Technical Report No. 2005-495
ON THE IMPORTANCE OF PARALLELISM FOR QUANTUM COMPUTATION AND THE CONCEPT OF A UNIVERSAL COMPUTER*

Marius Nagy and Selim G. Akl
School of Computing
Queen's University
Kingston, Ontario K7L 3N6
Canada
Email: {marius,akl}@cs.queensu.ca

Abstract

The role played by parallelism in the theory of computation depends on the particular paradigm or computational environment considered, but its importance has been confirmed with the emergence of each novel computing technology. In this paper we study the implications of parallelism in quantum information theory and show that a parallel approach can make the difference between success and failure when trying to distinguish between (entangled) quantum states. A (perhaps surprising) consequence of this fact is the impossibility of constructing a Universal Computer.

1 Introduction

Parallel computing was originally motivated by the need to speed up computation, especially for those tasks whose sequential running time is pro-

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

hibitively long. This traditional view of the role played by parallelism in computation has since evolved dramatically, with implications almost impossible to foresee when the field originated.

We know today that there are tasks and computational paradigms for which a parallel approach offers much more than just a faster solution [4]. A real-time environment, constraining the input data provided and the output produced at various moments in time, can have drastic effects on the quality of the solution obtained for a certain problem, unless parallelism is employed [13, 14, 15, 16]. A general framework is developed in [2] to show how a superlinear (with respect to the number of processors employed in the parallel approach) improvement in the quality of the solution computed to a real-time problem can be obtained.

In other cases, a sequential machine fails to tackle a certain task altogether, and parallelism is the only hope to see that task accomplished. Examples of this kind include measuring the parameters of a dynamical system [1, 7] or setting them in such a way as to avoid pushing the system into a chaotic behavior [6]. Also, some geometric transformations can only be performed successfully if we act simultaneously on a certain number of objects [3].

Progress in science and technology influences the way computations are carried and the emergence of novel computational environments and paradigms continually broadens the applicability and importance of parallelism. In this paper we exhibit an example of a problem from quantum information theory that clearly emphasizes the role of parallelism in this relatively new field of computation governed by the principles of quantum mechanics. The example we present also reinforces the argument developed in [5] demonstrating the infeasibility of a Universal Computer.

The remainder of the paper is organized as follows. The next section is intended to make the reader familiar with the fundamental notions of quantum computation. Section 3 introduces the problem of distinguishing quantum states and analyzes the instance defined by the four Bell states. A generalization to an arbitrary number of qubits entangled together is developed in section 4. Section 5 discusses the relevance of the problem investigated, in the context of Universal Computation. The contributions of this paper, stressing the importance of parallelism in general and for the concept of a Universal Computer in particular, are summarized in the last section.

2 Fundamentals of quantum computation and quantum information

This section introduces the basic elements of quantum computation and quantum information to the extent needed for a clear exposition of the main ideas presented in this paper.

Quantum information theory was developed much in analogy with classical information theory, enlarging the scope of the latter. Thus, quantum information theory deals with all the static resources and dynamical processes investigated by classical information theory, as well as additional static and dynamic elements that are specific to quantum mechanics.

2.1 The qubit

Probably, the most fundamental quantum resource manipulated by quantum information theory is the quantum analogue of the classical bit, called the *qubit*.

Though it may have various physical realizations, as a mathematical object the qubit is a unit vector in a two-dimensional state space, for which a particular orthonormal basis, denoted by $\{|0\rangle, |1\rangle\}$ has been fixed. The two basis vectors $|0\rangle$ and $|1\rangle$ must be orthogonal (*i.e.* their inner product is zero) and normalized (*i.e.* of unit length each), hence the orthonormality requirement. The basis vectors correspond to the two possible values a classical bit can take. However, unlike classical bits, a qubit can also take many other values. In general, an arbitrary qubit $|\psi\rangle$ can be written as a linear combination of the computational basis states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$ (the normalization condition ensuring that $|\psi\rangle$ is a unit vector). In order to describe the state of a qubit or ensemble of qubits in a compact way, we have adopted here the well-established *bra/ket* notation introduced by Dirac [10]. According to his conventional notation, *kets* like $|x\rangle$ are simply column vectors, typically used to describe quantum states. Similarly, the matching *bra* $\langle x|$ is a row vector denoting the conjugate transpose of $|x\rangle$. Thus, the *ket* $|\psi\rangle$ in equation (1) is just a short notation for the complex column vector

