Do We Need 'Quantum' for Quantum Computing?

D. K. Ferry*, R. Akis, M. J. Gilbert, and I. Knezevic
Department of Electrical Engineering and Center for Solid State Electronics Research
Arizona State University, Tempe, AZ 85287-5706

ABSTRACT

The concept of quantum computing has arisen as a methodology by which very rapid computations can be achieved. There also has been considerable discussion about physical implementations of the qubit. This has led, in recent years, to a situation in which quantum computing and quantum information theory are being rapidly developed. In general, the specific advantages offered by quantum computing have been somewhat nebulous. On the one hand, faster computing was promised, but we now know that no speedup of most algorithms exists relative the speed that can be obtained with massive parallel processing. Then, we are promised that the use of *entanglement* will make quantum computing possible with a much smaller use of resources. Yet, entanglement must be viewed as a hidden variable, which is not accessible in experiment. How does this provide the speedup? We have suggested that analog processing may provide a suitable alternative, and may be the basis which provides the speedup in quantum computing, but this is a controversial assertion. In this talk, we will discuss these particular viewpoints, along with several approaches to a wave basis for (quantum) computing.

Keywords: Computing, quantum physics, entanglement, wave processing

1. INTRODUCTION

A new computing paradigm has appeared in the past decade—quantum computing. This concept brings together ideas from information transmission, computer science, quantum physics, and quantum electronics (including optics)[1]. Quantum computing has become of interest due to the suggestion that it provides a methodology by which very rapid computations may be achieved with no dissipation[2]. In general, the speed of these computations has been compared to that of classical, sequential digital computers in which a single processor is used. Indeed, the speed of quantum computing has promised the prospect of factoring large integers into their prime factors[3], a task that is known to be quite hard on classical computers. In Shor's algorithm[3], as well as other quantum computing algorithms, a key subroutine is the *quantum* Fourier transform (QFT)[4]. In general, it is thought that it is this algorithm that provides the speedup found in quantum computing. The primary difference between the bits on a classical digital computer and the qubits of a quantum computer is that the latter incorporate quantum mechanical phase factors that allow a continuous range of projection onto the "0" and "1" states. As such, the qubits themselves should be thought of as *analog* objects. That is, the state is a continuous (complex) variable rather than merely a "0" or a "1". Hence, a quantum computer is essentially a parallel array (the set of qubits) of analog structures. Using this fact, we have proposed previously an array processor, using the quantum waves themselves, analogously to a classical antenna array, to perform a Fourier transform operation[5]. The use of the quantum waves for processing offers an advantageous implementation in semiconductor integrated systems[6].

There has subsequently been considerable discussion about the efficacy of such an approach, and we will discuss the constraints and limitations, as well as the questions which arise, in this paper. Questions which have to be asked are: is entanglement necessary and how does it appear in the array processor, what are the needed extra resources and how do they appear, how is the speed comparable to the qubit-based QFT processor, and how might other algorithms appear[7]. It is not clear that we can answer all of these questions to anyone's satisfaction (but our own), but they will be discussed in the following sections. In the next section, the array processor and Fourier transforms will be reviewed, before

* ferry@asu.edu; phone 1 480 965-2570; fax 1 480 965-8058; www.eas.asu.edu/~ferry/ferry.html

discussing the QFT itself. Then, we turn to issues of speedup and resources before addressing the critical issue of the role of entanglement and what it means. Hopefully, we will be able to at least identify a number of crucial questions that should be asked to clear away some of the general obfuscation that exists in the quantum computing world.

2. ANALOG ARRAY PROCESSING

Before proceeding too far, it is useful to see how the Fourier transform can be implemented in a wave processor. In general, we can expand any function (in general, this is a periodic function) in a discrete transform as

$$f(x_k) = \sum_j c_j \exp\left(i\omega_j x_k\right) \quad . \tag{1}$$

The various exponentials in this expansion form a set of *basis vectors* in the hyperspace of this expansion. If this set is complete and has a proper *norm* (provided by the normalization constant and which gives us the orthonormality of the basis vectors and the definition of an inner, or *scalar*, product), then they form a finite Hilbert space[8]. The quantum *wave* version works on the idea that waves propagating from a series of sources will have different phase shifts, due to different path lengths[5]. The path difference introduces a phase shift of

$$\Delta\varphi = k_0 d \cos\vartheta \quad , \tag{2}$$

where $k_0 = \omega/v_{group}$ is the propagation vector and d and ϑ are the spacing of the sources and the angle measured from the line of the sources. If the relative signal at each element is given by

$$I_n = I_{0,n} e^{i\varphi_n} \quad , \tag{3}$$

then the array pattern (which is equivalent to the envelope function in quantum mechanics) is given by

$$F(\vartheta) = \sum_{n=0}^{N-1} I_n e^{ik_0 nd\cos\vartheta} = \sum_{n=0}^{N-1} I_n e^{i\Omega t_n} \quad , \tag{4}$$

where $\Omega = \omega\cos\vartheta$, and $t_n = nd/v_{group}$. Hence, the Fourier variable is the angle in the output plane, and all "frequencies" can be computed at one time. In this sense, the output plane corresponds to a "frequency" space, while the input sequence of signals is a "temporal" space. Or, these can be viewed as the spatial frequency and space coordinate, respectively.

