On the Necessity of Entanglement for the Explanation of Quantum Speedup*

Michael E. Cuffaro

The University of Western Ontario, Department of Philosophy

March 28, 2013

Contents

*This paper has been adapted from Chapter 3 of Cuffaro (2013). I am indebted to Wayne Myrvold for discussion and for his comments and criticisms on earlier drafts.

1 Introduction

The significance of the phenomenon of quantum entanglement—wherein the most precise characterisation of a quantum system composed of previously interacting subsystems does not necessarily include a precise characterisation of those subsystems—has been at the forefront of the debate over the conceptual foundations of quantum theory, almost since that theory's inception. It is *the* distinguishing feature of quantum theory, for some (Schrödinger, 1935).[1] For others, it is evidence for the incompleteness of that theory (Einstein, Podolsky, & Rosen, 1935).[2] For yet others, the possibility of entangled quantum systems implies that physical reality is essentially non-local (Stapp, 1997).[3] For almost all, it has been, and continues to be, an enigma requiring a solution.

For most of the history of quantum theory, serious investigation into the significance and implications of entanglement has been conducted mainly by philosophers of physics and by a few philosophically-minded theoretical and experimental physicists interested in foundational issues. With the advent of quantum information theory, this has begun to change. In quantum information theory, quantum mechanical systems are utilised to implement communications protocols and computational algorithms that are faster and more efficient than any of their known classical counterparts. Because it is almost surely the case that one or more of the fundamental distinguishing aspects of quantum mechanics is responsible for this 'quantum advantage', quantum information theory has precipitated an explosion of physical research into the traditionally foundational issues of quantum theory.

Of the many and varied applications of quantum information theory, perhaps the most fascinating is the sub-field of quantum computation. In this sub-field, computational algorithms are designed which utilise the resources available in quantum systems in order to compute solutions to computational problems with, in some cases, exponentially fewer resources than any known classical algorithm. A striking example of this so-called 'quantum speedup' is Shor's algorithm (Shor, 1997) for factoring integers. A basic distinction, in computational complexity theory, is between those computational problems that are amenable to an *efficient* solution in terms of time and space resources, and those that are not. Easy (or 'tractable', 'feasible', 'efficiently solvable', etc.) problems are those which involve resources bounded by a polynomial in the input size, n (n^c time steps, for instance, where c is some constant). Hard problems are those which are not easy; they are those problems whose solution requires resources that are 'exponential' in n, i.e., that grow faster than any polynomial in n.[4,5] The factoring problem is believed to be hard, classically, and indeed, much of current Internet security relies on this fact. Shor's quantum algorithm for factoring

[1] For some more recent speculation on the the distinguishing feature(s) of quantum mechanics, see, for instance, Clifton et al. (2003); Myrvold (2010).

[2] For further discussion, and for Einstein's later refinements of the Einstein-Podolsky-Rosen (EPR) paper's main argument, see Howard (1985).

[3] For responses to Stapp's view and for further discussion, see: Unruh (1999); Mermin (1998); Stapp (1999).

[4] As this class of problems includes those solvable in, for instance, $n^{\log n}$ steps, this convention abuses, somewhat, the term exponential, hence my use of inverted commas.

[5] As we will discuss in more detail later, the easy-hard distinction is not meant to reflect any deep mathematical truth about the nature of computational algorithms, but is rather meant as a practical characterisation of what we normally associate with efficiency.

integers, however, makes the factoring problem efficiently solvable.

While the fact of quantum computational speedup is almost beyond doubt,[6] the source of quantum speedup is still a matter of debate. Candidate explanations of quantum speedup range from the purported ability of quantum computers to perform multiple function evaluations simultaneously (Deutsch, 1997; Duwell, 2004; Hewitt-Horsman, 2009),[7] to the purported ability of a quantum computer to compute a global property of a function without evaluating *any* of its values (e.g. Steane, 2003; Bub, 2010).

In most of these candidate explanations, the fact that quantum mechanical systems can sometimes exhibit *entanglement* plays an important role. On A.M. Steane's view, for instance, quantum entanglement allows one to manipulate the correlations between the values of a function without manipulating those values themselves. For proponents of the many worlds explanation, on the other hand, though they consider computational worlds to be the main component in the explanation of quantum speedup, they nevertheless view entanglement as indispensable to its analysis (Hewitt-Horsman, 2009, 889). It is thus somewhat disconcerting that recent physical research seems to suggest that entanglement, rather than being indispensable, may be irrelevant to the general explanation of quantum speedup.

Logically, entanglement may play the role of either a necessary or a sufficient condition (or both) in an overall explanation of quantum speedup. I address the question of whether entanglement may be said to be a sufficient condition elsewhere (Cuffaro, 2013). As for the assertion that entanglement is a necessary component in the explanation of speedup, this seems, prima facie, to be supported[8] by a result due to Jozsa & Linden (2003), who prove that for quantum algorithms which utilise *pure* states, "the presence of multi-partite entanglement, with a number of parties that increases unboundedly with input size, is necessary if the quantum algorithm is to offer an exponential speed-up over classical computation" (2003, p. 2014). When we consider quantum algorithms which utilise *mixed* states, however, then there appear to be counterexamples to the assertion that one must appeal to quantum entanglement in order to explain quantum speedup. In particular, Biham et al. (2004) have shown that it is possible to achieve a modest (sub-exponential) speedup using unentangled mixed states. Further, Datta et al. (2005, 2008) have shown that it is possible to achieve an exponential speedup using mixed states that contain only a vanishingly small amount of entanglement. In the latter case, further investigation has suggested to some that quantum correlations *other than* entanglement may be playing a more important role. One quantity in particular, *quantum discord*, appears to be intimately connected to the speedup that is present in the algorithm in question. In light of these results, it is tempting to conclude that it is not necessary to appeal to entanglement at all in order to explain quantum computational speedup and that the investigative focus should shift to the physical characteristics of

[6] Just as with other important problems in computational complexity theory, such as the $\mathbf{P} = \mathbf{NP}$ problem, there is currently no proof, though it is very strongly suspected to be true, that the class of problems efficiently solvable by a quantum computer is larger than the class of problems efficiently solvable by a classical computer.

[7] For criticisms of the version of this view that takes this parallel computation to occur in many parallel universes, see, for instance, Steane (2003); Duwell (2007); Cuffaro (2012).

[8] What I take to be supported by Jozsa & Linden's result is the claim that entanglement is required in order *to explain* quantum speedup. As we will discuss further in §3.2, this is distinct from the claim that one requires an entangled quantum state in order to achieve quantum speedup.

quantum discord or some other such quantum correlation measure instead.

In this paper I will argue that this conclusion is premature and misguided, for as I will show below, there is an important sense in which entanglement can indeed be said to be necessary for the explanation of the quantum speedup obtainable from both of these mixed-state quantum algorithms.

I will proceed as follows. After introducing the concept of entanglement and how it is quantified in §2, I introduce the *necessity of entanglement for explanation thesis* in §3.2. In §3.3, I show how what looks like a counter-example to the necessity of entanglement for explanation thesis for pure states—the fact that certain important quantum algorithms can be expressed so that their states are never entangled—is instead evidence for this thesis. Then, in §4, I examine the more serious challenges to the necessity of entanglement for explanation thesis posed by the cases of sub-exponential speedup with unentangled mixed states (§4.1) and exponential speedup with mixed states containing only a vanishingly small quantity of entanglement (§4.3).

Starting with the first type of counter-example, I begin by arguing that pure quantum states should be taken to provide a more fundamental representation of quantum systems than mixed states. I then show that when one considers the initially mixed state of the quantum computer as representing the space of its possible pure state preparations, the speedup obtainable from the computer can be seen as stemming from the fact that the quantum computer evolves some of these possible pure state preparations to entangled states—that the quantum speedup of the computer can be seen as arising from the fact that it implements an entangling transformation.

As for the second type of counter-example, where exponential speedup is achieved with only a vanishingly small amount of entanglement, and where it is held by some that another type of non-classical correlation, quantum discord, is responsible for the speedup of the quantum computer: I argue that, first, it is misleading to characterise discord as indicative of non-classical correlations. I then appeal to recent work done by Fanchini et al. (2011), Brodutch & Terno (2011), and Cavalcanti et al. (2011) who show, respectively, that when one considers the 'purified' state representation of the quantum computer, there is a conservation relation between discord and entanglement, and indeed that there is just as much entanglement in such a representation as there is discord in the mixed state representation; that entanglement must be shared between two parties in order to bilocally implement any bipartite quantum gate; and that entanglement is directly involved in the operational definition of quantum discord.

Given Jozsa & Linden's proof of the necessary presence of an entangled state for exponential speedup using pure states, and given the fundamentality of pure states as representations of quantum systems, the burden of proof is upon those who would deny the necessity of entanglement for explanation thesis to show either by means of a counter-example or by some other more principled method that it is false. Neither of the counter-examples discussed in this paper succeeds in doing so. We should conclude, therefore, that the necessity of entanglement for explanation thesis is true.

2 Preliminaries

2.1 Quantum entanglement

Consider the following representation of the joint state of two qubits:[9]

$$|\psi\rangle = |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle.$$

This expression for the overall state of the system represents the fact that the two qubits are in an equally weighted superposition of the four joint states (a)-(d) below:

$$\begin{array}{ccc} & q_1 & q_2 \\ \text{(a)} & |0\rangle & |0\rangle \\ \text{(b)} & |0\rangle & |1\rangle \\ \text{(c)} & |1\rangle & |0\rangle \\ \text{(d)} & |1\rangle & |1\rangle. \end{array}$$

This particular state is a *separable* state, for it can, alternatively, be expressed as a product of the pure states of its component systems, as follows:

$$|\psi\rangle = (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle).$$

Not all quantum mechanical states can be expressed as product states of their component systems, and thus not all quantum mechanical states are separable. Here are four such 'entangled' states:[10]

$$\begin{aligned} |\Phi^+\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\ |\Phi^-\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\ |\Psi^+\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} \\ |\Psi^-\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \end{aligned}$$

The skeptical reader is encouraged to convince himself that it is impossible to re-express any of these states as a product state of two qubits. They are called the Bell states, and I will refer to a pair of qubits jointly in a Bell state as a Bell pair.[11] Maximally entangled

[9] A qubit is the basic unit of quantum information, analogous to a classical bit. It can be physically realised by any two-level quantum mechanical system. Like a bit, it can be "on": $|1\rangle$ or "off": $|0\rangle$, but unlike a bit it can also be in a superposition of these values.