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

while its corresponding *bra* $\langle\psi|$ denotes the row vector $[\alpha^* \; \beta^*]$, where α^* and β^* are the complex conjugates of the complex numbers α and β, respectively.

Equation (1) reflects the fundamental difference distinguishing quantum bits from classical ones and is a direct application of the quantum principle of superposition of states. The qubit $|\psi\rangle$ is in a superposition of $|0\rangle$ and $|1\rangle$, a state in which it is not possible to say that the qubit is definitely in the state $|0\rangle$, or definitely in the state $|1\rangle$.

For a single qubit, there is a very intuitive geometric representation of its state as a point on a sphere. Taking $\alpha = e^{i\gamma}\cos(\theta/2)$ and $\beta = e^{i\gamma}e^{i\varphi}\sin(\theta/2)$ in equation (1), we can rewrite the state of qubit $|\psi\rangle$ as

$$|\psi\rangle = e^{i\gamma}(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle), \tag{2}$$

where θ, φ and γ are real numbers. Note that this is always possible since $|\alpha|^2 + |\beta|^2 = 1$. Also, because a global phase factor like $e^{i\gamma}$ has no observable effects (*i.e.* it does not influence the statistics of measurement predicted for qubit $|\psi\rangle$), we can effectively ignore it. Consequently, the pair (θ, φ) uniquely identifies a point $(\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)$ on a unit three-dimensional sphere called the *Bloch sphere* [19, 17].

Figure 1 depicts four possible states of a qubit using the Bloch sphere representation. Note that the states corresponding to the points on the equatorial circle have all equal contributions of 0-ness and 1-ness. What distinguishes them is the *phase*. For example, the two states displayed above, $1/\sqrt{2}(|0\rangle + |1\rangle)$ and $1/\sqrt{2}(|0\rangle - |1\rangle)$ are the same up to a relative phase shift of π, because the $|0\rangle$ amplitudes are identical and the $|1\rangle$ amplitudes differ only by a relative phase factor of $e^{i\pi} = -1$.

2.2 Measurements

We now turn our attention to the amount of information that can be stored in a qubit and, respectively, retrieved from a qubit. Since any point on the Bloch sphere can be characterized by a pair of real-valued parameters taking continuous values, it follows that, theoretically, a qubit could hold an infinite amount of information. As it turns out, however, we cannot extract more