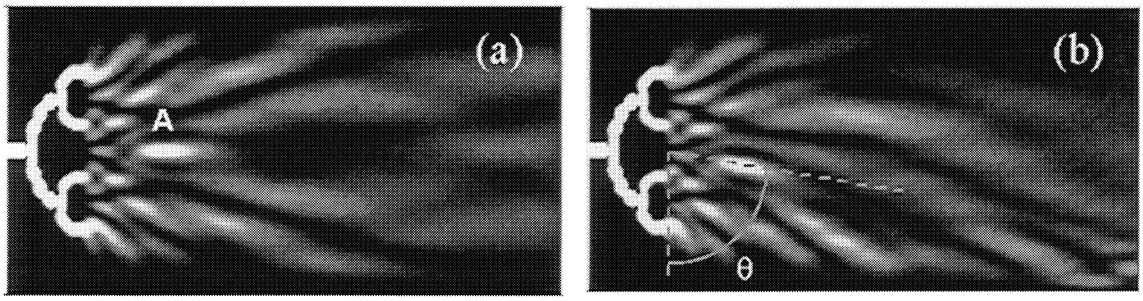

Fig. 1. (a) Radiation pattern from four quantum waveguides in which there is no phase shift between the sources. (b) Radiation pattern when a normal magnetic field of 50 mT is used to introduce a phase shift between the sources.

In Fig. 1, we show one implantation of a wave-based Fourier processor. Here, the sources are quantum waves which emanate from four waveguides. Hence, an interference pattern, representative of the Fourier transform of the input sources, should be formed at any detection plane to the right of the sources. In Fig. 1(a), we show the interference pattern that arises from a simulation of such an array, in which Schrödinger's equation is solved on a finite-difference grid using a stabilized variant of the transfer-matrix technique[9]. Here, all the sources are in phase with each other. Pictured is a region 1.4 μm long by 0.6 μm wide. All the quantum wire segments are each 0.04 μm wide, allowing a single propagating mode when the Fermi energy is 80 meV. The diameter of the smaller semicircular guides is 4 times this, while the larger semicircle of guides is 8 times this width. In Fig. 1(b), we show the results of applying a magnetic field of only 50 mT normal to the plane of the device. It is clear that the main peak has been rotated to a new angle due

to the phase shift introduced between the sources. This rotation angle is linear in the magnetic field. It is clear that a modest magnetic field can be used to sweep the pattern to almost any desired angle. Alternatively, phase shifters could be placed in each of the final four arms of the array, and the phase shift introduced electrically. In this simulation, each source has equal amplitude, and we will see below that this is a crucial part of the qubit-based QFT.

How do we introduce entanglement in such a processor? In fact, as we will see below, *both the classical Fourier transform and the QFT require only superposition*, and this is easily achieved in the array pattern as shown in Fig. 1. That is, entanglement is not needed, but may be required by other parts of the algorithm prior to the QFT. Building upon a concept of the Modena group[10], we have previously shown how two coupled waveguides (see Fig. 2) can be used to form a qubit, in which switching can be achieved either by an additional magnetic field[11] or by an applied voltage bias[12]. In addition, it has been shown how two such qubits can be entangled by an interaction between the waves in the individual qubits[13]. Thus, it is clear that any needed entanglement can be provided using interactions between quantum waves prior to their arrival at the source exits for the transform processor of Fig. 1. Consequently, the quantum waveguide processing scenario is a fully viable approach to quantum computing. It is important to point out here that, in this approach, we are using quantum waves, quite in the analogy to using quantum optics to simulate quantum computing[14], although some have suggested using classical waves as well[15].

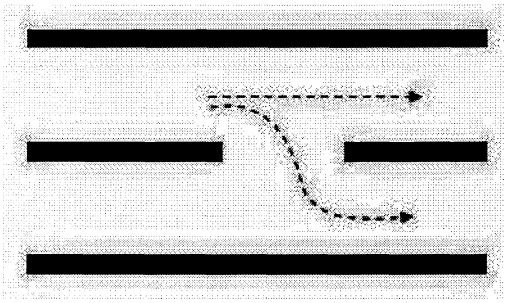

Figure 2: Two coupled quantum waveguides can be used as a qubit, in which switching is achieved by moving the output wave from one guide to the other. These guides are easily fabricated in a semiconductor heterostructure quasi-two-dimensional electron gas.

