Reflections on the Role of Entanglement in the Explanation of Quantum Computational Speedup

Michael E. Cuffaro

The University of Western Ontario, Department of Philosophy

February 3, 2012

Abstract

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. While the fact of quantum computational speedup is almost beyond doubt, the source of quantum speedup is still a matter of debate. In this paper I argue that entanglement is a necessary component for any explanation of quantum speedup and I address some purported counter-examples that some claim show that the contrary is true. In particular, I address Cleve et al.'s solution to Deutsch's problem, Biham et al.'s mixed-state version of the Deutsch-Jozsa algorithm, and Knill & Laflamme's deterministic quantum computation with one qubit (DQC1) model of quantum computation. I argue that these examples do not demonstrate that entanglement is unnecessary for the explanation of quantum speedup, but that they rather illuminate and clarify the role that entanglement does play.

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 (similarly to most other foundational issues), 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'

[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).

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). 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 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 candidate explanations for quantum speedup, the fact that quantum mechanical systems can sometimes exhibit *entanglement* plays an important role. On 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

[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 scare quotes.

[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.

[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 (2011).

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. In light of the Gottesman-Knill theorem (Nielsen & Chuang, 2000, 464), it is clear that entanglement cannot play the role of a sufficient condition. According to this theorem, any quantum computation which exclusively utilises the elements of a restricted subset of quantum gates[8] can be efficiently simulated by a classical computer. Interestingly, among the quantum informational protocols which can be so characterised are the teleportation and superdense coding protocols, and both of these (and others) involve the use of entangled quantum states. As for the assertion that entanglement is a necessary condition, this has gained wide acceptance and seems to be confirmed 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).

Jozsa & Linden's result does not seem to extend to *mixed* states, however, for Biham et al. (2004) have shown that it is possible to achieve a modest (sub-exponential) speedup using unentangled mixed states, while 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 features *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 lieu of these results, it is tempting to conclude that it is not necessary to appeal to entanglement at all in order to explain computational speedup and that the investigative focus should shift to the physical characteristics of quantum discord or some other such quantum correlations instead.

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. In the case where *sub-*

[8]These are the Clifford group of gates, which include the Hadamard, phase, controlled-not, and Pauli measurement gates.

exponential speedup has been demonstrated with unentangled mixed states, this has been accomplished through the use of so-called pseudo-entanglement. But while pseudo-entangled states are separable by definition, I will argue that there is nevertheless a clear sense in which entanglement plays a role in the computational work done by such states. Further, it can be shown that in order to turn the sub-exponential speedup into exponential speedup in Biham et al.'s example it is necessary to move from a pseudo-entangled state to an entangled state.

As for the concept of quantum discord, while it is indeed a useful information-theoretic concept, perhaps as useful as the concept of entanglement for the study of certain mixed-state quantum computational algorithms, I will argue that it is nevertheless misleading and indeed that it is likely erroneous to view it as a resource that is essentially distinct from quantum entanglement. Rather, one should view both discord and entanglement as manifestations of the same underlying physical resource, and indeed that entanglement is the more fundamental of these. In support of this conclusion I will appeal to recent work done by Fanchini et al. (2011), Brodutch & Terno (2011), and Devi et al. (2011) who show, respectively, that there is a conservation relation between discord and entanglement in tripartite settings; that entanglement must be shared between two parties in order to bilocally implement any bipartite quantum gate; and that a generalisation of the measurement scheme employed in the analysis of quantum correlations results in a collapse of the distinction between quantum discord and quantum entanglement.

This paper will proceed as follows. After introducing the concept of entanglement in §2, I will consider the role it plays in pure state quantum computation in §3, and I will show how what looks like a counter-example to the claim that entanglement is a necessary component of the explanation of speedup 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. The main concern of the paper will be taken up in §4 where I examine the more serious challenges 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 (§4.2).

2 Quantum Entanglement

Consider the following 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:

	q_1	q_2
(a)	$\|0\rangle$	$\|0\rangle$
(b)	$\|0\rangle$	$\|1\rangle$
(c)	$\|1\rangle$	$\|0\rangle$
(d)	$\|1\rangle$	$\|1\rangle$

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]

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$
$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

[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 $|\alpha\rangle \otimes |\beta\rangle$.

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 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 ($|\Psi^-\rangle$), 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. However any single $\hat{z}+$ experiment on just one of the two qubits will yield $|0\rangle$ or $|1\rangle$ with equal probability, for the marginal probabilities are completely mixed.