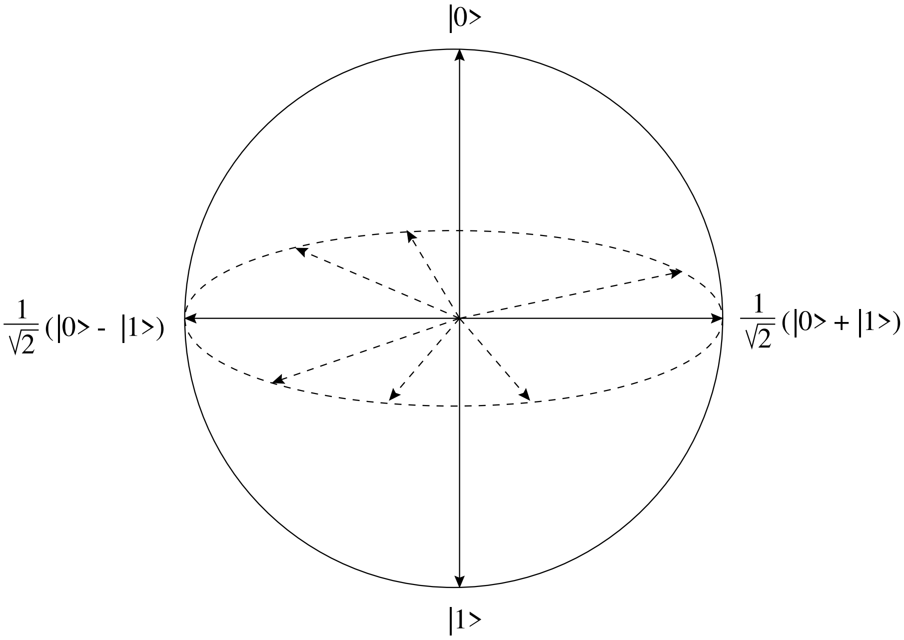

Figure 1: The Bloch sphere representation of a qubit.

information from such a qubit than we are able to extract from a classical bit. The reason is that we have to *measure* the qubit in order to determine in which state it is. Yet, according to a fundamental postulate of quantum mechanics (Postulate 3 in [17]), the amount of information that can be gained about a quantum state through measurement is restricted. Thus, when we measure 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 $|\beta|^2$. The condition that the probabilities must sum to one corresponds geometrically to the requirement that the qubit state be normalized to length 1, that is the inner product

$$\langle\psi|\psi\rangle = [\alpha^* \; \beta^*] \cdot \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha\alpha^* + \beta\beta^*$$

equals 1.

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.

Naturally, measurements in bases other than the computational basis are always possible, but this will not help us in determining α and β from a single measurement. In general, measurement of a state transforms the state into one of the measuring device's associated basis vectors. The probability that the state is measured as basis vector $|u\rangle$ is the square of the norm of the amplitude of the component of the original state in the direction of the basis vector $|u\rangle$. Unless the basis is explicitly stated, we will always assume that a measurement is performed with respect to the standard basis for quantum computation.

2.3 Putting qubits together

Let us examine now more complex quantum systems, composed of multiple qubits. In classical physics, individual two-dimensional state spaces of n particles combine through the Cartesian product to form a vector space of $2n$ dimensions, representing the state space of the ensemble of n particles. However, this is not how a quantum system can be described in terms of its components. Quantum states combine through the tensor product to give a resulting state space of 2^n dimensions, for a system of n qubits.

For a system of two qubits, each with basis $\{|0\rangle, |1\rangle\}$, the resulting state space is the set of normalized vectors in the four dimensional space spanned by basis vectors $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$, where $|x\rangle \otimes |y\rangle$ denotes the tensor product between column vectors $|x\rangle$ and $|y\rangle$. For example,

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \times 0 \\ 1 \times 1 \\ 0 \times 0 \\ 0 \times 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

It is customary to write the basis in the more compact notation $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. This generalizes in the obvious way to an n-qubit system with 2^n basis vectors.

2.4 Entanglement

Similar to single qubits, multiple-qubit systems can also be in a superposition state. The vector

$$|\Psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \tag{3}$$

describes a superposition state of a two-qubit system in which all four components (corresponding to the four basis vectors) have equal amplitudes. What about the two qubits composing the system? Can we characterize their states individually? If we rewrite equation (3) in order to express $|\Psi\rangle$ as the tensor product

$$|\Psi\rangle = (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \tag{4}$$

then we can legitimately assert that each of the component qubits is also in a superposition state, perfectly balanced between $|0\rangle$ and $|1\rangle$. Now let us drop the two middle terms in equation (3) and consider the superposition state described by

$$|\Phi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \tag{5}$$

In this case it is no longer possible to find complex numbers α, β, γ and δ such that

$$\begin{aligned}
&(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) = \\
&\quad = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \\
&\quad = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle
\end{aligned} \tag{6}$$