[10] From now on, I will usually, for brevity, omit the tensor product symbol from expressions for states of multi-particle systems; i.e., $|\alpha\beta\rangle$ and $|\alpha\rangle|\beta\rangle$ should be understood as shorthand forms of $|\alpha\rangle \otimes |\beta\rangle$.

[11] These are also sometimes referred to as 'EPR pairs'. EPR stands for Einstein, Podolsky, and Rosen. In their seminal 1935 paper, EPR famously used states analogous to the Bell states to argue that quantum mechanics is incomplete.

states,[12] such as these, completely specify the correlations between outcomes of experiments on their component qubits without specifying anything regarding the outcome of a single experiment on one of the qubits. For instance, in the singlet state (i.e., $|\Psi^-\rangle$), outcomes of experiments on the first and second qubits are perfectly anti-correlated with one another. If one performs, say, a $\hat{z}$ experiment on one qubit of such a system, then if the result is $|0\rangle$, a $\hat{z}$ experiment on the other qubit will, with certainty, yield an outcome of $|1\rangle$, and vice versa. In general, the expectation value for joint measurements on the two qubits is given by $-\hat{m}\cdot\hat{n} = -\cos\theta$, where $\hat{m}, \hat{n}$ are unit vectors representing the orientations of the two experimental devices, and θ is the difference in these orientations. Any single $\hat{z}$ experiment on just one of the two qubits, however, will yield $|0\rangle$ or $|1\rangle$ with equal probability.

We will put to one side the question of the *physical significance* of quantum entanglement. I discuss this at greater length in Chapters 4 and 5 of Cuffaro (2013). For the purposes of this paper it is most appropriate to give as minimal and uncontroversial a characterisation of entanglement as possible.

2.2 Entangled mixed states

The concepts of separability and of entanglement are also applicable to so-called 'mixed states'. To illustrate the concept of a mixed state, imagine that one draws a ball from an urn into which balls of different types have been placed, and that the probability of drawing a ball of type i is p_i. Corresponding to the outcome i, we then prepare a given system S in the pure state $|\psi_i\rangle$, representable by the density operator $\rho_i^S = |\psi_i\rangle\langle\psi_i|$. After preparing ρ_i^S, we then discard our record of the result of the draw. The resulting state of the overall system will be the mixed state:

$$\rho = \sum_i p_i \rho_i^S. \tag{2.1}$$

A *mixed state* is *separable* if it can be expressed as a mixture of pure product states, and *entangled* otherwise. In general, determining whether a mixed state of the form (2.1) is an entangled state is difficult, because in general the decomposition of mixtures is non-unique. For instance, the reader can verify that a mixed state represented by the density operator ρ, prepared as a mixture of pure states in the following way:

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|,$$

can also be equivalently prepared as:

$$\rho = \frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|\phi\rangle\langle\phi|,$$

where

$$|\psi\rangle \equiv \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle, \quad |\phi\rangle \equiv \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle.$$

[12]Note that not all entangled states are maximally entangled states. We will discuss this in more detail shortly.

This is so because both state preparations yield an identical density matrix representation (in the computational basis); i.e.,:

$$\begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix}.$$

As we will see in more detail later, a system that is prepared as a mixture of entangled states will sometimes yield the same density operator representation as a system prepared as a mixture of pure product states.

2.3 Quantifying entanglement

Entanglement is a potentially useful resource for quantum information processing. Masanes (2006) has shown, for instance, that for any non-separable state ρ, some other state σ is capable of having its teleportation fidelity enhanced by ρ's presence.[13] Given this, it is useful to be able to quantify the amount of entanglement contained in a given state. In order to do this, we employ so-called entanglement measures. Using such measures, it is easy to see, for instance, that the state

$$|\phi\rangle = \sqrt{\frac{1}{3}}|01\rangle + \sqrt{\frac{2}{3}}|10\rangle, \tag{2.2}$$

though entangled, is not a maximally entangled state (unlike the Bell states we encountered in §2.1, which are maximally entangled). This is explained in more detail in Cuffaro (2013), where a description of various entanglement measures is also given. This can also be found in Plenio & Virmani (2007).

2.4 Purification

Every mixed state can be thought of as the result of taking the partial trace of a pure state acting on a larger Hilbert space. In particular, for a mixed state ρ_A acting on a Hilbert space $\mathcal{H}_A$, with spectral decomposition $\sum_k p_k|k\rangle\langle k|$ for some orthonormal basis $\{|k\rangle\}$, a purification (in general non-unique) of ρ_A may be given by

$$|\psi_{AB}\rangle = \sum_k \sqrt{p_k}|k_A\rangle \otimes |k_B\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B,$$

where $\mathcal{H}_B$ is a copy of $\mathcal{H}_A$. We then have $\rho_A = \mathrm{tr}_B(|\psi_{AB}\rangle\langle\psi_{AB}|)$, with $|\psi_{AB}\rangle$ an entangled state.

3 Entanglement in the quantum computer

3.1 The Deutsch-Jozsa algorithm

Deutsch's problem (Deutsch, 1985) is the problem to determine whether a given function $f : \{0,1\} \rightarrow \{0,1\}$ is constant or balanced. Such a function is constant if it produces the

[13] The teleportation fidelity (cf. Nielsen & Chuang, 2000, §9.2.2) is a measure of the 'closeness' of the input and output states in the teleportation protocol (cf. Bennett et al., 1993).

same output value for each of its inputs; it is balanced if the output of one half of the inputs is the opposite of the output of the other half. Thus, the constant functions from $\{0,1\} \to \{0,1\}$ are $f(x) = 0$ and $f(x) = 1$; the balanced functions are the identity and bit-flip functions.

A generalised version of this problem enlarges the class of functions under consideration so as to include all of the functions $f : \{0,1\}^n \to \{0,1\}$. Its quantum solution is given by the Deutsch-Jozsa algorithm (Deutsch & Jozsa, 1992). In Cleve et al.'s improved version (Cleve et al., 1998), the algorithm begins by initialising the quantum registers of the computer to $|0^n\rangle|1\rangle$, after which we apply a Hadamard transformation[14] to all $n+1$ qubits, so that:

$$\begin{aligned} |0^n\rangle|1\rangle \xrightarrow{H} & \left(\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)^n\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \left(\frac{1}{2^{n/2}}\sum_x^{2^n-1}|x\rangle\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right). \end{aligned} \tag{3.1}$$

The unitary transformation,

$$U_f(|x\rangle|y\rangle) =_{df} |x\rangle|y \oplus f(x)\rangle, \tag{3.2}$$

is then applied, which has the effect:[15]

$$\xrightarrow{U_f} \left(\frac{1}{2^{n/2}}\sum_x^{2^n-1}(-1)^{f(x)}|x\rangle\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right). \tag{3.3}$$

If f is constant and $= 0$, this, along with a Hadamard transformation applied to the first n qubits, will result in:

$$f = 0: \qquad \left(\frac{1}{2^{n/2}}\sum_x^{2^n-1}|x\rangle\right)|-\rangle \xrightarrow{H^n \otimes I} |0^n\rangle|-\rangle,$$

where $|-\rangle =_{df} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. Otherwise if f is constant and $= 1$, then this, along with a Hadamard transformation applied to the first n qubits, will result in:

$$f = 1: \qquad -\left(\frac{1}{2^{n/2}}\sum_x^{2^n-1}|x\rangle\right)|-\rangle \xrightarrow{H^n \otimes I} -|0^n\rangle|-\rangle.$$

In either case, a measurement in the computational basis on the first n qubits yields the bit string $z = 000\ldots0 = 0^n = 0$ with certainty. If f is balanced, on the other hand, then half of the terms in the superposition of values of x in (3.3) will have positive phase, and half

[14] The Hadamard transformation (also called a Hadamard 'gate') takes $|0\rangle$ to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle$ to $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ and vice-versa.

[15] Given the state $|x\rangle(|0\rangle - |1\rangle)$ (omitting normalisation factors for simplicity), note that when $f(x) = 0$, applying U_f yields $|x\rangle(|0 \oplus 0\rangle - |1 \oplus 0\rangle) = |x\rangle(|0\rangle - |1\rangle)$; and when $f(x) = 1$, applying U_f yields $|x\rangle(|0 \oplus 1\rangle - |1 \oplus 1\rangle) = |x\rangle(|1\rangle - |0\rangle) = -|x\rangle(|0\rangle - |1\rangle)$.

negative. After applying the final Hadamard transform, the amplitude of $|0^n\rangle$ will be zero.[16] Thus a measurement of these qubits *cannot* produce the bit string $z = 000\ldots0 = 0^n = 0$. In sum, if the function is constant, then $z = 0$ with certainty, and if the function is balanced, $z \neq 0$ with certainty. In either case, the probability of success of the algorithm is 1, using only a *single* invocation. This is exponentially faster than any known classical solution.

