit depicted in Figure 1 performs the required quantum transformation for the case $n = 4$. The generalization to an arbitrary number of qubits is straightforward. In the general case the circuit consists of $2n - 2$ controlled-NOT gates and one Hadamard gate. Due to its symmetric nature, the same quantum circuit can also perform the inverse transformation, from the normal computational basis set to the entangled basis set. □

By applying the transformation realized by this circuit, the quantum computer can disentangle the qubits composing the system and thus make the act of measuring each qubit entirely independent of the other qubits. This will ensure obtaining the correct answer to the distinguishability problem 100% of the time. In other words, the function is efficiently computable (in quantum linear time) by a quantum computer.

Can the classical computer replicate the operations performed by the quantum machine? We know that a classical computer can simulate (even if inefficiently) the continuous evolution of a closed quantum system (viewed as a quantum computation in the case of an ensemble of qubits). So, whatever unitary operation is invoked by the quantum computer, it can certainly be simulated mathematically on a Turing machine. The difference resides in the way the two machines handle the uncertainty inherent in the input. The quantum computer has the ability to transcend this uncertainty about the quantum state of the input system by acting directly on the input in a way that is specific to the physical support employed to encode or describe the input. The classical computer, on the other hand, lacks the ability to process the information at its original physical level, thus making any simulation at another level futile exactly because of the uncertainty in the input.

We have to emphasize that had the input state been perfectly determined, then any transformation applied to it, even though quantum mechanical in nature, could have been perfectly simulated using the classical means available to a Turing machine. However, in our case, the classical computer does not have a description of the input in classical terms and can only try to obtain one through direct measurement. This will in turn collapse the entanglement in the input state, leaving the classical computer with only a 50% probability of correctly identifying the original quantum state. This means that the problem cannot be solved classically, not even by a PTM. There is no way to improve the 50% error rate of the classical approach to distinguish among the 2^n states.

So this problem tells us that what draws the separation line between a quantum and a classical computer, in terms of computational power, is not the ability to extract information from a quantum system through measurements, but the ability to process information at the physical level used to represent it. For the distinguishability problem discussed, this is the only way to deal with the non-determinism introduced by entanglement.

4 Some consequences

Distinguishing among entangled quantum states forms the basic building block for a series of information processing tasks that can only be accomplished by a quantum computer. Here are two such examples.

4.1 Conveying quantum information through a classical channel

The first one addresses the problem of transmitting unknown quantum information through a classical channel. In the general case, when we have no knowledge whatsoever about the quantum state to be transmitted, the task is obviously impossible. It requires a classical description of the quantum state, which cannot be obtained since a quantum measurement would ruin the original state and cloning an unknown quantum state was proven to be impossible.

Quantum teleportation actually requires the existence of a classical channel between the source and the destination, so it could be interpreted as the transmission of an unknown quantum state through a classical channel. There is an important point to make, however. Quantum teleportation refers only to a single qubit and requires an EPR state to be shared by the sender and the receiver prior to the teleportation. This entangled pair of qubits is actually a resource that will be consumed in the process. The same argument can be formulated in the case of another task that is not possible through classical means, namely, superdense coding. Unlike these remarkable applications of entanglement as a physical resource, the information processing tasks investigated in this paper do not assume the creation and distribution of entanglement in order to be completed.

After this necessary clarification, we note that the problem investigated in our first example is unsolvable (in its most general formulation) by both our classical and quantum computers. However, if we restrict the unknown quantum state to be a member of the set (2), then the task is only out of the capabilities of the classical machine. The quantum computer can still use the circuit in Figure 1 to obtain a "label" of the original quantum state in classical terms, which can be subsequently transmitted via the classical channel. At the other end, the same quantum circuit can reconstruct the original quantum state, based on the classical information received.

4.2 Protecting quantum information from classical attacks

The second example is taken from the field of cryptography and gives a more plastic representation of the physical limitations of a classical computer to process information. A simple protocol may be devised to enable the transmission of information through a quantum channel, without any possibility of eavesdropping from a third party resorting only to the computational power of a classical computer. For this purpose, each pair of qubits transmitted through the channel encodes one bit of information in the following way: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ represent a 0 bit, while $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ represent the bit 1. No single-qubit measurements are better than just flipping a coin in order to guess the *bit* transmitted, so no information whatsoever can be gained by the classical machine.

The quantum computer would be in the same situation if it would resort only to its measurement abilities. However, the quantum computer can first "evolve" the Bell basis into the normal computational basis (using the quantum circuit from Figure 1 for the case $n = 2$) and then identify the bit transmitted by reading the measurement outcome for the first qubit. Note that this protocol can be generalized to "beat" any classical computer endowed with *finite* measuring capabilities. If the classical computer is able to perform a joint measurement of k qubits (where k is unbounded, but finite) then it suffices to encode a bit of information into the relative phase of an entangled quantum state comprising $k + 1$ qubits. In this way, the information conveyed through the quantum channel is safely kept out of reach for the classical computer, due to its limitations in processing information at the very physical level chosen to embody it.