3. THE QUANTUM FOURIER TRANSFORM

In discussing the QFT, it is important to keep in mind just how much information one is utilizing. For instance, in eqn. (1), there are of order N values for each of the integers j and k. Hence, there are N^2 values of the coefficients. In one sense, we can then talk about having *analog* information of order N^2 (more will be said about this below). In this sense then, the output pattern of Fig. 1 will have some N beams, each of which has some N different possible amplitudes. *The QFT, however, is different.*

In the QFT, the system is regarded as being composed of qubits. Each qubit is composed of two basis states $|0_j\rangle$ and $|1_j\rangle$ subject to the fact that the amplitude of each qubit is required to have a magnitude of unity. This turns out to be a significant modification of the information contained in the Fourier transform. In essence, this saying that *each Fourier component contains precisely the same "energy" content. The only signal that produces this result is a delta function*, whose transform provides equal amplitude at all frequencies. This means that, in the terms of Fig. 1, only a single beam is produced in the output (given enough qubits to ensure the spatial resolution), and the direction of this beam is determined solely by the phase differences of the individual sources. Hence, this reduces the information content by a factor of *1/N*. But this single beam is precisely the important result required in the factoring algorithm. In the latter application, one seeks the periodicity in a set of numbers, and this is related to the factors. Thus, one makes use of this single delta function output and this property is quite important to the application.

In creating the QFT, only the superposition of the qubits is required, not any entanglement[4]. In the application, the entanglement appears in creation of the phase of each qubit. Thus, the set of qubits is an entangled representation of prior information processing[3,16]. In the quantum Fourier transform, two "registers" of n (= $\log_2 N$) qubits are used. The

first, or input, register is put into an entangled superposition of phase shifted values for each qubit, and the superposition of these is then formed in the output register through a sequence of qubit operations. In our proposed quantum wave implementation, we also use an input register of n qubits, which are the sources for the wave interaction of Fig. 1. Phase shifts are provided by both the wave propagation, in forming the output pattern, and in the relative phases of the input sources, which may be provided by the magnetic field or by inserting phase shifters in each waveguide.

It is quite often claimed that the QFT provides a dramatic speedup in the computational speed for algorithms which can use this approach. Indeed, it is claimed that the QFT can provide the Fourier transform in $O(n^2)$ time and complexity (that is, of order n^2 computational steps and of order n^2 logical gates)[17]. We can find the complexity of the classical Fourier transform if we view eqn. (1) as a set of N equations in the unknown complex coefficients c_j for the frequencies. Hence, the set of N equations, one for each value k, may be rewritten as

$$\mathbf{f} = \mathbf{A}\mathbf{c} \quad . \tag{5}$$

Here, the vector $\mathbf{f}$ is a $N \times 1$ column matrix whose kth row entry is $f(x_k)$. Similarly, $\mathbf{c}$ is a $N \times 1$ column matrix whose rows are the unknown (complex) coefficients c_j. The $N \times N$ matrix $\mathbf{A}$ contains the evaluations of the basis vectors. Hence, the discrete Fourier transform is equivalent to any other linear algebra problem. The complexity lies in the inversion of the $\mathbf{A}$ matrix, and naively this requires N^2 operations. However, there are faster algorithms, which make the complexity of order $N\log N$. In terms of the binary notation $N = 2^n$, then this complexity is of $O(n2^n)$, which is said to be of exponential complexity (the factor two is raised to a power). Thus, the quantum Fourier transform is said to produce exponential speedup over a classical computer. But, this is in reference to a classical *sequential* computer, and we must remember that the QFT reduces the complexity by a factor of $1/N$. It would be nice to have this same factor in the speedup of the classical case, but this is not correct. If each coefficient c_j is m bits deep (2^m distinct levels of digitization), then the information contenct is n^2m bits. The reduction to a single beam only takes off n bits. Hence, we expect that the required complexity remains of $O(2^n)$, or of exponential order. On the other hand, it turns out that the linear algebra problem (5) is a member of the class NC (referred to as Nick's class after the discoverer[18]), which is known to undergo significant speedup through the use of parallel processors. This class has been shown to have both an upper bound and a lower bound on the optimum computing time given by a polynomial in the logarithm of the number of equations (termed polylogarithmic) as[19]

$$O(\log N) \le t_{opt} \le O\left(\frac{3}{4}(\log N)^2\right) \quad . \tag{6}$$

We note that the upper bound is the same as that claimed for the quantum Fourier transform. The problem with the classical parallel algorithm, however, is the needed computer resources. There is a theorem by which the optimum computing time on a parallel architecture is achieved at the cost of an exponential number of processors, but the situation is usually worse than this. It seems that the most efficient approach can achieve the lower bound of (6) at the cost of more than N^2 processors[20]. Hence, *the ability to achieve polylogarithmic time with the quantum Fourier transform is not remarkable; the remarkable feature is that this is done with a polylogarithmic number of processors—the qubits.* Even accounting for the reduction in complexity by $1/N$, we still require of order N processors for the classical result. That is, achieving $O(n^2)$ time complexity can be done with parallel processors, but doing so with $O(n)$ qubits is the real efficiency gain. Nevertheless, the last result seems to be correct, as we can check this with a surface acoustic wave "chirp" filter. This latter is an inter-digitated transducer for which a delta function (in time) input produces a linear frequency sweep, and conversely. The required size (resources) is, in the present notation, of order N (linear in the magnitude of the frequency spectrum), and is therefore exponentially larger than the QFT. However, this is probably a trivial increase in resources given that the chirp filter exists,while the QFT is still problematic.