3.2 The necessity of entanglement for explanation thesis

In the literature on quantum computation (cf. Ekert & Jozsa 1998; Steane 2003) it is often suggested that entanglement, such as that present in states like (3.3), is *required* if a quantum algorithm is to be capable of achieving a speedup over its classical alternatives. I will call this the *necessity of an entangled state* thesis (NEST). I will call the related claim that entanglement is a necessary component of any *explanation* for quantum speedup the *necessity of entanglement for explanation* thesis (NEXT).[17]

Note that although the NEXT is related to the NEST, these two claims are not strictly speaking identical. As we will see in §4.1, it is possible for the NEXT to be true even if the NEST is false (in the technical sense of §2.2), and it is not incoherent to argue that the NEXT is false by citing, as a counter-example, a quantum computer whose state is always entangled, as we shall see in §4.3.

3.3 De-quantisation

At first sight the following consideration seems problematic for both the NEST and the NEXT. Consider the Deutsch-Jozsa algorithm (cf. §3.1) for the special case of $n = 1$. This case is essentially a solution for Deutsch's problem. Deutsch's (1985) original solution to this problem is regarded as the first quantum algorithm ever developed and as the first example of what has since come to be known as quantum speedup. If one considers the steps of the algorithm as given in §3.1, however, then the reader can confirm that, when $n = 1$, at no time during the computation are the two qubits employed actually entangled with one another. The thesis that entanglement is a necessary condition for quantum speedup thus seems false. But the situation is not as dark for the NEST and the NEXT as it appears, since for the case of $n = 1$, it is also the case that the problem can be 'de-quantised', i.e., solved just as efficiently using classical means.

[16] To illustrate, consider the case where $n = 2$. After applying U_f, the computer will be in the state: $(|00\rangle - |01\rangle + |10\rangle - |11\rangle)|-\rangle$. Applying a Hadamard transform to the two input qubits will yield:

$$\begin{aligned} & \Big((|00\rangle + |01\rangle + |10\rangle + |11\rangle) - (|00\rangle - |01\rangle + |10\rangle - |11\rangle) \\ + \quad & (|00\rangle + |01\rangle - |10\rangle - |11\rangle) - (|00\rangle - |01\rangle - |10\rangle + |11\rangle)\Big)|-\rangle \\ = \quad & (0|00\rangle + \ldots)|-\rangle. \end{aligned}$$

[17] The attentive reader who has noticed that there is actually no entanglement in (3.3) when $n = 1$ will be somewhat puzzled by both of these theses. In fact, as we will see, entanglement will only appear for $n \geq 3$. In what follows I will argue, however, that this turns out to be evidence for, not against, the NEXT, and indeed does not contradict the NEST. This will be clarified in the next section.

One method for doing this (cf. Abbott, 2012) is with a computer which utilises the complex numbers $\{1, i\}$ as a computational basis in lieu of $\{|0\rangle, |1\rangle\}$. A complex number $z \in \mathbb{C}$ can be written as $z = a + bi$, where $a, b \in \mathbb{R}$, and thus can be expressed as a superposition of the basis elements in much the same way as a qubit.[18] The algorithm proceeds in the following way. We first note that the action of U_f on the first n qubits in Eq. (3.3) can, for the case of $n = 1$, be expressed as:[19]

$$\begin{aligned} &\frac{1}{\sqrt{2}}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big) \\ =&\frac{(-1)^{f(0)}}{\sqrt{2}}\Big(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\Big). \end{aligned}$$

We now define an operator C_f, analogously to U_f, that acts on a complex number as follows:

$$C_f(a + bi) = (-1)^{f(0)}\Big(a + (-1)^{f(0)\oplus f(1)}bi\Big).$$

When f is constant, the reader can verify that $C_f(z) = \pm(a+bi) = \pm z$. When f is balanced, $C_f(z) = \pm(a - bi) = \pm z^*$. Multiplying by $z/2$ so as to project our output back on to the computational basis, we find, for the elementary case of $z = 1 + i$, that

$$\begin{aligned} f \text{ constant}: &\quad \tfrac{1}{2}z \cdot \pm z = \pm i \\ f \text{ balanced}: &\quad \tfrac{1}{2}z \cdot \pm z^* = \pm 1. \end{aligned}$$

Thus for any z, if the result of applying C_f is imaginary, then f is constant, else if the result is real, then f is balanced (indeed, by examining the sign we will even be able to tell *which* of the two balanced or two constant functions f is). This algorithm is just as efficient as its quantum counterpart.

It can similarly be shown (cf. Abbott, 2012) that no entanglement is present in (3.3) when $n = 2$, and that for this case also it is possible to solve the problem efficiently using classical means. When $n \geq 3$, however, (3.2) is an entangling evolution and (3.3) is an entangled state. Unsurprisingly, it is no longer possible to define an operator C_f analogous to U_f that takes product states to product states, and it is no longer possible to produce an equally efficient classical counterpart to the Deutsch-Jozsa algorithm (cf. Abbott, 2012).

Indeed, for the general case, Abbott has shown that a quantum algorithm can always be efficiently de-quantised whenever the algorithm does not entangle the input states. Far from calling into question the role of entanglement in quantum computational speedup, the fact that the Deutsch-Jozsa algorithm does not require entanglement to succeed for certain special cases actually provides (since in these cases it can be de-quantised) evidence for both the NEST and the NEXT.

---

[18]Regarding the physical realisation of such a computer, note that complex numbers can be used, for instance, to describe the impedances of electrical circuits and that we can apply the superposition theorem to their analysis.

[19]Note that, since $f(0) = f(0)$, $(-1)^{f(0)\oplus f(0)\oplus f(1)} = (-1)^{f(1)}$.

4 Challenges to the necessity of entanglement for explanation thesis

In their own analysis of de-quantisation, Jozsa & Linden (2003) similarly find that, for pure quantum states, "the presence of multi-partite entanglement, with a number of parties that increases unboundedly with input size, is necessary if the quantum algorithm is to offer an exponential speed-up over classical computation."[20] In the same article, however, Jozsa & Linden speculate as to whether it may be possible to achieve exponential speedup, without entanglement, using *mixed* states. In fact, as we will now see, it is possible to achieve a modest (i.e., sub-exponential) speedup using unentangled mixed states. As I will argue, however, entanglement nevertheless plays an important role in the computational ability of these states, despite their being unentangled in the technical sense of §2.2. Thus, while such counter-examples demonstrate the falsity of the NEST, they do not demonstrate the falsity of the NEXT.

4.1 The mixed-state Deutsch-Jozsa algorithm

We will call a 'pseudo-pure-state' of n qubits any mixed state that can be written in the form:

$$\rho^{\{n\}}_{\text{PPS}} \equiv \varepsilon|\psi\rangle\langle\psi| + (1-\varepsilon)\mathscr{I},$$

where $|\psi\rangle$ is a pure state on n qubits, and $\mathscr{I}$ is defined as the totally mixed state $(1/2^n)\mathrm{I}_{2^n}$. It can be shown that such a state is separable (cf. §2.2) and remains so under unitary evolution just so long as

$$\varepsilon < \frac{1}{1+2^{2n-1}}.$$

Now consider the Deutsch-Jozsa algorithm once again (cf. §3.1). This time, however, let us replace the initial pure state $|0^n\rangle|1\rangle$ with the pseudo-pure state:

$$\rho = \varepsilon|0^n\rangle|1\rangle\langle 0^n|\langle 1| + (1-\varepsilon)\mathscr{I}. \tag{4.1}$$

The algorithm will continue as before, except that this time our probability of success will not be unity.

To illustrate: assume that the system represented by ρ has been prepared in the way most naturally suggested by (4.1); i.e., that with probability ε, it is prepared as the pure state $|0^n\rangle|1\rangle$, and with probability $1-\varepsilon$, it is prepared as the completely mixed state $\mathscr{I}$. Now imagine that we write some of the valid Boolean functions $f : \{0,1\}^n \rightarrow \{0,1\}$ onto balls which we then place into an urn, and assume that these consist of an equal number of constant and balanced functions. We select a ball from the urn and then test the algorithm with this function to see if the algorithm successfully determines f's type.

Consider the case when f is a constant function. In this case, we will say the algorithm succeeds whenever it yields the bit string $z = 0$. We know, from §3.1, that the algorithm

[20] For some earlier results relating to specific classes of algorithms, see Linden & Popescu (2001); Braunstein & Pati (2002). For a review, see Pati & Braunstein (2009).

will certainly succeed (i.e., with probability 1) when the system is actually in the pure state $|0^n\rangle|1\rangle$ initially. Given our particular state preparation procedure, the system is in this state with probability ε. The rest of the time (i.e., with probability $1-\varepsilon$), the system is in the completely mixed state $\mathscr{I}$. In this latter case, since there are 2^n possible values that can be obtained for z, the probability of successfully obtaining $z=0$ will be $1/2^n$. Thus the overall probability of success associated with the system when f is constant is:

$$P(z=0|f \text{ is constant}) = \varepsilon + (1-\varepsilon)/2^n. \tag{4.2}$$

The probability of failure is:

$$P(z \neq 0|f \text{ is constant}) = \frac{2^n-1}{2^n} \cdot (1-\varepsilon). \tag{4.3}$$

In the case where f is balanced, a result of $z \neq 0$ represents success, and the respective probabilities of success and failure are:

$$P(z \neq 0|f \text{ is balanced}) = \varepsilon + \frac{2^n-1}{2^n} \cdot (1-\varepsilon), \tag{4.4}$$

$$P(z=0|f \text{ is balanced}) = (1-\varepsilon)/2^n. \tag{4.5}$$

Note that as I mentioned in §2.2, mixed states can in general be prepared in a variety of ways. What I have above called the 'most natural' state preparation procedure associated with (4.1), in particular, is only one of many possible state preparations that will yield an identical density matrix ρ. For ease of exposition, and in order to see clearly why Eqs. (4.2-4.5) hold, it was easiest to assume, as I did above, that the system has been prepared in the way most naturally suggested by (4.1). But note that there is no loss of generality here; the identities (4.2-4.5) do not depend on the fact that we have used this particular preparation procedure.