5 Conclusions

When he devised the Quantum Turing Machine as the first abstract model of quantum computation, David Deutsch already pointed to some features that set it apart from the classical Turing machine: intrinsic genuine non-determinism and entanglement. Naturally, these features have created a lot of speculations about the superiority of the quantum computer in terms of computability and complexity. Consequently, the computational powers of the quantum and classical machine have been evaluated and compared in a variety of contexts.

This paper shows that there is a whole class of information processing tasks relative to which a clear separation line exists between quantum computers and classical computers with respect to their computational powers. The set of problems solvable by classical means is therefore strictly smaller than the set of functions computable through quantum means. At the heart of this separation lies a problem (namely, distinguishing among entangled quantum states) that combines uncertainty and entanglement in a way that renders a classical simulation of the quantum solution impossible. Otherwise, taken separately, uncertainty can be dealt with (through measurements) in the absence of entanglement, while entanglement, as a particular case of superposition, can be simulated by a classical machine for the purpose of computation (due to the linearity of the unitary operators describing quantum transformations).

While quantum measurements are certainly required to distinguish among different quantum states, this is most emphatically not what gives the Quantum Turing Machine the advantage over the classical Turing machine. Also, this superiority is not due to some theoretical property specific to "hyper-computers", which breaks in one way or another the finiteness condition by implicitly assuming some form of unlimited computational resources. It is also not a matter of complexity, the ability to solve problems much faster than it is possible classically. This paper shows that quantum computers are better than classical ones (whether deterministic or probabilistic) in terms of computability (function evaluation) due to the power conferred to their computations by the way they represent information at the physical level.

Classical physics is just a particular, trivial case of quantum mechanics. Sometimes, information encoded in genuine quantum mechanical terms cannot be successfully manipulated unless the computing device has the power to process this information directly at the physical level used to represent it. The properties of the physical level chosen to embody information in a computational model ultimately determine its computational capabilities and power. The limitations of the classical Turing machine are therefore purely physical. So, is a machine that computes following the principles of quantum mechanics really more powerful than a computing device designed in accord with classical physics? We think that the answer is definitely affirmative. And the difference is made by those problems, defined in purely quantum mechanical terms, whose quantum solutions are impossible to be simulated classically.

References

[1] Selim G. Akl. The myth of universal computation. In R. Trobec, P. Zinterhof, M. Vajteršic, and A. Uhl, editors, *Parallel Numerics, Part 2, Systems and Simulation*, pages 211–236. University of Salzburg, Austria and Jožef Stefan Institute, Ljubljana, Slovenia, 2005.

[2] John Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[3] Eric Benjamin, Kenny Huang, Amir Kamil, and Jimmy Kittiyachavalit. Quantum computability and complexity and the limits of quantum computation. http://www.cs.berkeley.edu/∼kamil/quantum/qc4.pdf, December 2003.

[4] Charles H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992.

[5] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *Special issue on Quantum Computation of the SIAM Journal on Computing*, 26(5):1411–1473, October 1997. http://arxiv.org/abs/quant-ph/9701001.

[6] André Berthiaume and Gilles Brassard. Oracle quantum computing. *Journal of Modern Optics*, 41(12):2521–2535, December 1994.

[7] Cristian S. Calude and Boris Pavlov. Coins, quantum measurements, and Turing's barrier. *Quantum Information Processing*, 1(1–2):107–127, April 2002.

[8] David Deutsch. Quantum theory, the Church-Turing principle, and the Universal Quantum Computer. *Proceedings of the Royal Society of London A*, 400:97–117, 1985.

[9] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A*, 439:553–558, 1992.

[10] Richard Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6 & 7):467–488, 1982.

[11] Tien D. Kieu. Quantum adiabatic algorithm for Hilbert's tenth problem: I. The algorithm. http://arxiv.org/abs/quant-ph/0310052, October 2003.

[12] Arjen K. Lenstra and H. W. Lenstra, Jr., editors. *The Development of the Number Field Sieve.* Springer-Verlag, New York, 1993.

[13] Klaus Mattle, Harald Weinfurter, Paul G. Kwiat, and Anton Zeilinger. Dense coding in experimental quantum communication. *Physical Review Letters*, 76(25):4656–4659, 1996.

[14] Marius Nagy and Selim G. Akl. Quantum measurements and universal computation. to appear in the International Journal of Unconventional Computing.

[15] Sara Robinson. Emerging insights on limitations of quantum computing shape quest for fast algorithms. *SIAM News*, 36(1), January/February 2003.

[16] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *Special issue on Quantum Computation of the SIAM Journal on Computing*, 26(5):1484–1509, October 1997.