We have been discussing pure states, but the concepts of separability and of entanglement are applicable to mixed states as well. 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. After drawing the ball, we inform our friends Alice, Bob, Charles, and so on, that the outcome of the draw was i, after which they all locally create their own individual quantum states ρ_i^X (where ρ_i^X is the density matrix representation of X's state corresponding to outcome i). After creating these states they then discard the information they were given about the result of the draw. The resulting state of the overall system will be:

$$\rho^{ABC\ldots} = \sum_i p_i \rho_i^A \otimes \rho_i^B \otimes \rho_i^C \otimes \ldots \tag{1}$$

If all of the ρ_i^X are either pure or separable, then so is the overall state. In general, however, determining whether a mixed state of the form (1) is entangled is more subtle, because in general the decomposition of mixtures is non-unique. For instance, the reader can verify that a mixed state ρ, which

[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.

[12] Not all entangled states are maximally entangled states. For instance, the state $|\phi\rangle = \sqrt{\frac{1}{3}}|01\rangle + \sqrt{\frac{2}{3}}|10\rangle$, though entangled, is not a maximally entangled state. For more on the theory of entanglement measures, see Plenio & Virmani (2007).

is 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

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

since the two preparations will yield identical density matrices. In particular, as we will see in more detail later, a state that is prepared as a mixture of entangled states can sometimes be rewritten (and hence prepared) as a mixture of pure product states.[13]

The phenomenon of entanglement has deep implications for our understanding of the physical world. Consider an alternative theory of quantum mechanics in which λ is an assignment to a set of hidden variables determining the outcomes of experiments on the two subsystems of a Bell pair. Suppose λ satisfies the condition that it assigns probabilities to outcomes of experiments on the first subsystem that are independent of experimental outcomes on the second subsystem (and vice versa); i.e.,

$$p^a_\lambda(x_a|a,b) = p^a_\lambda(x_a|a,b,x_b). \tag{2}$$

This condition has variously been called *completeness* (Jarrett, 1984), *outcome independence* (Shimony, 1993), and *separability* (Howard, 1997). Bell's inequalities imply that any theory consistent with the predictions of quantum mechanics which satisfies (2) must assign different probabilities to outcomes of experiments on the first subsystem depending on the *choice of test* that is performed on the second subsystem; i.e., it must violate the condition that

$$p^a_\lambda(x_a|a,b) = p^a_\lambda(x_a|a,b'). \tag{3}$$

Jarrett and Howard call this second condition *locality*, while Shimony calls it *parameter independence*. It turns out, in fact, that Bell's inequalities imply

[13]The questions of which mixed states are entangled states, and of how much entanglement is present in a given state, are fascinating ones and the interested reader is encouraged to consult Plenio & Virmani (2007) for a more detailed discussion.

that any theory that is consistent with the predictions of quantum mechanics must violate either (2) or (3). In particular, a fully deterministic hidden variables theory, which the reader should convince herself must necessarily satisfy (2), must therefore necessarily violate (3). On the other hand, standard quantum mechanics obviously violates (2), but satisfies (3). It is worthwhile to note that a violation of (3) necessarily brings one into conflict with Special Relativity, but that it is not obvious that a mere violation of (2) does so (Shimony, 1993), even on a dynamical collapse interpretation of quantum mechanics (Myrvold, 2002).

We will have to forego a detailed consideration of the fundamental physical significance and interpretation of quantum entanglement, as such a discussion would bring us far beyond the issues relevant to this paper. Instead, in the remainder of the paper we will focus on the use that is made of entanglement as a quantum information theoretic resource, in particular, within the quantum computer. For these purposes my intention is to continue to characterise entanglement as neutrally and uncontroversially as possible.