In any case, consider the alternative to the Deutsch-Jozsa algorithm of performing *classical* function calls on f with the object of determining f's type. The reader should convince herself that a single such call, regardless of the result, will not change the probability of correctly guessing the type of the function f. Thus the amount of information about f's type that is gained from a single classical function call is zero.[21] On the other hand, as we should expect given (4.2-4.5), for the mixed-state version of the Deutsch-Jozsa algorithm, it can be shown that the information gained from a single invocation of the algorithm is greater than zero for all positive ε, and that this is the case even when $\varepsilon < \frac{1}{1+2^{2n-1}}$; i.e., the threshold below which ρ no longer qualifies as an entangled state. Indeed, this is the case even when ε is arbitrarily small (cf. Biham et al., 2004), although the information gain in this case is likewise vanishingly small.

4.2 Explaining speedup in the mixed-state Deutsch-Jozsa algorithm

The first question that needs to be answered here is whether the sub-exponential gain in efficiency that is realised by the mixed-state Deutsch-Jozsa algorithm should qualify as quan-

[21] This information gain is referred to as the *mutual information* between two variables (in this case, between the type of the function and the result of a function call). For more on the mutual information and other information-theoretic concepts, see Nielsen & Chuang (2000).

tum speedup at all. On the one hand, from the point of view of computational complexity theory (cf. Papadimitriou, 1994; Aaronson, 2012), the solution to the Deutsch-Jozsa problem provided by this algorithm is no more efficient than a classical solution: from a complexity-theoretic point of view, a solution S_1 to a problem P is deemed to be just as efficient as a solution S_2 so long as S_1 requires at most a polynomial increase in the (time or space) resources required to solve P as compared with S_2. From this point of view, only an *exponential* reduction in time or space resources can qualify as a true increase in efficiency. Clearly, the mixed-state Deutsch-Jozsa algorithm does not yield a speedup over classical solutions, in this sense, when ε is small. In fact it can be shown (Vedral, 2010, 1148) that exponential speedup, and hence a true increase in efficiency from a complexity-theoretic point of view, is achievable *only* when ε is large enough for the state to qualify as an entangled state.

On the other hand, there is a very real difference, in terms of the amount of information gained, between one invocation of the black box (4.1) and a single classical function call—which is all the more striking since the amount of information one can gain from a single classical function call is actually zero. Further, one should not lose sight of the fact that the complexity-theoretic characterisation of efficient algorithms is artificial and, in a certain sense, arbitrary. For instance, on the complexity-theoretic characterisation of computational efficiency, a problem, which for input size n, requires $\approx n^{1000}$ steps to solve is polynomial in terms of time resources in n and thus tractable, while a problem that requires $\approx 2^{n/1000}$ steps to solve is exponential in terms of time resources in n and therefore considered to be intractable. In this case, however, the 'intractable' problem will typically require much less time to compute than the 'tractable' problem, for all but very large n.[22] Such extraordinary examples aside, for most practical purposes the complexity-theoretic characterisation of efficiency is a good one. Nevertheless it is important to keep in mind that this is a practical definition of efficiency which does not reflect any deep mathematical truth or make any deep ontological claim about what is and is not efficient in the common or pre-theoretic sense of that term.

But let us come back now from this slight digression to our main discussion, and let us consider the question of whether entanglement plays a role in the speedup exhibited by this mixed state. The strongest argument in favour of a negative answer to this question is, I believe, the following. Recall that what I have called the 'most natural' state preparation procedure associated with (4.1) is only one of many possible ways to prepare the system represented by ρ. It is possible to prepare the system in an alternate way if we so desire. Likewise, when ε is sufficiently small, it is possible to prepare the final state of the computer, ρ_{fin}, as a mixture of product states. This, in fact, is the significance of asserting that ρ_{fin} is unentangled. Thus while the state preparation most naturally suggested by (4.1) may well function as a conceptual tool for *finding* mixed quantum states that display a computational advantage (i.e., by enabling a facile derivation of the identities (4.2-4.5)), *once found*, it seems as though we may do away with this way of thinking of the system entirely. Hence there seems to be no need to invoke entanglement in order to explain the speedup obtainable with this state.

I believe this line of reasoning to be misleading, however, for it emphasises the abstract

[22] For example, for $n = 1,000,000$, the easy problem requires $(10^6)^{1000} = 10^{6000}$ steps to complete while the hard problem requires 2^{1000} steps.

density operator representation of the computational state at the cost of obscuring the nature of the computational process that is actually occurring in the computer. To the point: the density operator corresponding to a quantum system should not be understood as a representation of the actual physical state of the system. Rather, the density operator representation of a quantum system should be understood as a representation of our knowledge of the space of physical states that the system can possibly be in, and of our ignorance as to which of these physical states the system is actually in.

From the point of view of quantum mechanics, it is *pure* states of quantum systems which should be seen as representations of the 'actual' physical states of such systems, for pure states represent the most specific description of a system that is possible from within the theory. I have enclosed the word *actual* within inverted commas in the preceding sentence in order to emphasise the weakness of the claim I am making. This claim is not intended to rule out that there may be a deeper physical theory underlying quantum mechanics, within which quantum mechanical pure states can be seen as merely derivative representations. Nor is it intended to rule out that quantum mechanics only incompletely (as a matter of principle) specifies the nature of the physical world. I am only making what should be the uncontroversial claim that relative to quantum mechanics itself, pure states should be interpreted as those which are most fundamental, in the sense that they represent a maximally specific description, within the theory, of the systems in question—i.e., they represent the best *grasp* available, from within that theory, of the real physical situation.

Physics is the science of what is real, in the very minimal sense that physical concepts *purport* to *give us some idea* of what the world is like. And if pure states represent the best possible, i.e., the most specific, representation of the physical situation from the point of view of a theory, then with right should they be treated as the more fundamental concepts of the theory. Mixed states, on the other hand, should be seen as derivative in the sense that they are abstract characterisations of our knowledge of the space *of pure states* a system may be possibly in,[23] and of our ignorance of precisely which state within this space the system is actually in.

If the reader accepts this difference in fundamental status that I have accorded to pure and mixed quantum states,[24] then she should agree that if it is an explanation of the physical process actually occurring in the computer that we desire, then it will not do to limit ourselves to analysing the characteristics of the computer's 'black box' mixed state; rather,

[23]If one prefers, one can think of a mixed state as a *statistical* state, representing the mean values of a hypothetical ensemble of systems. The difference is inessential to this discussion.

[24]My claim is intended to be weak enough to be compatible with interpretations of the quantum state such as Spekkens's, in which quantum states are analogous to the state descriptions of his toy theory (cf. Spekkens 2007), in that they represent *maximal*, though in principle incomplete, knowledge *of* the system in question. It is also intended to be compatible with Fuchs's statement that "... the quantum state represents a collection of subjective degrees of belief about *something* to do with that system ..." (Fuchs, 2003, 989-990). Nevertheless, the compatibility of my claim with Fuchs's and Spekkens's views may be doubted by some. This is not the place to attempt to give a reading of either Fuchs's or Spekkens's opinions on the interpretation of the quantum state description, however. While I may be incorrect as regards the compatibility of my claim with their views, I hope that most readers will, regardless, appreciate the benign nature of and be agreeable to the claim that I am making here. In any case I will be assuming it in the remainder of this paper. (For a more in-depth treatment of Fuchs's and Spekkens's interpretation of the quantum state description, see: Tait 2012.)

we should attempt to give a more detailed 'white box' characterisation of the operation of the computer in terms of its underlying pure states. Recall the fact—which we noted in our earlier discussion of de-quantisation—that the unitary evolution (3.2) is, in general, an *entangling evolution*; i.e., it will take pure product states, such as, for instance, $|0^n\rangle|1\rangle$, to entangled states. Now imagine that the computer is initially prepared in the most natural way suggested by the pseudo-pure state representation (4.1). Call this 'most natural' state preparation: s_{ini}. Imagine further that the computer evolves in accordance with the entangling unitary transformation U_f. This will yield the transformation

$$|0^n\rangle|1\rangle \xrightarrow{U_f} |\phi\rangle$$

with probability ε, and the transformation

$$\mathscr{I} \xrightarrow{U_f} \mathscr{I}$$

with probability $1-\varepsilon$, where $|\phi\rangle$ is an entangled state. Thus at the end of the computation, the system will be in the state $|\phi\rangle$ with probability ε and in the state $\mathscr{I}$ with probability $1-\varepsilon$. Call this combination of possible states for the system s_{fin}. Now at the end of the computation, the state of the computer will be expressible by means of the density operator

$$\rho_{fin} = \varepsilon|\phi\rangle\langle\phi| + (1-\varepsilon)\mathscr{I}.$$

The most natural way that suggests itself for preparing the system represented by ρ_{fin} is s_{fin}. However, one may instead imagine a state preparation procedure s'_{fin} involving only product states that would result in an equivalent density operator representation. Because of this, it is concluded by some that entanglement plays no role in the computational advantage exhibited by the computer in this case.

The significance of the fact that U_f is an entangling evolution, however, is that s_{ini}, evolved in accordance with U_f, will *not* result in the combination of states s'_{fin}—rather, it will result in the combination of states s_{fin}. Since both state preparations, s_{fin} and s'_{fin}, yield the same density matrix representation, they are, from this point of view, equivalent, but one *cannot* directly obtain s'_{fin} from an application of U_f to s_{ini}.[25]

What of the fact, however, that ε in the state preparation s_{fin} may be *vanishingly small* in principle and yet *still* lead to a computational advantage—does not this tell against attributing the speedup exhibited by the computer to entanglement? I do not believe it does. One must not lose sight of the fact that "vanishingly small" $\neq 0$. If ε *were* actually equal to zero, it is evident that there would, in fact, be no performance advantage.