The state of the system cannot be decomposed into a product of the states of the constituents. Even though the state of the system is well defined (through the state vector $|\Phi\rangle$), neither of the two component qubits is in a well-defined state. This is again in contrast to classical systems, whose states can always be broken down into the individual states of their components. Furthermore, if we try to measure the two qubits, the superposition will collapse into one of the two basis vectors contributing to the superposition, and the outcomes of the two measurements will always coincide. In other words, if one of the qubits is found to be in state $|0\rangle$, then the second one will necessarily be in the same state, while a state $|1\rangle$ observed through measurement will be shared by both qubits. Therefore, we say that the two qubits are *entangled*[1] and $|\Phi\rangle$ describes an entangled state of the system.

Entanglement defines the strong correlations exhibited by two or more particles when they are measured, and which cannot be explained by classical means. This does not imply that entangled particles will always be observed in the same state, as entangled states like

$$\frac{1}{\sqrt{2}}|01\rangle \pm \frac{1}{\sqrt{2}}|10\rangle \tag{7}$$

prove it. In this last example, a measurement will always reveal the two qubits to be in opposite states (when one is 0 the other is 1 and vice-versa). States like these or the one in equation (5) are known as *Bell states* or *EPR pairs* after some of the people [11, 8] who pointed out their strange properties.

In some sense, we can say that superposition encompasses entanglement, since entanglement can be viewed as a special case of superposition. It is also interesting to make an analogy between entanglement and the concept of primality from number theory. Indeed, an entangled state of the system corresponds to a prime number, since it cannot be factored or decomposed as a product of subsystem states.

3 Quantum distinguishability

We introduce the problem of distinguishing quantum states through a metaphor involving two prototypical characters, named Alice and Bob. Suppose we have a fixed set of quantum states described using the usual Dirac notation $|\Psi_i\rangle$ $(1 \leq i \leq n)$ known to both Alice and Bob. Alice randomly chooses a state from the set and prepares a qubit (or set of qubits) in that particular state. She then gives the qubit(s) to Bob who is free to investigate (measure) them in any way he likes. His task is to identify the index i of the state characterizing the qubit(s) Alice has given him.

The only case in which a set of quantum states can be reliably (that is, 100% of the time) distinguished from one another is if they are pairwise orthogonal. For example, the four states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ form an orthonormal basis (each vector is a unit vector and distinct vectors have a zero inner product) for the state space spanned by two qubits. Consequently, they can be reliably distinguished by an appropriate measurement. In this

[1] It was Schrödinger who actually named the phenomenon *entanglement* in 1935 [18].

case, we can simply measure each qubit (sequentially) in the computational basis (defined by the basis vectors $|0\rangle$ and $|1\rangle$).

On the other hand, it is impossible to reliably distinguish $|0\rangle$ from $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. While the first state will consistently yield a 0 upon measurement, the second state also has a 50% chance to be observed as a 0. It is this component in the direction of the basis vector $|0\rangle$ which is present in both quantum states that prevents us from distinguishing them reliably. If the vectors describing the quantum states would be orthogonal, then a measurement basis would exist with respect to which the quantum states share no common components.

Consider now the case in which we try to distinguish between the four Bell states
$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, $\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$, $\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$, $\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$.
No sequential approach (that is, measuring the qubits one after the other) will be of any help here, regardless of the basis in which the measurements are performed. By measuring the two qubits, in sequence, in the computational basis, Bob can distinguish the states $\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ from $\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. He does this by checking if the outcomes of the two measurements are the same or not. But this kind of measurement makes it impossible to differentiate between $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, or between $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

Alternatively, Bob can decide to perform his measurements in a different basis, like $(|+\rangle, |-\rangle)$, where the basis vectors are

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

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

Due to the fact that

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|++\rangle + |--\rangle}{\sqrt{2}}$$

and

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}} = \frac{|+-\rangle + |-+\rangle}{\sqrt{2}},$$