3 Entanglement in the quantum computer

3.1 The Deutsh-Jozsa algorithm

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

$$|0^n\rangle|1\rangle \xrightarrow{H} \left(\frac{1}{2^{n/2}}(|0\rangle+|1\rangle)^n\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$
$$= \left(\frac{1}{2^{n/2}}\sum_{x}^{2^n-1}|x\rangle\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right). \quad (4)$$

The unitary transformation,

$$U_f(|x\rangle|y\rangle) =_{df} |x\rangle|y\oplus f(x)\rangle, \quad (5)$$

is then applied, which has the effect:[14]

$$\xrightarrow{U_f} \left(\frac{1}{2^{n/2}}\sum_{x}^{2^n-1}(-1)^{f(x)}|x\rangle\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right). \quad (6)$$

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 (6) will have positive phase, and half negative. After applying the

[14] Given the state $|x\rangle(|0\rangle-|1\rangle)$ (omitting normalisation factors for simplicity), note that when $f(x)=0$, applying U_f yields $|x\rangle(|0\oplus0\rangle-|1\oplus0\rangle) = |x\rangle(|0\rangle-|1\rangle)$; and when $f(x)=1$, applying U_f yields $|x\rangle(|0\oplus1\rangle-|1\oplus1\rangle) = |x\rangle(|1\rangle-|0\rangle) = -|x\rangle(|0\rangle-|1\rangle)$.

final Hadamard transform, the amplitude of $|0^n\rangle$ will be zero.[15] 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.

It is often suggested that the entanglement present in states like (6) is a necessary component of any explanation of quantum speedup.[16] I will call this the *necessity of entanglement thesis* (NET), and it has been defended, for instance, by Ekert & Jozsa (1998) and Steane (2003). Consider the individual state spaces of two quantum mechanical systems, $\mathcal{H}_1^{d_1}$ and $\mathcal{H}_2^{d_2}$, where d_1 and d_2 are the dimensionality of the first and second system, respectively. In quantum mechanics, the overall state space of the combined system is given by the tensor product of the two systems, $\mathcal{H}_1^{d_1} \otimes \mathcal{H}_2^{d_2}$, with dimensionality $d_1 \cdot d_2$. Thus the state space of a combined system of n two-dimensional qubits is $\otimes^n\mathcal{H}^2$, with overall dimensionality 2^n. In classical mechanics, on the other hand, the total state space of two individual subsystems $\omega_1^{d_1}, \omega_2^{d_2}$ is given by the cartesian product, $\omega_1^{d_1} \times \omega_2^{d_2}$, with dimensionality $d_1 + d_2$. Thus the dimensionality of the state space of a classical system of n two-dimensional subsystems is $2n$.

As Ekert & Jozsa note, the possibility of entangled quantum systems is what is responsible for this difference in the allowable state space. To illustrate, consider how one would go about representing a general superposition of n two-dimensional systems classically. It is possible to describe certain

[15] 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:

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

[16] The attentive reader who has noticed that there is actually no entanglement in (6) when $n = 1$ will be somewhat puzzled by this statement. 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 necessity of entanglement thesis. This will be clarified shortly.

classical systems in terms of superpositions; for instance, the state of motion of a vibrating string can be characterised as a superposition of its two lowest energy modes, in the same way that the state of a qubit can be characterised as a superposition of the states $|0\rangle$ and $|1\rangle$. The joint state of a system of n strings, however, will always be a *product* state; *general* superpositions, of which there are 2^n possibilities, and which include, in particular, entangled states, cannot be physically represented using n classical systems in this way. As an alternative, one may use a single classical system which allows for the discrimination of 2^n resource levels within it. The cost of such a representation scales exponentially with n, however, either (if the spacing between resource levels is kept fixed) in terms of the total amount of resource required, or (if the total amount of the resource is kept fixed) in terms of the increasing precision required to discriminate the different resource levels. Thus, because quantum mechanical states can be entangled with one another, they allow us to fully exploit the representational capacity of Hilbert spaces, and it is this capacity for efficient representation that is required for quantum computational speedup, according to the NET.

At first sight, however, the following consideration seems to be problematic for the NET. Consider the Deutsch-Jozsa algorithm 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 very first quantum algorithm developed and as the first example of what has since come to be known as quantum speedup. If one considers the steps of Cleve et al.'s improved version of the algorithm, however, then the reader can confirm that 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 NET 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.

One method for doing this (cf. Abbott, 2010) 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.[17] The algorithm proceeds in the following way. We

[17]Regarding the physical realisation of such a computer, note that complex numbers can be used, for instance, to model the impedances of electrical circuits and that we can

first note that the action of U_f on the first n qubits in (6) can, for the case of $n = 1$, be expressed as:[18]

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

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, the sign will tell us *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, 2010) that no entanglement is present in (6) 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, (5) is an entangling evolution and (6) 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 thus it is no longer possible to produce an equally efficient classical counterpart to the Deutsch-Jozsa algorithm (cf. Abbott, 2010).