It is interesting, nevertheless, to consider the question of what can happen in the quantum computer when $\varepsilon = 0$; i.e., when the state of the computer initially just is the totally mixed

[25] I am indebted to Wayne Myrvold for suggesting this line of thought, and for helping to clear up the conceptual confusions regarding this issue that have plagued me to date. I am also indebted to the discussion in Jozsa & Linden (2003, §5). I should note, also, that Long et al. (2002) make a similar point to the one made here; but in making it they unnecessarily rely on interpreting the density matrix of a system as representing the average values of a physical ensemble (i.e. of an actual collection of physical systems). The objection is equally forceful, however, whether one thinks of the mixed state as representing a physical or a statistical ensemble, and whether one thinks of the probabilities as ignorance probabilities or as representing relative frequencies.

state $\mathscr{I}$. Note that this does not signify that it is impossible for the computer to actually have been prepared in the pure state $|0^n\rangle|1\rangle$ initially. Rather, it represents the circumstance where we are *completely ignorant* of the initial state preparation of the quantum computer; for instance, if the computer has been prepared as an equally weighted mixture of the basis states:

$$\rho_{ini} = \mathscr{I} = \frac{1}{2^n}\sum_{x=0}^{2^n-1}|x\rangle\langle x|. \tag{4.6}$$

Suppose then, that the quantum computer, represented by the density operator $\rho_{ini} = \mathscr{I}$, actually is in $|0^n\rangle|1\rangle$ at the start of the computation. Is a computational process occurring which would enable quantum speedup? From one point of view, the answer is yes, for the entangling unitary evolution U_f evolves the computer to an entangled state which is then capable of being utilised in principle in order to solve the problem under consideration with fewer computational resources than a classical computer. In fact, it is not even necessary for the computer to actually be in the state $|0^n\rangle|1\rangle$ initially to enable a performance advantage. As long as we know, or at least are not completely ignorant of, the actual initial pure state of the computer, any of the basis states can, with suitable manipulation, be used to obtain a performance advantage.

From another point of view, however, the answer is no, for because we are completely ignorant as to the actual initial state of the computer, we will be completely ignorant as to which operation to perform in order to take advantage of this resource. This sounds paradoxical, but I think it rather illustrates an important distinction: between what is actually occurring in a physical system, on the one hand, and the use which can be made of it by *us*, who are attempting to achieve some particular end. In the example we are considering here there assuredly is a process occurring in the computer that is of the right sort to enable a quantum speedup, but because we are completely ignorant of the computer's initial state—i.e., because there is too much 'noise' in the computer—we are unable to take advantage of it to achieve the end of solving the Deutsch-Jozsa problem using fewer computational resources than a classical computer.

4.3 DQC1: The power of one qubit

In the last subsection we saw that it is possible to achieve a sub-exponential speedup for the Deutsch-Jozsa problem with an unentangled mixed-state. We concluded that while this does disprove the NEST, it does not constitute a counter-example to the NEXT, since the computational algorithm in question is successful only when the evolution of the state of the computer is an entangling evolution; therefore the underlying final state of the computer will always contain some entanglement despite the fact that the density operator representation of the final state will be unentangled.

We now consider another purported counter-example to the NEXT. This is the *deterministic quantum computation with one qubit* (DQC1) model of quantum computation, which utilises a mixed quantum state to compute the trace of a given unitary operator and displays an *exponential* speedup over known classical solutions. As we will see, the claim sometimes made to the effect that the DQC1 achieves this speedup without the use of entanglement is

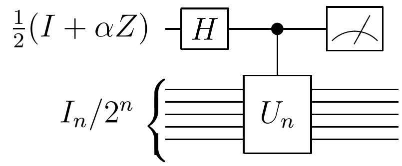

Figure 1: The DQC1 algorithm for computing the trace of a unitary operator.

unsubstantiated. The NEXT, however, is not the claim that any state that displays quantum computational speedup must be entangled. That is the NEST. The NEXT is, rather, the different claim that entanglement must play a role in any physical *explanation* of quantum speedup. We saw in the last section how it is possible for the NEST to be false[26] and the NEXT to be true. In this section I will address the objection that the NEXT is false even if it is the case that the state of the quantum computer is always entangled. Those defending such a view claim that another measure of quantum correlations, *quantum discord*, is far better suited for the explanatory role. In what follows I will argue that this conclusion is misguided. Quantum discord is indeed an enormously useful theoretical quantity for characterising mixed-state quantum computation—perhaps even more useful than entanglement. Nevertheless, more than just pragmatic considerations must be appealed to if one is to make the case that a particular feature of quantum systems explains quantum speedup. Thus I will argue that when one looks deeper, and considers the quantum state from the *multi-partite* point of view, one finds that entanglement is involved in the production, and even in the very definition, of quantum discord; indeed, there are some preliminary indications that quantum discord is, in fact, but a manifestation of and not conceptually distinct from entanglement.

In the DQC1, or as it is sometimes called: 'the power of one qubit', model of quantum computation (cf. Knill & Laflamme, 1998),[27] a collection of n 'unpolarised' qubits in the completely mixed state $I_n/2^n$ is coupled to a single 'polarised' control qubit, initialised to $1/2(I + \alpha Z)$. When the polarisation, α, is equal to 1, the control qubit is in the pure state $|0\rangle\langle 0| = 1/2(I + Z)$, otherwise it is in a mixed state. The problem is to compute the trace of an arbitrary n-qubit unitary operator, $\mathrm{Tr}(U_n)$. To accomplish this, we begin by applying a Hadamard gate to the control qubit,[28] which is then forwarded as part of the input to a controlled unitary gate that acts on the n unpolarised qubits (see Figure 1). This results in the following state for all of the $n + 1$ qubits:

$$\begin{aligned} \rho_{n+1} &= \frac{1}{2^{n+1}} \big(|0\rangle\langle 0| \otimes I_n + |1\rangle\langle 1| \otimes I_n + \alpha |0\rangle\langle 1| \otimes U_n^\dagger + \alpha |1\rangle\langle 0| \otimes U_n \big) \\ &= \frac{1}{2^{n+1}} \begin{pmatrix} I_n & \alpha U_n^\dagger \\ \alpha U_n & I_n \end{pmatrix}. \end{aligned} \tag{4.7}$$

[26] I mean false in the technical sense explained in §2.2.

[27] In this exposition of the DQC1, I am closely following (Datta et al., 2005).

[28] This will yield, for instance, when the control qubit is pure, $|0\rangle\langle 0| \xrightarrow{H} \frac{1}{2}\big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\big)$.

The reduced state of the control qubit is

$$\rho_c = \begin{pmatrix} 1 & \alpha \mathrm{Tr}(U_n)^\dagger \\ \alpha \mathrm{Tr}(U_n) & 1 \end{pmatrix},$$

thus the trace of U_n can be retrieved by applying the X and Y Pauli operators to ρ_c. In particular, the expectation values of the X and Y operators will yield the real and imaginary parts of the trace, $\langle X \rangle = \mathrm{Re}[\mathrm{Tr}(U_n)]/2^n$ and $\langle Y \rangle = -\mathrm{Im}[\mathrm{Tr}(U_n)]/2^n$, respectively; so in order to determine, for instance, the real part, we run the circuit repeatedly, measuring X on the control qubit at the end of each run, while assuming that the results are part of a distribution whose mean is the real part of the trace.

Classically, the problem of evaluating the trace of a unitary matrix is believed to be hard, however for the quantum algorithm it can be shown that the number of runs required does not scale exponentially with n, yielding an exponential advantage for the DQC1 quantum computer. When $\alpha < 1$, the expectation values, $\langle X \rangle$ and $\langle Y \rangle$, are reduced by a factor of α and it becomes correspondingly more difficult to estimate the trace. However as long as the control qubit has non-zero polarisation, the model still provides an efficient method for estimating the trace (and thus an exponential speedup over any known classical solution) in spite of this additional overhead.

We might ask whether, in a way analogous to the mixed-state Deutsch-Jozsa algorithm, we can make α small enough so that the overall state of the DQC1 is demonstrably separable. The answer seems to be no. On the one hand, for any system of $n+1$ qubits there is a ball of radius r (measured by the Hilbert-Schmidt norm and centred at the completely mixed state), within which all states are separable (Braunstein et al., 1999; Gurvits & Barnum, 2003). On the other hand, the state of the DQC1 is at all times at a fixed distance $\alpha 2^{-(n+1)/2}$ from the completely mixed state. Unfortunately the radius of the separable ball decreases exponentially faster than $2^{-(n+1)/2}$ (Datta et al., 2005, 2).

Thus, as (Datta et al., 2005, 2) assert, there appears to be good reason to suspect that the state (4.7) is an entangled state, at least for some U_n; but it is not obvious where this entanglement *is*. On the one hand, there is no bipartite entanglement among the n unpolarised qubits. On the other hand the most natural bipartite split of the system, with the control qubit playing the role of the first subsystem and the remaining qubits playing the role of the second, reveals no entanglement between the two subsystems, regardless of the choice of U_n. When $\alpha > 1/2$, entanglement can be found when we examine other bipartite divisions amongst the $n+1$ qubits (see Figure 2), however, besides being exceedingly difficult to detect, the amount of entanglement in the state (as measured by the multiplicative negativity; cf. Plenio & Virmani 2007) becomes vanishingly small as n gets large. Commenting on this circumstance, Datta et al. (2005, 13) write "This hints that the key to computational speedup might be the global character of the entanglement, rather than the amount of the entanglement. ... what happier motto can we find for this state of affairs than *Multam ex Parvo*, or A Lot out of A Little."