Bob can now reliably distinguish the quantum state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ from $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. Indeed, if the two qubits yield identical outcomes when measured in this new basis, then we can assert with certainty that the state was not $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. Similarly, if the measurement outcomes for the qubits are different, the original state could not have been $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Unfortunately, in this new setup, the quantum states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ become indistinguishable and the same is true about $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

The computational bases $(|0\rangle, |1\rangle)$ and $(|+\rangle, |-\rangle)$ are, respectively, the two extremities of an (theoretically) infinite number of choices for the basis relative to which the quantum measurements are to be performed. But even though the separation line between the four Bell states will drift with the choice of the basis vectors, the two extreme cases discussed above offer the best possible distinguishability.

Intuitively, this is due to the entanglement exhibited between the two qubits in all four states. As soon as the first qubit is measured (regardless of the basis), the superposition describing the entangled state collapses to the specific state consistent with the measurement result. In this process, some of the information originally encapsulated in the entangled state is irremediably lost. Consequently, measuring the second qubit cannot give a complete separation of the four EPR states. But the Bell states do form an orthonormal basis, which means that (at least theoretically) they can be distinguished by an appropriate quantum measurement. However, this measurement must be a *joint* measurement of both qubits simultaneously, in order to achieve the desired distinguishability. Not surprisingly, this is very difficult to accomplish in practice.

The distinguishability of the four Bell (or EPR) states is the key feature in achieving superdense coding [9]. However, in the experimental demonstration of this protocol [12] two of the possibilities cannot be distinguished from one another, precisely because of the difficulties associated with implementing a joint measurement.

4 Generalization

A more compact representation of the Bell basis is through a square matrix where each column is a vector describing one of the Bell states:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}$$

The elements of each column are the amplitudes or proportions in which the computational basis states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ are present in the respective EPR state.

This scenario can be extended to ensembles of more than two qubits. The following matrix describes eight different entangled states that cannot be reliably distinguished unless a joint measurement of all three qubits involved is performed:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

In general, for a quantum system composed of n qubits, one can define the following 2^n entangled states of the system:

$$\tfrac{1}{\sqrt{2}}(|000\cdots 0\rangle \pm |111\cdots 1\rangle)$$

$$\tfrac{1}{\sqrt{2}}(|000\cdots 1\rangle \pm |111\cdots 0\rangle)$$

$$\vdots$$

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

These vectors form an orthonormal basis for the state space corresponding to the n-qubit system. The only chance to differentiate among these 2^n states using quantum measurement(s) is to observe the n qubits simultaneously, that is, perform a single joint measurement of the entire system. In the given context, *joint* is really just a synonym for *parallel.* Indeed, the device in charge of performing the joint measurement must posses the ability to "read" the information stored in each qubit, in parallel, in a perfectly synchronized manner. In this sense, at an abstract level, the measuring apparatus can be viewed as having n probes. With all probes operating in parallel, each probe can "peek" inside the state of one qubit, in a perfectly synchronous operation. The information gathered by the n probes is seen by the measuring device as a single, indivisible chunk of data, which is then interpreted to give one the 2^n entangled states as the measurement outcome.

¿From a mathematical (theoretical) point of view, such a measurement operator can be easily constructed by defining each of the 2^n states that are to be distinguished to be a projector associated with the measurement operation. We are well aware though, that a physical realization of this mathematical construction is extremely difficult, if not impossible to achieve in practice, with today's technology. The experimental demonstration of the superdense coding protocol mentioned at the end of previous section clearly shows this difficulty (for just two qubits!). Yet, if there is any hope to see a joint measurement performed in the future, then only a device operating in a parallel synchronous fashion on all n qubits (as explained above) would succeed.

It is perhaps worth emphasizing that if such a measurement cannot be applied then the desired distinguishability can no longer be achieved regardless of how many other measuring operations we are allowed to perform. In other words, even an infinite sequence of measurements touching at most $n-1$ qubits at the same time cannot equal a single joint measurement involving all n qubits.