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

apply the superposition theorem to their analysis.

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

entanglement in quantum computational speedup, the fact that Deutsch's algorithm does not require entanglement to succeed for certain special cases actually provides (since in these cases it can be de-quantised) evidence for the NET.

4 Quantum computing with mixed states

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."[19] 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 by definition.

4.1 The mixed-state Deutsch-Jozsa algorithm

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

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

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) and remains so under unitary evolution just so long as

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

Now consider the Deutsch-Jozsa algorithm again (cf. §3.1). This time, however, instead of beginning with the pure state $|0^n\rangle|1\rangle$, we begin with the pseudo-pure state:

$$\rho = \varepsilon|0^n\rangle|1\rangle\langle 0^n|\langle 1| + (1-\varepsilon)\mathscr{I}. \tag{7}$$

[19] Multi-partite entanglement is entanglement between multiple parties (in general, more than two). See Plenio & Virmani (2007) for a more detailed discussion.

The algorithm continues as before, except that this time our probability of success is not unity.

To illustrate: imagine that we write some of the valid boolean functions $f : \{0,1\}^n \to \{0,1\}$ onto balls which we 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 will certainly succeed when ρ is in its pure part;[20] i.e., $|0^n\rangle|1\rangle\langle 0^n|\langle 1|$. This occurs with probability ε. When ρ is in its completely mixed part, on the other hand, then since there are 2^n possible values that can be obtained for z, the probability of successfully obtaining $z = 0$ in this case is $1/2^n$. The overall probability of success for the initial state ρ when f is constant is thus:

$$P(z = 0|f \text{ is constant}) = \varepsilon + (1 - \varepsilon)/2^n. \tag{8}$$

The probability of failure is:

$$P(z \neq 0|f \text{ is constant}) = \frac{2^n - 1}{2^n} \cdot (1 - \varepsilon). \tag{9}$$

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

$$P(z \neq 0|f \text{ is balanced}) = \varepsilon + \frac{2^n - 1}{2^n} \cdot (1 - \varepsilon), \tag{10}$$

$$P(z = 0|f \text{ is balanced}) = (1 - \varepsilon)/2^n. \tag{11}$$

Now consider 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 0.[21] On the

[20] As we noted in §2, mixed states such as (7) can be prepared in a variety of ways. In order to see clearly why (8-11) hold, however, it is easiest to assume that the state has been prepared as in (7).

[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).

other hand, as we should expect given (8-11), 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.

4.1.1 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 quantum speedup at all. On the one hand, from the point of view of computational complexity theory, 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.[22] 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 (7) 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

[22]For more detail on the basic concepts of computational complexity theory, see Papadimitriou (1994).

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.[23] 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.

When one considers the state (7) and the relations (8-11), one can say that there is an intuitive sense in which entanglement is playing a role in the computational ability of that state, even when ε is small enough so as to make the state unentangled by definition. To illustrate my meaning, consider the following, somewhat fanciful, situation. A fisherman in a maritime society with a largely fish-based economy one day discovers that by painting her nets yellow she is able to increase her yield of fish by a significant factor. The practice quickly becomes widespread, but after a time it is realised that the supply of yellow pigment is quickly becoming depleted and that the society's new-found affluence is fast becoming unsustainable. In the face of this, and with the aim of economising the use of yellow pigment, the society's best scientists undertake an investigation into just how yellow a net must be in order to effect an improvement in catch size. They experiment with various paint mixes, and find that the average catch size of a net decreases as they decrease the proportion of yellow pigment in the mixture used to paint it. Nevertheless, as long as even a small proportion of yellow paint is used, there is an improvement in catch size over what is possible when no yellow paint is added to the mixture at all. Amazingly, they discover that there is an improvement in catch size even when the proportion of yellow paint in the mixture is vanishingly small—small enough so that one would not call the resulting colour yellow on any reasonable criterion of yellowness.

Now if the scientists were to conclude that their experiments demonstrate yellow pigment is not necessary after all, we would judge them to be gravely in error. We would say that although it is clear that only a vanishingly small amount of yellow pigment is necessary to effect an improvement in catch size, "vanishingly small" $\neq 0$; for if *no* yellow paint at all were added to the

[23]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.

mixture, there would be no increase in catch size. The situation here seems to be analogous to the case of the mixed-state Deutsch-Jozsa algorithm, with the pure state $|0^n\rangle|1\rangle\langle 0^n|\langle 1|$ playing the role of yellow pigment and ε its proportion in the mixture. With probability ε, the unitary transformation (5) takes $|0^n\rangle|1\rangle\langle 0^n|\langle 1|$ to an entangled state and this leads to an increased probability of success despite the fact that ε is small enough to make the overall state of the system unentangled and despite the fact that ε may be vanishingly small in principle.