For our quantum wave approach, the resource need is one of area. The transform in Fig. 1 consumes area, but is probably not the most efficient approach. However, the width of the area shown in Fig. 1 is of order n. The area itself is nearly triangular, with a "height" of order $\log_2 n$. That is, for 4 sources, we require two levels of branching, which gives the quoted value. Hence, the required area is approximately $n(\log_2 n)/2$. The output area should be of order $n \times n = n^2$, and this area dominates the total area. We note that this is still within the resource bound of the QFT, which is really to be expected.

4. ENTANGLEMENT

Entanglement arose above in the context of complex algorithms which provided the state of individual qubits, which represented entangled information from previous processing. The *nonlocal* correlation between distanced quantum states has been of interest since the Einstein-Podolsky-Rosen (EPR) question[21], which is most commonly explained in terms of *nonlocally* correlated spin states[22]. Generally, the wave function for this situation is said to be *entangled*[23] and, in recent years, entanglement has become a crucial element of quantum information and quantum computing. However, it has been quite difficult to quantify entanglement itself, with measures of entanglement arising in theory,[24,25,26] but not in experiment. This difficulty exists since it is generally believed that entanglement can only occur in tensor-product Hilbert spaces, yet any physical system can also be represented by non-tensor-product spaces.

As Eckert and Jozsa[27] point out, a general system of n particles, each with two states, forms a logical basis for quantum computation in a tensor product Hilbert space, each portion of which has two states, but could as well be represented by a single particle with 2^n states. These two choices represent different basis sets, with the former capable of entanglement that must disappear in the latter. Yet, any physically measurable variable must produce an expectation value that is independent of the basis set, since one basis may be transformed into another by a properly chosen similarity transformation[28]. If entanglement is unique to a specific basis set, such as the tensor product basis set, then it is not an observable of the system and should be considered as a "hidden" variable whose value can only be determined statistically through multiple measurements. In the Appendix, we give a simple proof that no operator exists which can yield a measure of the entanglement as the result of simply taking the expectation value of that operator.

Since the entanglement is not a measurable variable, then it must be a hidden variable as stated above. But, one can argue that it may not be a variable at all, in the strictest sense, although it is certainly a parameter or property of the wave function (1). Bohm adopted a hydrodynamic picture in his hidden variable theory of quantum mechanics[29]. There, he considered the positions and momentum of the particles associated with the wave as hidden variables, but one could also assert that the quantum potential, so essential to the motion of the particles, is also a hidden variable in that it only appears in this one picture of quantum mechanics (another view of which variables are hidden is given by Holland[30]). It is in this sense that entanglement may be viewed as a hidden variable. We go further, and conclude that, since there can be no operator which yields a measure of the entanglement as its expectation value, entanglement must be a hidden variable, and must be nonlocal in character. This explains to a large measure the difficulty found in measuring the degree to which entanglement occurs. If we accept the fact that entanglement is a hidden variable, then it is easy to explain why it is so difficult to isolate and cannot be enhanced. Moreover, it is important to note that simply writing down a tensor-product Hilbert space description does not create entanglement (it can only describe this prior existing entanglement). Entanglement must occur through a physical interaction, such as the generation of the spin states in the EPR experiment. Hence, we cannot do post processing to increase this degree of nonlocal correlation between the states.

Spreeuw[31], however, has argued that *there are two types of entanglement.* One is a multi-particle entanglement which is nonlocal, and only this type should be properly termed quantum entanglement. The second type is a single particle entanglement which can be called classical entanglement. Indeed, he has demonstrated that this second type of entanglement can be treated with classical waves[32]. This is carried further, where it has been shown that local hidden variables can allow a simulation of a Bell* state[33], a result which has also been referred to as classical entanglement[34]. It is only the nonlocal entanglement that is truly quantum mechanical. Yet, this will allow us to draw a strong distinction between the two and to estimate the complexity and where the quantum mechanics is needed. We consider a neural network based associative memory. The latter is one in which partial information is used to recover the data, which we take to be an image. Such a memory uses local entanglement, which is obtained by "learning" algorithms[35]. If we use N artificial neurons, then we can store N images. Each image consists of N pixels, with an amplitude in each pixel of M levels ($= 2^m$ bits). Hence, the amount of information is n^2m bits. We can use the Fourier wave processor for this, as the output will be one of the N beam positions, which thus selects the proper image. Hence, each qubit must have nm

* A Bell state is a particularly formed entangled state between two e.g. spins, which propagate away from each other. The discussion of the information content and the measurement was the heart of the EPR discussion[21] and subsequent controversy. The Bell inequality is a limitation on the expectation values for a set of measurements[38].

distinct values for the phase. Now, we cannot use an artificial neuron for the qubit, as the latter has only a real analog signal level, and we require phase information in the complex amplitude. However, classical waves can be used to simulate the qubits quite effectively[32,36]. While we have talked about the QFT, this storage analogy carries over to other quantum algorithms, where the quantum search algorithm has been simulated with classical waves[37].