Furthermore, with respect to the particular distinguishability problem that we have to solve, a single joint measurement capable of observing $n-1$ qubits simultaneously offers no advantage whatsoever over a sequence of $n-1$ consecutive *single* qubit measurements. This is due to the fact that an entangled state like

$$\frac{1}{\sqrt{2}}(|000\cdots 0\rangle + |111\cdots 1\rangle)$$

cannot be decomposed neither as a product of $n-1$ individual states nor as a product of two states (one describing a single qubit and the other describing the subsystem composed of the remaining $n-1$ qubits). Any other intermediate decomposition is also impossible.

5 Universal Computation

Finally, we relate the example presented in this paper with the hypothetical notion of a Universal Computer, as defined in [5]. Such a machine must be able to follow (execute) the steps of any program made up of basic input, output, arithmetic and logical operations. It must also have a means of communicating with the outside world at any time during a computation, either for receiving input or producing output. The program, the input, the output and all intermediate results are stored in (and can be retrieved from) a memory which is generously allowed to be unlimited.

To make this Universal Computer a "realistic" model of computation, it is subjected to the *finiteness condition*: In one step, requiring one time unit, the Universal Computer can execute a finite and fixed number of basic operations. It is precisely this limitation (quite natural and reasonable) that makes the Universal Computer a utopian concept. Specifically, three classes of computable functions $\mathcal{F}$ are described in [5], which cannot be computed by any machine obeying the finiteness condition.

One of these classes of problems involves measuring a set of interacting variables. Formally, suppose there are n variables x_0, x_1, $\cdots$, x_{n-1}. These variables may represent the parameters of a physical or biological system. The dependence of each variable on all others induces the system to continually evolve until a state of equilibrium may eventually be reached. In the absence of any external perturbations, the system can remain in a stable state indefinitely. We can model the interdependence between the n variables through a set of functions, as follows:

$$\begin{aligned}
x_0(t+1) &= f_0(x_0(t), x_1(t), \ldots, x_{n-1}(t)) \\
x_1(t+1) &= f_1(x_0(t), x_1(t), \ldots, x_{n-1}(t)) \\
&\vdots \\
x_{n-1}(t+1) &= f_{n-1}(x_0(t), x_1(t), \ldots, x_{n-1}(t))
\end{aligned} \tag{8}$$

This system of equations describes the evolution of the system from state $(x_0(t), x_1(t), \ldots, x_{n-1}(t))$ to state $(x_0(t+1), x_1(t+1), \ldots, x_{n-1}(t+1))$, one time unit later. In the case where the system has reached equilibrium, its parameters will not change over time. It is important to emphasize that, in most cases, the dynamics of the system are very complex, so the mathematical description of functions $f_0, f_1, \ldots, f_{n-1}$ is either not known to us or we only have rough approximations for them.

Assuming the system is in an equilibrium state, our task is to measure its parameters in order to compute a function $\mathcal{F}$, possibly a global property of the system at equilibrium. In other words, we need the values of $x_0(\tau), x_1(\tau), \ldots, x_{n-1}(\tau)$ at moment τ, when the system is in a stable state, in order to compute

$$\mathcal{F}(x_0(\tau), x_1(\tau), \ldots, x_{n-1}(\tau)).$$

We can obtain the value of $x_0(\tau)$, for instance[2], by measuring the respective parameter at time τ. Although we can acquire the value of $x_0(\tau)$ easily in this way, the consequences for the entire system can be dramatic. Unfortunately, any measurement is an external perturbation for the system, and in the process, the parameter subjected to measurement will be affected unpredictably.