There is an important disanalogy between the two cases, however; in the case of the paint mixture, we could always consider it to be composed of a certain proportion of yellow pigment combined with a certain proportion of, say, uncoloured paint; but in the case of the mixed-state algorithm, (7) is only *one* way of preparing ρ. It is possible to prepare ρ in an alternate way if we so desire, for instance (when ε is sufficiently small) as a product of n pure states. And since such a state remains separable under unitary evolution, it will be capable of a product state representation throughout the computation. The pseudo-pure state representation may well function as a tool for *finding* mixed quantum states that display a computational advantage—but *once found*, it seems as though we may do away with this representation entirely. Hence there seems to be no need to invoke entanglement in order to explain the speedup obtainable with this state.

Such a conclusion ignores the nature of the computational process that is actually occurring in the computer, however. In particular, it ignores the fact—which we emphasised in our discussion of de-quantisation—that the unitary evolution (5) is, in general, an *entangling evolution*. If the computer is more likely than a classical computer to correctly guess the type of a given function, it is because it takes some of the product states in the ensemble, those of the form (4), to entangled states of the form (6).

Assume the computer is more effective than a classical computer at guessing the type of a function that it has been given, and let $\rho_P = \sum_i p_i \rho_i^A \otimes \rho_i^B \otimes \rho_i^C \otimes \dots$ be a mixed product state representation of the computer before the application of the transformation U_f and $\rho'_P = \sum_j p_j \rho_j'^A \otimes \rho_j'^B \otimes \rho_j'^C \otimes \dots$ be a mixed product state representation of the computer after U_f has been applied. The significance of the fact that U_f is an entangling transformation is that when it is applied to ρ_P, the state will *not* evolve to ρ'_P—rather, it will evolve to the state ρ'_E, which is a mixture of entangled states. Since both ρ'_P and ρ'_E share the same density matrix representation, ρ'_E can then be *re-expressed* as the mixed product state, ρ'_P; but we cannot directly obtain

ρ'_P from an application of U_f to ρ_P.[24]

To make the same point but from a different perspective, consider the density matrix representation of the state of the computer, ρ_{ini}, before the application of the unitary transformation U_f. This representation subsumes various preparation procedures, including the pseudo-pure preparation (7); and a unitary transformation applied to any of these preparations will yield a state whose preparation can be subsumed under the density matrix representation ρ_{fin}. Now we know that U_f evolves the pure product state (4) to the pure entangled state (6), and thus we know that U_f will evolve the pseudo-pure state (7) to a mixture of entangled states. But because the density matrix representation of the computer's final state, ρ_{fin} must subsume all evolutions from preparations associated with ρ_{ini}, after evolving ρ_{ini} it will be possible to express ρ_{fin} as a mixture of entangled states; i.e., ρ_{fin} will be a pseudo-entangled state. Thus because U_f is an entangling transformation, ρ_{fin} will be a pseudo-entangled state, and our situation *will* be analogous to the situation of the scientists in our imaginary maritime society—and we should come to a similar conclusion, for we, like them, have been given no reason to abandon the NET.

4.2 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 this does not constitute a counter-example to the NET, since the computational algorithm in question is successful only when the evolution of the state of the computer is an entangling evolution; therefore the final state of the computer will always contain some entanglement (i.e., the state will be pseudo-entangled) despite the fact that the overall state will be unentangled.

We now consider another purported counter-example to the NET. This

[24] I am indebted to Wayne Myrvold for suggesting this line of thought, and also to the discussion in Jozsa & Linden (2003, §5). I should also note that Long et al. (2002) make a similar point; 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.