Others have expressed a different viewpoint on the matter. In fact, both the DQC1 and the mixed-state version of the Deutsch-Jozsa algorithm have led many (see for instance, Vedral 2010) to seriously question whether entanglement plays a necessary role in the explanation of quantum speedup. The result has been a shift in investigative focus from

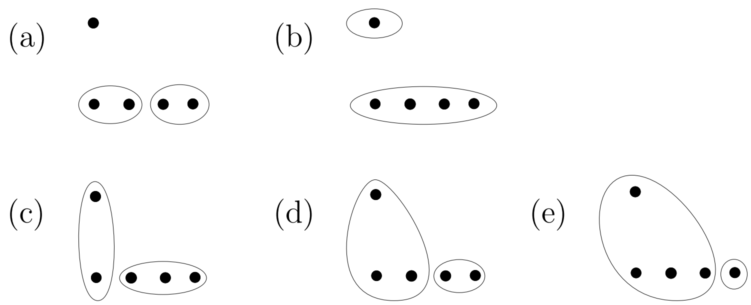

Figure 2: Some of the bipartite splits possible in the DQC1 for $n = 4$. No entanglement can ever occur amongst the n unpolarised qubits (a) or between the polarised qubit and the rest (b); however, bipartite splits such as (c), (d), and (e) can exhibit entanglement (Datta et al., 2005).

entanglement to other types of quantum correlations. One alternative in particular, *quantum discord* (which I will explain in more detail shortly), has received much attention in the literature in recent years (see, e.g., Merali, 2011).

On the one hand, the following facts all seem to run counter to the NEXT: there is no entanglement in the DQC1 circuit between the polarised and unpolarised qubits—the most natural bipartite split that suggests itself—during a computation; tests to detect entanglement along other bipartite splits in the DQC1 when $\alpha \leq 1/2$ have thus far been unsuccessful;[29] and finally, even when α is relatively large, only a vanishingly small amount of entanglement can be found in the state of the DQC1 (4.7). On the other hand, when we consider the correlations between the polarised and unpolarised qubits from the point of view of *quantum discord*, it turns out that the discord at the end of the computation is *always* non-zero along this bipartite split for *any* $\alpha > 0$ (Datta et al., 2008). Datta et al. (2008, 4) therefore write, *and I agree*, that "for some purposes, quantum discord might be a better figure of merit for characterizing the quantum resources available to a quantum information processor." All the same, as I will argue below, it is a mistake to conclude as they and others do that the NEXT is false; i.e., that entanglement may play no role in the explanation of the quantum speedup of the DQC1 (Datta et al., 2008; Vedral, 2010; Merali, 2011); for the NEXT *is compatible* with all of these facts.

[29]The criterion used by Datta et al. (2005) to detect entanglement is the Peres-Horodecki, or Positive Partial Transpose (PPT) criterion (Peres, 1996; Horodecki et al., 1996). The partial transpose of a bipartite system, $\sum_{ijkl} p^{ij}_{kl} |i\rangle\langle j| \otimes |k\rangle\langle l|$ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ is defined (with respect to the system B) as:

$$\rho^{T_B} \equiv (I \otimes T)\rho = \sum_{ijkl} p^{ij}_{kl} |i\rangle\langle j| \otimes (|k\rangle\langle l|)^T = \sum_{ijkl} p^{ij}_{kl} |i\rangle\langle j| \otimes |l\rangle\langle k|,$$

where T is the transpose map on matrices. The PPT criterion states that, if ρ is a separable state, then the partial transpose of ρ has non-negative eigenvalues. Satisfying the PPT criterion is a necessary (but not sufficient) condition for the joint density matrix of two systems to be separable. While Datta et al. were unable to detect entanglement in the DQC1 (along any bipartite split) for the case of $\alpha \leq 1/2$, they nevertheless note that it is very likely that both entanglement and bound entanglement are present in the state. A state exhibits *bound entanglement* (cf. Hyllus et al., 2004) when, in spite of the fact that it is entangled, no pure entangled state can be obtained from it by means of LOCC operations. One important characteristic of bound entangled states is that they (at least sometimes) satisfy the PPT criterion despite the fact that they are entangled.

4.4 Quantum discord

Quantum discord (Henderson & Vedral, 2001; Ollivier & Zurek, 2002)[30] quantifies the difference between the quantum generalisations of two classically equivalent measures of mutual information,[31]

$$\mathcal{I}_c(A : B) = H(A) + H(B) - H(A, B), \tag{4.8}$$
$$\mathcal{J}_c(A : B) = H(A) - H(A|B). \tag{4.9}$$

These two expressions are not equivalent quantum mechanically, for while (4.8) has a straightforward quantum generalisation in terms of the von Neumann entropy S:

$$\mathcal{I}_q(A : B) = S(A) + S(B) - S(A, B), \tag{4.10}$$

things are more complicated for the quantum generalisation of (4.9). The quantum counterpart, $S(A|B)$, to the conditional entropy requires a specification of the information content of A given a determination of the state of B. Determining the state of B requires a measurement, however, which requires the choice of an observable. But in quantum mechanics observables are, in general, non-commuting. Thus the conditional entropy will be different depending on the observable we choose to measure on B. If, for simplicity, we consider only perfect measurements, represented by a set of one dimensional projection operators, $\{\Pi_j^B\}$, this yields, for the quantum version of (4.9), the expression:

$$\mathcal{J}_q(A : B) = S(A) - S(A|\{\Pi_j^B\}). \tag{4.11}$$

We now define discord as the minimum value (taken over $\{\Pi_j^B\}$) of the difference between (4.10) and (4.11):

$$\mathcal{D}(A, B) \equiv \min_{\{\Pi_j^B\}} \mathcal{I}_q(A : B) - \mathcal{J}_q(A : B). \tag{4.12}$$

Discord is, in general, non-zero for mixed states, while for pure states it effectively becomes a measure of entanglement (Datta et al., 2008, 3); i.e., for pure states it is equivalent to the entropy of entanglement (cf. Plenio & Virmani, 2007).

Interestingly, there are some mixed states which, though *separable*, exhibit non-zero quantum discord. For instance, consider the following bipartite state:

$$\rho_{\text{disc}} = \frac{1}{2}(|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B) + \frac{1}{2}(|1\rangle\langle 1|_A \otimes |+\rangle\langle +|_B). \tag{4.13}$$

This state is obviously separable. Since $|0\rangle$ and $|+\rangle$ are non-orthogonal states, however, $\mathcal{J}_q(A : B)$ will yield a different value depending on the experiment performed on system B; and thus this state will yield a non-zero quantum discord. Note that this is impossible for a

[30]Quantum discord was introduced independently by both Henderson & Vedral and by Ollivier & Zurek, with slight differences in their respective formulations (Henderson & Vedral consider not just projective measurements but positive operator valued measures more generally). These and other alternative formulations of quantum discord do not differ in essentials. The definition of discord I introduce here is Ollivier & Zurek's.

[31]See Nielsen & Chuang (2000) for an overview of the basic concepts of classical and quantum information theory.

classical state: classically, it is *always* possible to prepare a state as a mixture of *orthogonal* product states.

In most of the literature on this topic, one is introduced to quantum discord as a quantifier of the non-classical *correlations* present in a state which are not necessarily identifiable with entanglement. Such an interpretation of the significance of this quantity is supported by the fact that, in the classical scenario at least, the mutual information contained in a system of two random variables is held to be representative of the extent of the correlations between them. Since the quantum generalisations of the two classically equivalent measures of mutual information $\mathcal{I}_c(A:B)$ and $\mathcal{J}_c(A:B)$ are not equivalent, then, this is taken to represent the presence of non-classical correlations over and above the classical ones, some, but not all of which may be accounted for by entanglement, and some by 'quantum discord'.

Interpreting discord as a type of non-classical correlation is nevertheless puzzling. Consider, for instance, a classically correlated state represented by the following probability distribution:

$$\frac{1}{2}([+]_l, [+]_r) + \frac{1}{2}[-]_l[-]_r. \tag{4.14}$$

Here, let $[\cdot]_l$ represent the circumstance that Linda (in Liverpool) finds a letter in her mailbox today containing a piece of paper on which is inscribed the specified symbol ($+$ or $-$), and let $[\cdot]_r$ represent the occurrence of a similar circumstance for Robert (in Ravenna). According to the probability distribution, it is equally likely that they both receive a letter today inscribed with $+$ as it is that they both receive one inscribed with $-$, but it cannot happen that they each today receive letters with non-matching symbols. These correlations are easily explainable classically, of course. It so happens that yesterday I flipped a fair coin. I observed the result of the toss and accordingly jotted down either $+$ or $-$ on a piece of paper, photocopied it, and sent one copy each to Robert in Ravenna and Linda in Liverpool (by overnight courier, of course).

A quantum analogue for classically correlated states such as (4.14) is a mixed state decomposable into product states:

$$\sum_{ij} p_{ij}|i\rangle\langle i| \otimes |j\rangle\langle j| \tag{4.15}$$

such that the $|i\rangle$ and $|j\rangle$ are mutually orthogonal sub-states of the first and second subsystem, respectively. For such a state it is easy to provide a 'hidden variables' explanation, similar to the one above, that will account for the observed probabilities of joint experiments on the two subsystems.

We can equally give such a local hidden variables account of the discordant state ρ_{disc}: tossing a fair coin, I prepare the state $|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B$ if the coin lands heads, and $|1\rangle\langle 1|_A \otimes |+\rangle\langle +|_B$ if it lands tails. Let $Pr(X, Y|a, b, \lambda)$ refer to the probability that Alice's a-experiment and Bob's b-experiment determine their qubits to be in states X and Y, respectively, given that the result of the coin toss is λ. Then (omitting bras and kets for readability):

$$\begin{aligned}
Pr(0, 0|\hat{z}, \hat{z}, H) &= Pr(0, \cdot|\hat{z}, \cdot, H) \times Pr(\cdot, 0|\cdot, \hat{z}, H) = 1, \\
Pr(1, 1|\hat{z}, \hat{z}, T) &= Pr(1, \cdot|\hat{z}, \cdot, T) \times Pr(\cdot, 1|\cdot, \hat{z}, T) = 1/2, \\
Pr(0, +|\hat{z}, \hat{x}, H) &= Pr(0, \cdot|\hat{z}, \cdot, H) \times Pr(\cdot, +|\cdot, \hat{x}, H) = 1/2, \\
Pr(1, +|\hat{z}, \hat{x}, T) &= Pr(1, \cdot|\hat{z}, \cdot, T) \times Pr(\cdot, +|\cdot, \hat{x}, T) = 1,
\end{aligned}$$

and so on. More generally, $Pr(X, Y|a, b, \lambda) = Pr(X, \cdot|a, \cdot, \lambda) \times Pr(\cdot, Y|\cdot, b, \lambda)$. Thus once we specify the value of λ there are no remaining correlations in the system and the probabilities for joint experiments are *factorisable*. This should be unsurprising. Given a specification of λ, the state of the system is in a *product state*, after all.