Thus, the measurement operation will change the state of the system from $(x_0(\tau), x_1(\tau), \ldots, x_{n-1}(\tau))$ to $(x'_0(\tau), x_1(\tau), \ldots, x_{n-1}(\tau))$, where $x'_0(\tau)$ denotes the value of variable x_0 after measurement. Since the measurement process has a non-deterministic effect upon the variable being measured, we cannot estimate $x'_0(\tau)$ in any way. Note also that the transition from $(x_0(\tau), x_1(\tau), \ldots, x_{n-1}(\tau))$ (that is, the state before measurement) to $(x'_0(\tau), x_1(\tau), \ldots, x_{n-1}(\tau))$ (that is, the state after measurement) does not correspond to the normal evolution of the system according to its dynamics described by functions f_i, $0 \leq i < n$.

However, because the equilibrium state was perturbed by the measurement operation, the system will react with a series of state transformations, governed by equations (8). Thus, at each time step after τ, the parameters of the system will evolve either towards a new equilibrium state or maybe fall into a chaotic behavior. In any case, at time $\tau + 1$, all n variables have acquired new values, according to the expressions of functions f_i:

$$x_0(\tau + 1) \;=\; f_0(x'_0(\tau), x_1(\tau), \ldots, x_{n-1}(\tau))$$

[2]The choice of x_0 here is arbitrary. The argument remains the same regardless of which of the n parameters we choose to measure first.

$$
\begin{aligned}
x_1(\tau+1) &= f_1(x'_0(\tau), x_1(\tau), \ldots, x_{n-1}(\tau)) \\
&\vdots \\
x_{n-1}(\tau+1) &= f_{n-1}(x'_0(\tau), x_1(\tau), \ldots, x_{n-1}(\tau))
\end{aligned}
\tag{9}
$$

Consequently, unless we are able to measure all n variables, in parallel, at time τ, some of the values composing the equilibrium state

$$(x_0(\tau), x_1(\tau), \ldots, x_{n-1}(\tau))$$

will be lost without any possibility of recovery.

The finiteness condition restricts in this case the number of variables that can be measured in parallel. So, if the Universal Computer is able to measure n variables in parallel (that is, during one step), where n can be arbitrarily large, but finite, then the Universal Computer will fail to solve the same problem for a system involving $n+1$ variables. In other words, the Universal Computer cannot simulate a computation that is perfectly possible for another machine. However, it is exactly the principle of *simulation* that lies at the heart of *universality*.

Choosing a machine endowed with $n+1$ probes (and therefore capable of measuring $n+1$ variables in parallel) as the Universal Computer is not a solution. By an adversary argument, we can construct an instance of the above problem, only this time involving $n+2$ parameters to be measured, and the Universal Computer will fail once again to compute the required function $\mathcal{F}$, although it can be trivially computed by a machine with $n+2$ probes. This argument is valid for *any* given Universal Computer, having a fixed (and finite) number of probes and therefore a limited degree of parallelism to tackle such inherently parallel tasks.

Coming back to the example presented in this paper, it is easy to see that a device capable of measuring at most n qubits simultaneously (where n is a fixed, finite number) will fail to solve the distinguishability problem for $n+1$ qubits. Our example, taken from the quantum information area is similar in nature with the interacting variables example described in [5] and supports the idea formulated therein about the impossibility of realizing the concept of a Universal Computer. In the case that we have described, interdependence between variables takes the form of entanglement between qubits, the phenomenon ultimately responsible for making a parallel approach imperative.

6 Conclusion

We have exhibited an example of a task which cannot be successfully completed unless a parallel approach is employed. The task is to distinguish between the elements of a set of quantum states, using any quantum measurements that can be theoretically applied. There are no restrictions concerning the number of measurements allowed or the time when the task has to be completed. We have shown that there exists a set of entangled states, forming an orthonormal basis in the state space spanned by n qubits, for which only a *joint* measurement (in that respective basis) of all the qubits composing the system can achieve perfect distinguishability. An important characteristic of the task is that if the degree of parallelism necessary to successfully solve the problem is not available, then the solution is no better than a purely sequential approach. Such inherently parallel tasks have been shown to exist in a variety of environments, namely, real-time systems [4], dynamical systems [1, 7, 6] and geometric problems [3].