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 false. The NET, however, is not the claim that any state that displays quantum computational speedup must be entangled; it is, rather, the different claim that entanglement must play a role in any *explanation* of quantum speedup. We saw in the last section how it is possible for the first claim to be false and the latter (the NET) to be true. In this section I will address the objection that the NET 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. I will argue that this conclusion is misguided. Quantum discord is indeed an enormously useful theoretical quantity for characterising mixed-state quantum computation; nevertheless, I will argue that quantum discord is 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),[25] 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,[26] 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:

$$\begin{aligned}\rho_{n+1} &= \frac{1}{2^{n+1}}\big(|0\rangle\langle 0| \otimes I_n + |1\rangle\langle 1| \otimes I_n + \alpha|0\rangle\langle 1| \otimes U_n^\dagger + \alpha|1\rangle\langle 0| \otimes U_n\big) \\ &= \frac{1}{2^{n+1}}\begin{pmatrix} I_n & \alpha U_n^\dagger \\ \alpha U_n & I_n \end{pmatrix}. \end{aligned} \tag{12}$$

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

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

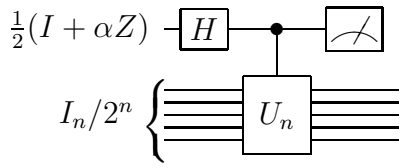

Figure 1: The DQC1 algorithm for computing the trace of a unitary operator.

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

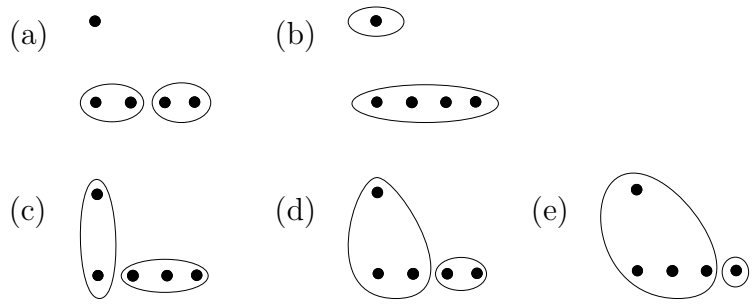

Figure 2: Some of the bipartite splits possible in the DQC1 for $n = 4$. No entanglement can ever occur amongst the n unpolarised qubits (a) or between the polarised qubit and the rest (b); however, bipartite splits such as (c), (d), and (e) can exhibit entanglement (Datta et al., 2005).

the radius of the separable ball decreases exponentially faster than $2^{-(n+1)/2}$, (Datta et al., 2005, 2).

It appears, therefore, that the state (12) must be an entangled state; 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[27]) 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. The fact that only a vanishingly small amount of entanglement can be found in (12) even when α is relatively large seems, for some, to run counter to what one would expect to be the case if the NET were true. In fact, both 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

[27]The definition of multiplicative negativity is given in Vidal & Werner (2002).

role in quantum speedup, at least in these cases. The result has been a shift in investigative focus from entanglement to other types of quantum correlations. One alternative in particular, *quantum discord*, has received much attention in the literature in recent years (e.g., Merali, 2011).

Quantum discord (Zurek, 2000; Ollivier & Zurek, 2002; Henderson & Vedral, 2001)[28] quantifies the difference between the quantum generalisations of two classically equivalent measures of mutual information,

$$\mathcal{I}_c(A:B) = H(A) + H(B) - H(A,B), \tag{13}$$

$$\mathcal{J}_c(A:B) = H(A) - H(A|B). \tag{14}$$

These two expressions are not equivalent quantum mechanically, for while (13) has a straightforward quantum generalisation in terms of the von Neumann entropy S:

$$\mathcal{I}_q(A:B) = S(A) + S(B) - S(A,B), \tag{15}$$

things are more complex for the quantum generalisation of (14). 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 (14), the expression:

$$\mathcal{J}_q(A:B) = S(A) - S(A|\{\Pi_j^B\}). \tag{16}$$

We now define discord as the minimum value (taken over $\{\Pi_j^B\}$) of the difference between (15) and (16):

$$\mathcal{D}(A,B) =_{df} \min_{\{\Pi_j^B\}} \mathcal{I}_q(A:B) - \mathcal{J}_q(A:B), \tag{17}$$

[28] 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.

which is, in general, non-zero for mixed states. For pure states, quantum discord is equivalent to the entropy of entanglement, and therefore reduces to entanglement (Datta et al., 2008, 3).[29]

4.2.1 Explaining speedup in the DQC1

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, and tests to detect entanglement along other bipartite splits in the DQC1 when $\alpha \leq 1/2$ have (thus far) been unsuccessful.[30] When we consider the correlations between the polarised and unpolarised qubits from the point of view of *quantum discord*, however, 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." I believe it is a mistake, however, to conclude as they and others do that entanglement may play no role in the explanation of the quantum speedup of the DQC1 (Datta et al., 2008; Vedral, 2010; Merali, 2011).