Of course, there is the objection that Bell's inequality rules out hidden variables[38], but only local ones[39]. Yet, we calmly discussed the use of local hidden variables in the previous paragraphs. In fact, Bell himself argued for the pilot wave theory exemplified by Bohm's hydrodynamic approach[40]. Werner[41] has earlier argued that EPR correlations can admit to a hidden variable model of quantum states. We add to this the experimental observations that quantum correlations already violate Bell's inequality[42]. This has been interpreted as a difference in quantum mechanics and classical mechanics—quantum physics is said to violate Bell's inequality due to nonlocal correlations (entanglement). But, we should ask: "Aren't there classical experiments on correlation which violate Bell's inequality?" In fact, this is the case and, in particular, classical simulations of qubits have shown violations of Bell's inequality[36]. Since it is assumed that one cannot really simulate quantum physics with classical systems, this must be a true classical violation of the inequality. Now, if both quantum systems and classical systems are known to violate the Bell inequality, does it really have any truth to it? This has been quite controversial and a topic of much discussion. But, recently, it has been demonstrated that there are questions about the Bell derivation, and a proper approach, taking into account the temporal correlations, does allow for local hidden variables and is compatible with all of the experiments[43,44]. This will certainly not end the discussion, but it is clear that the interpretation of quantum mechanics is still under debate.

5. CONCLUSIONS

We have discussed the quantum wave implementation and demonstrated that it is fully equivalent to the more standard qubit based QFT. Only superposition is necessary for the Fourier transform, but entanglement must be put into the qubits beforehand, if it is required. Moreover, the QFT is a not a general Fourier transform, but is a very special one that produces only a delta function in the output, which is necessary for the algorithms that have been discussed. This does not provide such a large reduction in resources as one would expect.

We have not answered the question asked at the beginning. But it seems to be clear that "quantum" is not required in many of the applications foreseen for quantum computing. Here, it is of interest to make a determination of whether true quantum entanglement, a nonlocal correlation, is required or whether only local correlation is sufficient, especially as the latter is basically classical in nature. Only recently has the distinction between local and nonlocal entanglement been discussed, and this is crucial in identifying those applications which truly need the QFT.

The authors have enjoyed discussions with S. M. Goodnick, J. P. Bird, K. Hess, and D. Lidar, some of whom take issue with our approach. This work was supported by the Office of Naval Research.

APPENDIX

We begin by considering a simple case of two qubits, which may be defined on a 2×2 tensor-product Hilbert space. As mentioned above, we could also use a 4×1 Hilbert space, but only the former will show entanglement. In this sense, a typical entangled state may be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right) = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right). \quad (1)$$

This is an entangled state since it cannot be decomposed into the product of two pure states, one of which is in each of the separate Hilbert spaces. Let us assume that we can define an operator E on the 2×2 composite Hilbert space of a two-bit system, such that it measures entanglement. Measuring entanglement ought to produce the following type of results on a pure density matrix (i.e., that of the form $\rho = |\psi\rangle\langle\psi|$)

$$\langle E\rangle = Tr(E\rho) = \langle\psi|E|\psi\rangle = \begin{cases} = 0, \text{ if } |\psi\rangle \text{ non-entangled} \\ \neq 0, \text{ if } |\psi\rangle \text{ entangled} \end{cases} \tag{2}$$

For the rest of the proof, E only has to be normal (i.e., commute with its adjoint, so that it would have an eigenbasis), but if it is to be an observable, it actually has to be Hermitian.

We begin from the non-entangled basis $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$. Since E can be diagonalized, there exists a unitary matrix U which will transform the representation matrix of E to its eigenbasis, in which it will be diagonal

$$UEU^{+} = E_{diag}\,. \tag{3}$$

All operators which have the same eigenbasis will commute with E. So, operators of the form

$$L = U^{+}L_{diag}U\,, \tag{4}$$

where for L_{diag} we can choose any diagonal matrix with real coefficients, will commute with E. Every such L generates a one-parameter group of rotations

$$U_L(\varphi) = \exp(iL\varphi)\,, \tag{5}$$

and such rotations leave E invariant, i.e.,

$$[L,E] = 0\,,\quad U_L(\varphi)EU_L^{+}(\varphi) = E\,. \tag{6}$$

Lemma: For a given operator E, it is always possible to find a Hermitian operator L, a parameter φ, and a non-entangled state $|\psi_{n-e}\rangle$, such that L commutes with E, and $U_L(\varphi)|\psi_{n-e}\rangle$ is an entangled state.