In this paper, we have shown that parallelism is equally important for yet another computational paradigm, essentially different from the classical theory of computation, namely quantum computation and quantum information. It is important to note that we refer here to the common understanding of the term *parallelism* and not to *quantum parallelism*. The latter syntagm is used to denote the ability to perform a certain computation simultaneously on all terms of a quantum superposition, regardless of the number of qubits composing the quantum register whose state is described by that superposition. As opposed to this interpretation, we refer to parallelism as the ability to act simultaneously on a certain number of qubits. Thus, we can rightfully assert that parallelism transcends the laws of physics and represents a fundamental aspect of computation, regardless of the particular physical way chosen to embody information.

The second contribution of the paper addresses the notion of a Universal Computer obeying the finiteness condition [5]. Distinguishing between entangled quantum states is, conceptually, a quantum example of measuring interdependent variables. This problem, arising in quantum information theory, strengthens the conclusion that there is no *finite*[3] computing device (conventional or unconventional) upon which the attribute *universal* can be bestowed.

References

[1] Selim G. Akl. Coping with uncertainty and stress: A parallel computation approach. To appear in the *International Journal of High Performance Computing and Networking.*

[2] Selim G. Akl. Discrete steepest descent in real time. *Parallel and Distributed Computing Practices*, 4(3):301–317, 2001.

[3] Selim G. Akl. Inherently parallel geometric problems. Technical Report 2004–480, School of Computing, Queen's University, Kingston, Ontario, April 2004. 19 pages.

[4] Selim G. Akl. Superlinear performance in real-time parallel computation. *The Journal of Supercomputing*, 29(1):89–111, 2004.

[5] Selim G. Akl. The myth of universal computation. Technical Report 2005–492, School of Computing, Queen's University, Kingston, Ontario, January 2005. 21 pages.

[6] Selim G. Akl, Brendan Cordy, and W. Yao. An analysis of the effect of parallelism in the control of dynamical systems. To appear in the *International Journal of Parallel, Emergent and Distributed Systems.*

[7] Selim G. Akl and W. Yao. Parallel computation and measurement uncertainty in nonlinear dynamical systems. *Journal of Mathematical Modelling and Algorithms, Special Issue on Parallel and Scientific Computations with Applications*, 4:5–15, 2005.

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

[9] 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.

[3] in the sense introduced in [5] and briefly described in the previous section.

[10] P. Dirac. *The Principles of Quantum Mechanics.* Oxford University Press, 4th edition, 1958.

[11] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, May 1935.

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

[13] Marius Nagy and Selim G. Akl. Real-time minimum vertex cover for two-terminal series-parallel graphs. In *Proceedings of the Thirteenth IASTED International Conference on Parallel and Distributed Computing and Systems*, pages 526–534, Anaheim, California, August 2001.

[14] Marius Nagy and Selim G. Akl. Locating the median of a tree in real time. In *Proceedings of the Fourteenth IASTED International Conference on Parallel and Distributed Computing and Systems*, pages 108–113, Cambridge, Massachusetts, November 2002.

[15] Marius Nagy and Selim G. Akl. Computing nearest neighbors in real time. In *Proceedings of the Fifteenth IASTED International Conference on Parallel and Distributed Computing and Systems*, volume II, pages 518–524, Marina Del Rey, California, November 2003.

[16] Naya Nagy and Selim G. Akl. The maximum flow problem: A real-time approach. *Parallel Computing*, 29:767–794, 2003.

[17] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[18] Erwin Schrödinger. Discussion of probability relations between separated systems. *Proceedings of the Cambridge Philosophical Society*, 31:555–563, 1935.

[19] Eric W. Weisstein et al. *Bloch sphere.* From *MathWorld*–A Wolfram Web Resource. http://mathworld.wolfram.com/BlochSphere.html.