[29]For a more detailed discussion of the entropy of entanglement, $E(|\psi\rangle\langle\psi|) =_{df} S(\mathrm{tr}_A|\psi\rangle\langle\psi|) = S(\mathrm{tr}_B|\psi\rangle\langle\psi|)$, see Plenio & Virmani (2007).

[30]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:

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

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 (see Plenio & Virmani (2007) for a definition and discussion 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.

As is well known, there has been and continues to be debate within the philosophical community over precisely how to characterise a proper scientific explanation. On some accounts, all legitimate scientific explanation must appeal to the causal mechanisms that give rise to the phenomena they purport to explain (e.g., Salmon, 1984; Humphreys, 1989). Such accounts represent a somewhat extreme view in that they rule out, as not being true explanations, mathematical and structural explanations which by their very nature do not appeal to causal processes. More liberal views (Railton, 1978) allow that scientific explanation is not always causal explanation, but nevertheless take a highly reductionist view in holding that *all* explanations, including those given in the special sciences, must be given in terms of the concepts and quantities of physics in order to be classified as true and complete explanations.[31] I do not believe that *all* explanations, regardless of their subject matter, must be given in physical terms; nor do I believe that all *physical* explanations must explicitly refer to causal processes and mechanisms in order to count as true explanations. I do believe, however, that explanations of *physical processes*—for instance, the computational process that we are now discussing—must be given in physical terms, and that when possible, such explanations must appeal to the fundamental concepts of physical theory which give rise to the phenomena under investigation.[32]

What we are seeking, here, is a physical explanation for the speedup displayed by the DQC1 circuit. It is not enough, therefore, to point to the information theoretic measure, quantum discord, as the explanation for this speedup without first seeking for a physical interpretation of this concept. Fortunately, we have an important first step toward such an interpretation—an operational definition of the concept—independently provided by Madhok & Datta (2011) and by Cavalcanti et al. (2011),[33] who show that it is possible to characterise quantum discord in terms of the entanglement consumed in an extended version of the quantum state merging protocol.

In this protocol, three parties: Alice, Bob, and Corey, share a state

[31]Railton (1981) allows that partial explanations (e.g., explanations given wholly in terms of the concepts and terms of one of the special sciences) can still convey what he calls *explanatory information*, but these nevertheless do not qualify as true and complete explanations in the proper sense of that term.

[32]The reader who does not consider my belief in these propositions a sufficient reason to believe them himself is encouraged to consult Cuffaro (2008) for an actual argument.

[33]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.

$|\psi_{ABC}\rangle$. Quantum state merging characterises the process,

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

by which Alice effectively transfers her part of the state to Bob while maintaining its coherence with Corey's part. It turns out that in order to effect this protocol a certain amount of entanglement must be consumed. When we add to this the amount of entanglement needed (as quantified by the entanglement of formation[34]) 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 Corey at the time the state is prepared.

Cavalcanti et al.'s operational interpretation of discord has an affinity with Fanchini et al.'s own illuminating analysis of the DQC1 circuit (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. From this tripartite point of view, therefore, there is just as much entanglement 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 $\alpha > 0$. All of this accords with what we would expect given Cavalcanti et al.'s operational interpretation of quantum discord: an increase in quantum discord requires an increase

[34]See Plenio & Virmani (2007) for a definition and discussion of the entanglement of formation.

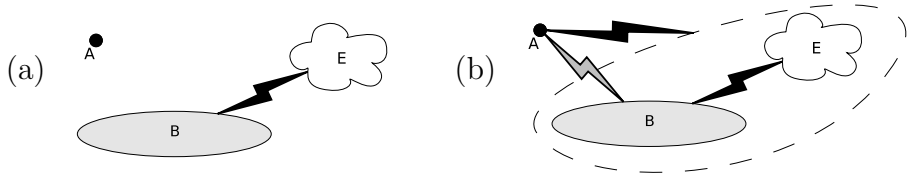

Figure 3: A (pure) tripartite representation of the elements of the DQC1 protocol before (a) and after (b) the application of the controlled not gate. Black and grey thunderbolts represent entanglement and discord, respectively. After the application of the controlled not gate, there is an increase in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

in the entanglement available for consumption in a potential quantum state merging process.