Proof: First, let us examine the most general form of a non-entangled state for the two-bit system, with each of the bits having two states. Then, the most general form of a non-entangled state is given by the form

$$\begin{aligned} |\psi_{n-e}\rangle &= (\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_2|0\rangle + \beta_2|1\rangle) \\ &= \underbrace{\alpha_1\alpha_2}_{a}|00\rangle + \underbrace{\alpha_1\beta_2}_{b}|01\rangle + \underbrace{\beta_1\alpha_2}_{c}|10\rangle + \underbrace{\beta_1\beta_2}_{d}|11\rangle\,. \end{aligned} \tag{7}$$

We see that a state $|\psi_{n-e}\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ is non-entangled if

$$\frac{a}{c} = \frac{b}{d} \equiv \gamma\,. \tag{8}$$

(Of course, this parametrization is not the only one, and with this one we must be cautious when c and d vanish, but, since these constraints are not of major impact, we will not go into more details of the structure. Our entangled state (1) does not meet the requirement of (8), since $a = d = 0$.) Thus, according to (7) and (8), a non-entangled state can be represented, in the non-correlated basis $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ by the column

$$|\psi_{n-e}\rangle = \begin{pmatrix} \gamma c \\ \gamma d \\ c \\ d \end{pmatrix}. \tag{9}$$

Let us see what the most general form of an operator should be, in order for it to map all non-entangled states into only non-entangled states.

$$\begin{pmatrix} \gamma' c' \\ \gamma' d' \\ c' \\ d' \end{pmatrix} = \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \begin{pmatrix} \gamma c \\ \gamma d \\ c \\ d \end{pmatrix}, \tag{10}$$

where P,Q,R, and S are 2×2 block-matrices. If we introduce a 2×2 matrix Z which maps $C \equiv (c \quad d)^T$ into $C' \equiv (c' \quad d')^T$, we obtain

$$\begin{bmatrix} \gamma' & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} Z & 0 \\ 0 & Z \end{bmatrix} \begin{bmatrix} C \\ C \end{bmatrix} = \begin{bmatrix} P & Q \\ R & S \end{bmatrix} \begin{bmatrix} \gamma & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} C \\ C \end{bmatrix}, \tag{11}$$

where γ,γ' are scalar 2×2 matrices. So, for the above equation to be valid for all C, we conclude that

$$\begin{bmatrix} P & Q \\ R & S \end{bmatrix} = \begin{bmatrix} \gamma' & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} Z & 0 \\ 0 & Z \end{bmatrix} \begin{bmatrix} \gamma^{-1} & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \gamma(\gamma')^{-1} Z & 0 \\ 0 & Z \end{bmatrix}. \tag{12}$$

Therefore, only matrices of the form

$$M_{(n-e)\to(n-e)} = \begin{bmatrix} \xi Z & 0 \\ 0 & Z \end{bmatrix}, \tag{13}$$

where ξ is a complex number, will map all non-entangled stated into only non-entangled states (the structure of these mappings contains more detail, but for our purpose here, we will be satisfied with (13)). If mapping (13) is to preserve norm, Z obviously must be unitary, and ξ must be a complex number of unit magnitude, i.e.,

$$U_{(n-e)\to(n-e)} = \begin{bmatrix} e^{i\phi} U_{2\times 2} & 0 \\ 0 & U_{2\times 2} \end{bmatrix}. \tag{14}$$

For a given operator E (not necessarily the entanglement operator, just any normal operator), there may not be any unitary operators $U_L(\varphi)$ of the form (14) with which it commutes, so it is clear that, in this case, there will exist some non-entangled states which will be mapped into entangled states, which agrees with the statement of the Lemma. On the other hand, if there are operators of the form (13) that commute with E, then E can be diagonalized by a unitary transformation of the block form

$$U = \begin{bmatrix} U_E & 0 \\ 0 & U_E \end{bmatrix}, \quad UEU^{+} = E_{diag}. \tag{15}$$

However, if we choose $L_{diag} = diag(l_1, l_2, l_3, l_4)$, such that all diagonal elements are real and different, and we choose φ so that $\exp[i(l_1 - l_3)\varphi] \neq \exp[i(l_2 - l_4)\varphi]$, then

$$\begin{aligned} U_L(\varphi) &= \begin{bmatrix} U_E^{+} & 0 \\ 0 & U_E^{+} \end{bmatrix} \exp\left(iL_{diag}\,\varphi\right) \begin{bmatrix} U_E & 0 \\ 0 & U_E \end{bmatrix} \\ &= \begin{bmatrix} U_E^{+} \begin{bmatrix} e^{il_1\varphi} & 0 \\ 0 & e^{il_2\varphi} \end{bmatrix} U_E & 0 \\ 0 & \underbrace{U_E^{+} \begin{bmatrix} e^{il_3\varphi} & 0 \\ 0 & e^{il_4\varphi} \end{bmatrix} U_E}_{U_{2\times 2}} \end{bmatrix} \\ &= \begin{bmatrix} e^{i(l_1 - l_3)\varphi} U_{2\times 2} & 0 \\ 0 & U_{2\times 2} \end{bmatrix} + \begin{bmatrix} X & 0 \\ 0 & 0 \end{bmatrix}, \end{aligned} \tag{16}$$

where

$$X = \left\{ e^{il_2\varphi} - e^{i(l_1 + l_4 - l_3)\varphi} \right\} U_E^{+} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} U_E. \tag{17}$$

Apparently, due to the form $U_L(\varphi)$ in (16), in this case, as well, there will exist some non-entangled states that will be mapped by $U_L(\varphi)$ into an entangled state, which concludes the proof of the Lemma.