Contrast this with an entangled quantum system such as, for instance, the one represented by the pure state

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Bell's theorem (Bell, 2004 [1964]) demonstrates that the correlations between subsystems present in such a state cannot be reproduced by any local hidden variables theory in the manner described above. These correlations are non-classical.

There is certainly *something* non-classical about a state such as ρ_{disc}; viz., a quantum state such as ρ_{disc}, though separable, cannot be prepared as a mixture of orthogonal product states. Yet it is always possible to so prepare classical states. As a result, the information one can gain about Alice's system through an experiment in the $\{+, -\}$ basis on Bob's system will be different from the information one can gain about Alice's system through an experiment in the computational basis on Bob's system. On the one hand, in the absence of a specification of a hidden parameter such as λ, given an experiment on B in the computational basis which determines B to be in state $|0\rangle$, it is still unclear, because of the way in which system B was prepared, whether the joint system is in the state $|0\rangle \otimes |0\rangle$ or in the state $|1\rangle \otimes |+\rangle$. Given an experiment on B in the $\{+, -\}$ basis which yields $|+\rangle$, on the other hand, it is perfectly clear which product state the joint system is in. But these facts by themselves are certainly not indicative of the presence of non-classical *correlations* between the two subsystems.

There is one indirect sense, however, in which ρ_{disc} can be said to contain non-classical correlations. Recall from §2.4 that any mixture can be considered as the result of taking the partial trace of a pure entangled state on a larger Hilbert space. Given that, as I argued in §4.2, the pure state representation of a quantum system should be taken as fundamental, we can consider the bipartite state ρ_{disc} as in reality but a partial representation of a tripartite entangled quantum system, where the third party is an external environment with enough degrees of freedom to purify the overall system. And since entangled systems do not admit of a description in terms of local hidden variables, it follows that the system partially represented by ρ_{disc} can legitimately be said to contain non-classical correlations.

Even so it is unclear how these non-classical correlations *per se* can have anything to do with the quantum discord exhibited by ρ_{disc}, for it is also the case that a classically correlated mixture of *orthogonal* product states, i.e. one of the form (4.15), can be purified in just the same way as a discordant one and hence also the case that it can be given a multi-partite representation in which entanglement is present.

As we will now see, however, there is in fact a tight relationship between the *amount* of discord associated with a bipartite mixed state and the *amount* of entanglement associated with a tripartite representation of that state. And, interestingly from our point of view, what emerges from this is a correspondingly tight relationship between the quantum speedup exhibited by the DQC1 and the amount of entanglement associated with its purified tripartite representation, and thus a confirmation, not a refutation, of the NEXT.

4.5 Explaining speedup in the DQC1

Quantum discord was introduced independently by Henderson & Vedral and by Ollivier & Zurek in 2001 and 2002, respectively; however, it was only recently given an operational interpretation, independently by Madhok & Datta (2011) and by Cavalcanti et al. (2011).[32] On both characterisations, quantum discord is operationally defined in terms of the entanglement consumed in an extended version of the quantum state merging protocol (cf. Horodecki et al., 2005).

In the quantum state merging protocol, three parties: Alice, Bob, and Cassandra, share a state $|\psi_{ABC}\rangle$. Quantum state merging characterises the process,

$$|\psi_{ABC}\rangle \rightarrow |\psi_{B'BC}\rangle,$$

by which Alice effectively transfers her part of the system to Bob while maintaining its coherence with Cassandra's part. It turns out that in order to effect this protocol a certain amount of entanglement must be consumed (quantified on the basis of the quantum conditional entropy, $S(A|B)$; cf. Nielsen & Chuang 2000.). When we add to this the amount of entanglement needed (as quantified by the entanglement of formation; cf. Plenio & Virmani 2007) to prepare the state $|\psi_{ABC}\rangle$ to begin with, the result is a quantity identical to the quantum discord between the subsystems belonging to Alice and Cassandra at the time the state is prepared.

The foregoing operational interpretation of discord has an affinity with an illuminating analysis of the DQC1 circuit due to Fanchini et al. (2011). Fanchini et al. show that a relationship between quantum discord and entanglement emerges when we consider the DQC1 circuit, not as a bipartite system composed of polarised and unpolarised qubits respectively, but as a tripartite system in which the environment plays the role of the third subsystem. Fanchini et al. note that an alternate way of characterising the completely mixed state of the unpolarised qubits, $I_n/2^n$, is to view it as part of a bipartite entangled state, with the second party an external environment having enough degrees of freedom to purify the overall system. This yields a tripartite representation for the DQC1 circuit as a whole (see Figure 3).

Fanchini et al. show that, for an arbitrary tripartite pure state, there is a conservation relation between entanglement of formation and quantum discord. In particular, the sum of the bipartite entanglement that is shared between a particular subsystem and the other subsystems of the system cannot be increased without increasing the sum of the quantum discord between this subsystem and the other subsystems as well (and vice versa). In the DQC1, after the application of the controlled not gate (see Figure 1), there is an increase in the quantum discord between B and A. This therefore necessarily involves a corresponding increase in the entanglement between A and the combined system BE. All of this accords with what we would expect given the above operational interpretation of quantum discord: an increase in quantum discord requires an increase in the entanglement available for consumption in a potential quantum state merging process.

Note also that from this tripartite point of view, there is just as much entanglement

[32] I present here the definition given by Cavalcanti et al., although the conclusion I will draw is the same regardless of which definition is used.

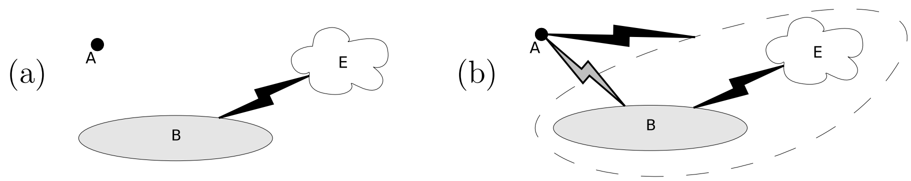

Figure 3: A (pure) tripartite representation of the elements of the DQC1 protocol before (a) and after (b) the application of the controlled not gate. Black and grey thunderbolts represent entanglement and discord, respectively. After the application of the controlled not gate, there is an increase in the discord between A and B and a corresponding increase in the entanglement between A and the combined system BE.

in the circuit as there is discord; in particular, exactly as for quantum discord, there is entanglement in the circuit whenever it displays a quantum speedup, i.e., for any $\alpha > 0$.

Fanchini et al. speculate that it is not the presence of entanglement or discord (however the latter is interpreted) per se that is necessary for the quantum speedup of the DQC1, but rather the ability of the circuit to *redistribute* entanglement and discord. This thought seems to be confirmed by a theoretical result of Brodutch & Terno (2011), who show that shared entanglement is required in order for two parties to bilocally implement[33] *any* bipartite quantum gate—even one that operates on a restricted set $\mathcal{L}$ of unentangled input states and transforms them into unentangled output states. This means, in particular, that entanglement is required in order to implement a gate that changes the discord of a quantum state.

By themselves, these considerations already amount to confirmations of the NEXT, for entanglement appears to be involved in the very definition of discord, and it appears that we require entanglement even for the production of discord in a quantum circuit. But in addition, there are indications that quantum discord need not be appealed to at all to give an account of quantum speedup (though such a characterisation will of course be less practical, as I have already mentioned), in light of one other recent theoretical result. Devi et al. (2008; 2011) have pointed out that more general measurement schemes than the positive operator valued measures (POVM) used thus far exist for characterising the correlations present in bipartite quantum systems.

POVMs are associated with completely positive maps and are well suited for describing the evolution of a system when we can view the system as uncorrelated with its external environment. When the system is initially correlated with the environment, however, the reduced dynamics of the system may, according to Devi et al., be 'not completely positive'. But as Devi et al. show, from the point of view of a measurement scheme that incorporates not completely positive maps in addition to completely positive maps, all quantum correlations reduce to entanglement.

In sum, it is, I believe, unsurprising that on the standard analysis the DQC1 circuit displays strange and anomalous correlations in the form of quantum discord, for the DQC1 is typically characterised as a *bipartite* system, and from the point of view of a measurement framework that incorporates only completely positive maps. As Fanchini et al. have shown, however, the DQC1 circuit is more properly characterised, not as an isolated system, but as a system initially correlated with an external environment. The evolution of such a

[33] Bilocal implementation means, in this context, an implementation in which Alice and Bob are limited to local operations and classical communications (cf. Plenio & Virmani, 2007).

system is best captured by a measurement framework incorporating not completely positive maps, and within such a framework, the anomalous correlations disappear and are subsumed under entanglement. From this point of view the equivalence of entanglement and discord for pure bipartite states is also unsurprising, for it is precisely pure states for which the correlation with the environment can be ignored and for which a framework incorporating only completely positive maps is appropriate.

The use of not completely positive maps to characterise the evolution of open quantum systems is not wholly without its detractors. The question of whether such not completely positive maps are 'unphysical' is an interesting and important one, though I will not address it here.[34] But regardless of the answer to this question, it should be clear, even without the appeal to this more general framework, that entanglement has *not* been shown to be unnecessary for quantum computational speedup. Far from being a counter-example to the NEXT, the DQC1 model of quantum computation rather serves to illuminate the crucial role that entanglement plays in the quantum speedup displayed by this computer.