Fanchini et al. speculate that it is not the presence of entanglement or discord 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[35] *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 itself, these considerations already amount to confirmations of the NET, 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. I believe, however, that the further case can be made that we can eliminate quantum discord entirely from the physical explanation of quantum speedup (though such a characterisation may be less practical for many purposes), 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 to describe the evolution of a system when we can view the system as uncorrelated with its external environment. When the system is initially correlated

[35]Bilocal implementation means, in this context, an implementation in which Alice and Bob are limited to LOCC operations. See Plenio & Virmani (2007).

with the environment, however, the reduced dynamics of the system may not be completely positive.[36] 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 from the point of view of a measurement framework incorporating 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 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 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 not completely positive maps are 'unphysical' is an interesting and important one but I will not address it here (see Shaji & Sudarshan 2005 for a discussion). 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 NET, the DQC1 model of computation rather serves to highlight 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

[36]For more information on completely positive and not completely positive maps, see Sudarshan et al. (1961); Jordan & Sudarshan (1961); Jordan et al. (2004); Carteret et al. (2008).

over classical computation, but in recent years this idea has faced important challenges in the form of counter-examples. We examined three such counter-examples in this paper. Upon closer examination we found none of these three, neither the lack of entanglement in the original version of Deutsch's algorithm, nor 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

Abbott, A. A. (2010). The Deutsch-Jozsa problem: De-quantisation and entanglement. arXiv:0910.1990v3.

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.

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.

Carteret, H. A., Terno, D. R., & Życzkowski, K. (2008). Dynamics beyond completely positive maps: Some properties and applications. *Physical Review A*, *77*, 042113.

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. (2008). *A Metaphysically Neutral Theory of Singular Scientific Explanation*. Master's thesis, Concordia University, Montréal.

Cuffaro, M. E. (2011). Many worlds, the cluster-state quantum computer, and the problem of the preferred basis. arXiv:1110.2514v1.

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. arXiv:1105.4115v2.

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.

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.

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

Howard, D. (1997). Space-time and separability: Problems of identity and individuation in fundamental physics. In R. S. Cohen, M. Horne, & J. Stachel (Eds.) *Potentiality, Entanglement and Passion-at-a-distance*, (pp. 113–142). Dordrecht: Kluwer Academic Publishers.

Humphreys, P. (1989). Scientific explanation: The causes, some of the causes, and nothing but the causes. In P. Kitcher, & W. C. Salmon (Eds.) *Scientific Explanation (Minnesota Studies in the Philosophy of Science, Volume XIII)*, (pp. 283–306). Minneapolis: University of Minnesota Press.

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

Jarrett, J. P. (1984). On the physical significance of the locality conditions in the Bell arguments. *Noûs*, *18*, 569–589.

Jordan, T. F., Shaji, A., & Sudarshan, E. C. G. (2004). Dynamics of initially entangled open quantum systems. *Physical Review A*, *70*, 052110.

Jordan, T. F., & Sudarshan, E. C. G. (1961). Dynamical mappings of density operators in quantum mechanics. *Journal of Mathematical Physics*, *2*, 772–775.

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.

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.

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. (2002). On peaceful coexistence: Is the collapse postulate incompatible with relativity? *Studies in History and Philosophy of Modern Physics*, *33*, 435–466.

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.

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.

Railton, P. (1978). A deductive-nomological model of probabilistic explanation. *Philosophy of Science*, *45*, 206–226.

Railton, P. (1981). Probability, explanation, and information. *Synthese*, *48*, 233–256.

Salmon, W. C. (1984). *Scientific Explanation and the Causal Structure of the World*. Princeton: Princeton University Press.

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

Shaji, A., & Sudarshan, E. C. G. (2005). Who's afraid of not completely positive maps? *Physics Letters A*, *341*, 48–54.

Shimony, A. (1993). *Search for a Naturalistic Worldview, Volume 2: Natural Science and Metaphysics*. Cambridge: Cambridge University Press.

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

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.

Sudarshan, E. C. G., Mathews, P. M., & Rau, J. (1961). Stochastic dynamics of quantum-mechanical systems. *Physical Review*, *121*, 920–924.

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.

Vidal, G., & Werner, R. F. (2002). Computable measure of entanglement. *Physical Review A*, *65*, 032314.

Zurek, W. H. (2000). Einselection and decoherence from an information theory perspective. *Annalen der Physik*, *9*, 855–864.