Let us choose one such non-entangled and normalized state, $|\psi_{n-e}\rangle$, and the mapping $U_L(\varphi)$ that commutes with the entanglement operator E, and which maps $|\psi_{n-e}\rangle$ into an entangled state $|\psi_e\rangle$. Now, we wish to evaluate $\langle E\rangle$ in the state $|\psi_{n-e}\rangle$, and we obtain

$$\langle E\rangle = Tr\left(E|\psi_{n-e}\rangle\langle\psi_{n-e}|\right) = 0, \tag{18}$$

according to the definition (2). On the other hand

$$
\begin{aligned}
\langle E \rangle &= \mathrm{Tr}\left(E|\psi_{n-e}\rangle\langle\psi_{n-e}|\right) = \mathrm{Tr}\left(\underbrace{U_L^+(\varphi)U_L(\varphi)}_{1} E \underbrace{U_L^+(\varphi)U_L(\varphi)}_{1}|\psi_{n-e}\rangle\langle\psi_{n-e}|\right) \\
&= \mathrm{Tr}\left(\underbrace{U_L(\varphi)EU_L^+(\varphi)}_{E,\ \text{after (6)}} U_L(\varphi)|\psi_{n-e}\rangle\langle\psi_{n-e}|U_L^+(\varphi)\right) \\
&= \mathrm{Tr}\left\{E\underbrace{\left[U_L(\varphi)|\psi_{n-e}\rangle\right]}_{|\psi_e\rangle}\underbrace{\left[\langle\psi_{n-e}|U_L^+(\varphi)\right]}_{\langle\psi_e|}\right\} \\
&= \mathrm{Tr}\left\{E|\psi_e\rangle\langle\psi_e|\right\} \neq 0 .
\end{aligned}
\tag{19}
$$

Apparently, (18) and (19) are in contradiction, *which means that the entanglement operator E, whose action would be given by (2), cannot exist.* That is, there is no operator which can yield a measure of the entanglement as its expectation value, and this completes the proof.

REFERENCES

1 A. Steane, "Quantum Computing," Rep. Prog. Phys. **61**, 117-173 (1998).

2 P. Benioff, "Quantum mechanical Hamiltonian models of Turing machines that dissipate no energy," Phys. Rev. Lett. **48**, 1581-1585 (1982).

3 P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proc. 35th Ann. Symposium on Foundations of Computational Science*, Ed. by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994) 124-134.

4 Y. S. Weinstein, M. A. Pravia, E. M. Fortunato, S. Lloyd, and D. G. Cory, "Implementation of the Quantum Fourier Transform," Phys. Rev. Lett. **86**, 1889-1991 (2001).

5 R. Akis and D. K. Ferry, "Quantum waveguide array generator for performing Fourier transforms: Alternate route to quantum computing," Appl. Phys. Lett. **79**, 2823-2825 (2001).

6 D. K. Ferry, R. Akis, and J. Harris, "Quantum wave processing," Superlatt. Microstruc. **30**, 81-94 (2001).

7 Many of these questions have been posed to the authors by D. Lidar, *private communication*.

8 J. Wiedmann, *Linear Operators in Hilbert Spaces* (Springer-Verlag, New York, 1980).

9 R. Akis, D. K. Ferry, and J. P. Bird, "Magnetotransport fluctuations in semiconductor ballistic quantum dots," Phys. Rev. B 54, 17705-17715 (1995).

10 A. Bertoni, P. Bordone, R. Brunetti, C. Jacoboni, and S. Reggiani, "Quantum Logic Gates based on Coherent Electron Transport in Quantum Wires," Phys. Rev. Lett. **84**, 5912-5915 (2000).

11 J. Harris, R. Akis, and D. K. Ferry, "Magnetically switched quantum waveguide qubit," Appl. Phys. Lett. **79**, 2214-2216 (2001).

12 M. J. Gilbert, R. Akis, and D. K. Ferry, "Magnetically and electrically tunable semiconductor quantum waveguide invertor," Appl. Phys. Lett. **81**, 4284-4286 (2002).

13 A. Bertoni, R. Ionicioiu, P. Zanardi, F. Rossi, and C. Jacoboni, "Simulation of entangled electronic states in semiconductor quantum wires," Physica B **314**, 10-14 (2002).

14 N. J. Cerf, C. Adami, and P. G. Kwiat, "Optical simulation of quantum logic," Phys. Rev. A **57**, R1477-R1480 (1998).