5 Conclusion

Quantum entanglement is considered by many to be a necessary resource that is used to advantage by a quantum computer in order to achieve a speedup over classical computation. Given Jozsa & Linden's and Abbott's general results for pure states, and given that, as I argued in §4.2, a pure state should be considered as the most fundamental representation of a quantum system possible in quantum mechanics, the burden is upon those who deny the NEXT to either produce a counter-example or to show, in some other more principled way, why the view is false. We examined two such counter-examples in this paper. Upon closer examination we found neither of these, neither the sub-exponential speedup of the unentangled mixed-state version of the Deutsch-Jozsa algorithm, nor the exponential speedup of the DQC1 model of quantum computation, demonstrate that entanglement is unnecessary for quantum speedup; they rather make clearer than before the role that entanglement *does* play, and point the way to a fuller understanding of both entanglement and quantum computation.

References

Aaronson, S. (2012). Complexity zoo. *Qwiki*: http://qwiki.stanford.edu/index.php/Complexity_Zoo.

Abbott, A. A. (2012). The Deutsch-Jozsa problem: De-quantisation and entanglement. *Natural Computing*, *11*, 3–11.

Bell, J. S. (2004 [1964]). On the Einstein-Podolsky-Rosen paradox. In *Speakable and Unspeakable in Quantum Mechanics*, (pp. 15–21). Cambridge: Cambridge University Press.

[34] For a more detailed discussion, and qualified defence of the use of not completely positive maps, see Cuffaro & Myrvold (2012).

Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., & Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, *70*, 1895–1899.

Biham, E., Brassard, G., Kenigsberg, D., & Mor, T. (2004). Quantum computing without entanglement. *Theoretical Computer Science*, *320*, 15–33.

Braunstein, S. L., Caves, C. M., Jozsa, R., Linden, N., Popescu, S., & Schack, R. (1999). Separability of very noisy mixed states and implications for NMR quantum computing. *Physical Review Letters*, *83*, 1054–1057.

Braunstein, S. L., & Pati, A. K. (2002). Speed-up and entanglement in quantum searching. *Quantum Information & Computation*, *2*, 399–409.

Brodutch, A., & Terno, D. R. (2011). Entanglement, discord and the power of quantum computation. *Physical Review A*, *83*, 010301.

Bub, J. (2010). Quantum computation: Where does the speed-up come from? In A. Bokulich, & G. Jaeger (Eds.) *Philosophy of Quantum Information and Entanglement*, (pp. 231–246). Cambridge: Cambridge University Press.

Cavalcanti, D., Aolita, L., Boixo, S., Modi, K., Piani, M., & Winter, A. (2011). Operational interpretations of quantum discord. *Physical Review A*, *83*, 032324.

Cleve, R., Ekert, A., Macchiavello, C., & Mosca, M. (1998). Quantum algorithms revisited. *Proceedings of the Royal Society of London A*, *454*, 339–354.

Clifton, R., Bub, J., & Halvorson, H. (2003). Characterizing quantum theory in terms of information-theoretic constraints. *Foundations of Physics*, *33*, 1561–1591.

Cuffaro, M. E. (2012). Many worlds, the cluster-state quantum computer, and the problem of the preferred basis. *Studies in History and Philosophy of Modern Physics*, *43*, 35–42.

Cuffaro, M. E. (2013). *On The Physical Explanation for Quantum Computational Speedup*. Ph.D. thesis, The University of Western Ontario, London, Ontario.

Cuffaro, M. E., & Myrvold, W. C. (2012). On the debate concerning the proper characterisation of quantum dynamical evolution. In preparation (arXiv:1206.3794v1).

Datta, A., Flammia, S. T., & Caves, C. M. (2005). Entanglement and the power of one qubit. *Physical Review A*, *72*, 042316.

Datta, A., Shaji, A., & Caves, C. M. (2008). Quantum discord and the power of one qubit. *Physical Review Letters*, *100*, 050502.

Deutsch, D. (1985). Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences*, *400*, 97–117.

Deutsch, D. (1997). *The Fabric of Reality*. New York: Penguin.

Deutsch, D., & Jozsa, R. (1992). Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences*, *439*, 553–558.

Devi, A. R. U., & Rajagopal, A. K. (2008). Generalized information theoretic measure to discern the quantumness of correlations. *Physical Review Letters*, *100*, 140502.

Devi, A. R. U., Rajagopal, A. K., & Sudha (2011). Quantumness of correlations and entanglement. *International Journal of Quantum Information*, *9*, 1757–1771.

Duwell, A. (2004). *How to Teach an Old Dog New Tricks: Quantum Information, Quantum Computing, and the Philosophy of Physics*. Ph.D. thesis, University of Pittsburgh, Pittsburgh.

Duwell, A. (2007). The many-worlds interpretation and quantum computation. *Philosophy of Science*, *74*, 1007–1018.

Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, *47*, 777–780.

Ekert, A., & Jozsa, R. (1998). Quantum algorithms: Entanglement-enhanced information processing. *Philosophical Transactions of the Royal Society A*, *356*, 1769–1782.

Fanchini, F. F., Cornelio, M. F., de Oliveira, M. C., & Caldeira, A. O. (2011). Conservation law for distributed entanglement of formation and quantum discord. *Physical Review A*, *84*, 012313.

Fuchs, C. A. (2003). Quantum mechanics as quantum information, mostly. *Journal of Modern Optics*, *50*, 987–1023.

Gurvits, L., & Barnum, H. (2003). Separable balls around the maximally mixed multipartite quantum states. *Physical Review A*, *68*, 042312.

Henderson, L., & Vedral, V. (2001). Classical, quantum, and total correlations. *Journal of Physics A: Mathematical and General*, *34*, 6899–6905.

Hewitt-Horsman, C. (2009). An introduction to many worlds in quantum computation. *Foundations of Physics*, *39*, 869–902.

Horodecki, M., Horodecki, P., & Horodecki, R. (1996). Separability of mixed states: Necessary and sufficient conditions. *Physics Letters A*, *223*, 1.

Horodecki, M., Oppenheim, J., & Winter, A. (2005). Partial quantum information. *Nature*, *436*, 673–676.

Howard, D. (1985). Einstein on locality and separability. *Studies in History and Philosophy of Science*, *16*, 171–201.

Hyllus, P., Moura Alves, C., Bruß, D., & Macchiavello, C. (2004). Generation and detection of bound entanglement. *Physical Review A*, *70*, 032316.

Jozsa, R., & Linden, N. (2003). On the role of entanglement in quantum-computational speed-up. *Proceedings of the Royal Society of London. Series A. Mathematical, Physical and Engineering Sciences*, *459*, 2011–2032.

Knill, E., & Laflamme, R. (1998). Power of one bit of quantum information. *Physical Review Letters*, *109*, 275–309.

Linden, N., & Popescu, S. (2001). Good dynamics versus bad kinematics: Is entanglement needed for quantum computation? *Physical Review Letters*, *87*, 047901.

Long, G. L., Yan, H. Y., Li, Y. S., Tu, C. C., Zhu, S. J., Ruan, D., Sun, Y., Tao, J. X., & Chen, H. M. (2002). Quantum mechanical nature in liquid NMR quantum computing. *Communications in Theoretical Physics*, *38*, 305–308.

Madhok, V., & Datta, A. (2011). Interpreting quantum discord through quantum state merging. *Physical Review A*, *83*, 032323.

Masanes, L. (2006). All bipartite entangled states are useful for information processing. *Physical Review Letters*, *96*, 150501.

Merali, Z. (2011). Quantum computing: The power of discord. *Nature*, *474*, 24–26.

Mermin, N. D. (1998). Nonlocal character of quantum theory? *American Journal of Physics*, *66*, 920.

Myrvold, W. C. (2010). From physics to information theory and back. In A. Bokulich, & G. Jaeger (Eds.) *Philosophy of Quantum Information and Entanglement*, (pp. 181–207). Cambridge: Cambridge University Press.

Nielsen, M. A., & Chuang, I. L. (2000). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press.

Ollivier, H., & Zurek, W. H. (2002). Quantum discord: A measure of the quantumness of correlations. *Physical Review Letters*, *88*, 017901.

Papadimitriou, C. H. (1994). *Computational Complexity*. New York: Addison-Wesley.

Pati, A. K., & Braunstein, S. L. (2009). Role of entanglement in quantum computation. *Journal of the Indian Institute of Science*, *89*, 295–302.

Peres, A. (1996). Separability criterion for density matrices. *Physical Review Letters*, *77*, 1413–1415.

Plenio, M. B., & Virmani, S. (2007). An introduction to entanglement measures. *Quantum Information & Computation*, *7*, 1–51.

Schrödinger, E. (1935). Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, *31*, 555–563.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, *26*, 1484–1509.

Spekkens, R. W. (2007). Evidence for the epistemic view of quantum states: A toy theory. *Physical Review A*, *75*, 032110.

Stapp, H. P. (1997). Nonlocal character of quantum theory. *American Journal of Physics*, *65*, 300.

Stapp, H. P. (1999). Comment on "nonlocality, counterfactuals, and quantum mechanics". *Physical Review A*, *60*, 2595–2598.

Steane, A. M. (2003). A quantum computer only needs one universe. *Studies in History and Philosophy of Modern Physics*, *34*, 469–478.

Tait, M. (2012). *The Case for Quantum State Realism*. Ph.D. thesis, The University of Western Ontario, London, Ontario.

Unruh, W. (1999). Nonlocality, counterfactuals, and quantum mechanics. *Physical Review A*, *59*, 126–130.

Vedral, V. (2010). The elusive source of quantum speedup. *Foundations of Physics*, *40*, 1141–1154.