15 R. J. C. Spreeuw, "Classical wave-optics analogy of quantum-information processing," Phys. Rev. A **63**, 06302 (2001).

16 A. Ekert and R. Jozsa, "Quantum computation and Shor's factoring algorithm," Rev. Mod. Phys. **68**, 733-753 (1996).

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

18 N. Pippinger, "On Simultaneous Resource Bounds," *Proc. 20th Annual Symposium on Foundations of Computer Science* (IEEE Comp. Soc., Washington, D. C., 1979) 307.

19 M. Cosnard and D. Trystram, *Parallel Algorithms and Architectures* (Intern. Thomson Comp. Press, London, 1995).

20 P. Chaudhuri, *Parallel Algorithms: Design and Analysis* (Prentice Hall, New York, 1992).

21 A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete," Phys. Rev. **47**, 777-780 (1935).

22 D. Bohm, *Quantum Theory* (Prentice-Hall, Englewood Cliffs, N.J., 1951) pp. 611-23.

23 E. Schrödinger, "Discussion of Probability Relations between Separated Systems," *Proc. Camb. Phil. Soc.* **31,** 555 (1935).

24 V. Vedral, M. B. Plenio, M. A. Rippen, and P. L. Knight, "Quantifying Entanglement," Phys. Rev. Lett. **78,** 2275-2279 (1997).

25 S. Popescu and D. Rohrlich, "Thermodynamics and the measure of entanglement," Phys. Rev. A **56,** R3319-R3321 (1997).

26 M. Horodecki, P. Horodecki, and R. Horodecki, "Limits for Entanglement Measures," Phys. Rev. Lett. **84,** 2014-2017 (2000).

[27] A. Eckert and R. Jozsa, "Quantum algorithms: entanglement-enhanced information processing," Phil. Trans. Roy. Soc. Lond. A **356,** 1769-1782 (1998).
[28] E. Merzbacher, *Quantum Mechanics*, 2nd Ed. (Wiley, New York, 1970).
[29] D. Bohm, "A suggested interpretation of the quantum theory in terms of 'hidden' variables," Phys. Rev. **85,** 166-193 (1952).
[30] P. Holland, *The Quantum Theory of Motion* (Cambridge U. P., Cambridge, 1993) 106-7.
[31] R. J. C. Spreeuw, "A Classical Analogy of Entanglement," Found. Phys. 28, 361-374 (1998).
[32] R. J. C. Spreeuw, "Classsical wave-optics analogy of quantum-information processing," Phys. Rev. A 63, 062302 (2001).
[33] G. Brassard, R.Cleve, and A. Tapp, "Cost of exactly simulating quantum entanglement with classical communication," Phys. Rev. Lett. **83**, 1874-1877 (1999).
[34] S. Massar, D. Bacon, N. J. Cerf, and R. Cleve, "Classical simulation of quantum entanglement without local hidden variables," Phys. Rev. A 63, 052305 (2001).
[35] T. J. Sejnowski and P. K. Stanton, "Covariance Storage in the Hippocampus," in *An Introduction to Neural and Electronic Networks*, Ed. by S. F. Zornetzer, J. L. Davis, and C. Lau (Academic Press, San Diego, 1990) 365-378.
[36] K. F. Lee and J. E. Thomas, "Experimental Simulation of Two-Particle Entanglement using Classical Fields," Phys. Rev. Lett. **88**, 09702 (2002).
[37] N. Bhattacharya, H. B. van Linden van den Heuvell, and R. J. C. Spreeuw, "Implentation of Quantum Search Algorithm using Classical Optics," Phys. Rev. Lett. **88**, 137901 (2002).
[38] J. S. Bell, "On the Einstein Podolsky Rosen Paradox," Physics **1,** 195-200 (1964).
[39] J. S. Bell, "Locality in quantum mechanics: reply to critics," *Epistem. Lett.*, Nov. 1975, p. 2; reproduced in Bell, J. S., *Speakable and Unspeakable in Quantum Mechanics* (Cambridge U. P., Cambridge, 1993) 63-66.
[40] See, e.g., J. S. Bell, "On the impossible pilot wave," Found. Phys. **12,** 989-990 (1982).
[41] R. F. Werner, "Quantum states with Einstein-Podolsky-Rosen correlation admitting a hidden variable model," Phys. Rev. A **40,** 4277-4281 (1989).
[42] See, e.g., A. Aspect, "Testing Bell's Inequalities," in *Quantum Reflections*, Ed. by J. Ellis and D. Amati (Cambridge University Press, Cambridge, 2000) pp. 69-78, and references therein.
[43] K. Hess and W. Philipp, "A possible loophole in the theorem of Bell," Proc. Nat. Acad. Sci. 98, 14224-14227 (2001).
[44] K. Hess and W. Philipp, "Bell's theorem and the problem of decidability between the views of Einstein and Bohr," Proc. Nat. Acad. Sci. 98, 14228-14233 (2001).