Entangling Operations and Their Implementation Using a Small Amount of Entanglement

J. I. Cirac,[1] W. Dür,[1] B. Kraus,[1] and M. Lewenstein[2]
[1]*Institut für Theoretische Physik, Universität Innsbruck, A-6020 Innsbruck, Austria*
[2]*Institut für Theoretische Physik, Universität Hannover, Hannover, Germany*
(Received 18 July 2000)

We study when a physical operation can produce entanglement between two systems initially disentangled. The formalism we develop allows us to show that one can perform certain nonlocal operations with unit probability by performing local measurement on states that are weakly entangled.

DOI: 10.1103/PhysRevLett.86.544 PACS numbers: 03.67.Hk, 03.65.Ca, 03.65.Ta

Much of the theoretical effort in quantum information theory has been focused so far in characterizing and quantifying the entanglement properties of multiparticles states. The reason for that lies, in part, in the fact that those states offer interesting applications in the fields of computation and communication. In practice, these states are created by some physical action (or operation) involving the interaction between several systems. This suggests that the analysis of these operations with regard to the possibility of creating entanglement may play an important role in quantum information theory. The first steps in this direction have been recently reported [1,2]. There, given a Hamiltonian describing the interactions of two systems, it has been analyzed how to produce entanglement.

In this Letter, we investigate which physical operations acting on two spatially separated systems are capable of producing entanglement. This goal is partly motivated by the recent spectacular experimental progress in the field, where several physical setups have been recognized to produce entangled states [3,4]. Thus, some of the questions we analyze in this paper can be stated as follows: given a machine acting on two systems, can it create entanglement? If so, what kind of entanglement? The basic mathematical tool to answer these questions is the isomorphism introduced by Jamiolkowski [5]. We will extend such an isomorphism to relate physical operations [equivalently, completely positive maps (CPM) $\mathcal{E}$] on two systems and unnormalized states (positive operators E) acting on two other systems. This allows us to reduce the problem of the characterization of physical operations to the one of physical states, which has been extensively studied in recent years.

This relation between physical operations and states has a well-defined physical meaning. In fact, from the isomorphism it follows naturally that given a physical operation $\mathcal{E}$ acting on two separated systems A and B initially disentangled (but entangled locally to some other ancilla systems) we can always obtain the corresponding state E as an outcome. What is even more surprising is that, starting from the state E, we can always perform some local measurements such that for certain outcomes the state of systems A and B changes exactly as if we had applied the corresponding operation $\mathcal{E}$.

This last property will allow us to answer an intriguing question raised in the context of quantum information theory. Let us assume that we have two qubits A and B at different locations and we want to apply some nonlocal operation. This situation raises, for example, in the context of distributed quantum computation [6], where nonlocal operations between different quantum computers are required. So far, it is known that one can use maximally entangled states, local operations, and classical communication (LOCC) to perform that task as follows: we can teleport the state of A to the location of B, perform the operation locally, and then teleport the corresponding state back to A. In this process one has to consume two maximally entangled states (i.e., two ebits) apart from transmitting two classical bits in each direction [7]. However, it is known that for some kind of operations (like the controlled–NOT gate) one can economize the resources, such that only one ebit is consumed [8]. In fact, all the operations that have been studied so far [7–10] require *an integer number of ebits*. We will show here that many operations require *a noninteger number of ebits*. In particular, if the operation can only entangle qubits weakly, the required number is much smaller than one. This automatically implies that many tasks in distributed quantum computation can be performed with a much smaller entanglement than the one required so far.

Let us consider two systems A and B at different locations, whose states are represented by vectors in the Hilbert space $\mathcal{H}_{A,B}$, respectively, both of dimension d. Any physical action on those systems is represented mathematically by a completely positive linear map $\mathcal{E}$ mapping the density operator ρ of those systems onto another positive operator $\mathcal{E}(\rho)$. The map can be written as

$$\mathcal{E}(\rho) = \sum_k O_k \rho O_k^\dagger , \tag{1}$$

where O_k are operators acting on $\mathcal{H}_A \otimes \mathcal{H}_B$. For the sake of generality, we have not imposed that the map preserves the trace of ρ, since we may be interested in physical actions that occur with certain probability [11].

Our first goal is to determine when a given CPM is able to produce entangled states. Thus, we first recall the definition of separable operators. We say that a density operator ρ is separable with respect to systems A and B if it can be written as [12]

$$\rho = \sum_{i=1}^{n} |a_i\rangle_A\langle a_i| \otimes |b_i\rangle_B\langle b_i|, \tag{2}$$

for some integer n, and $|a_i\rangle_A \in \mathcal{H}_A$ and $|b_i\rangle_B \in \mathcal{H}_B$. Otherwise, we say that it is nonseparable (or entangled). Separable positive operators describe states that can be prepared using local operations and classical communication out of product states, i.e., are useless for quantum information tasks that require entanglement. During the last years, much theoretical effort has been devoted to the study of the separability properties of operators [13]. In particular, a necessary condition for separability of a given positive operator ρ is that $\rho^{T_A} \geq 0$ [14,15], where T_A denotes transposition in $\mathcal{H}_A$ in a given orthonormal basis $S_A = \{|k\rangle\}_{k=1}^{d}$. This condition turns out to be sufficient as well when the sum of the dimensions of $\mathcal{H}_{A,B}$ does not exceed five (for example, for two qubits). In higher dimension there are examples of entangled states represented by nonseparable operators whose partial transpose is positive [16].

We can similarly define separable CPM; that is, $\mathcal{E}$ is separable [17] if its action can be expressed in the form

$$\mathcal{E}(\rho) = \sum_{i=1}^{n} (A_i \otimes B_i)\rho(A_i \otimes B_i)^{\dagger}, \tag{3}$$

for some integer n and where A_i and B_i are operators acting on $\mathcal{H}_{A,B}$, respectively. Otherwise, we say that it is nonseparable. Up to a proportionality constant, separable maps are those that can be implemented using local operations and classical communication only [18], i.e., useless for several tasks in quantum information.

From definitions (2) and (3) it follows that, if $\mathcal{E}$ and ρ are separable, then $\mathcal{E}(\rho)$ is also separable. This reflects the fact that by local actions one cannot create entanglement.

Now, let us consider two systems, A and B, spatially separated, each of them composed of two particles ($A_{1,2}$, and $B_{1,2}$). Let us consider a CPM $\mathcal{E}$ acting on systems A_1 and B_1. We are interested in whether this CPM can create "nonlocal" entanglement between the systems A and B [19]. We define the operator $E_{A_1A_2,B_1B_2}$ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ [where now $\mathcal{H}_A = \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ and $\mathcal{H}_B = \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$, and $\dim(\mathcal{H}_{A_i}) = \dim(\mathcal{H}_{B_i}) = d$] as follows:

$$E_{A_1A_2,B_1B_2} = \mathcal{E}(P_{A_1A_2} \otimes P_{B_1B_2}). \tag{4}$$

Here, $P_{A_1A_2} = |\Phi\rangle_{A_1A_2}\langle\Phi|$ with

$$|\Phi\rangle_{A_1A_2} = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle_{A_1} \otimes |i\rangle_{A_2}, \tag{5}$$

and $S = \{|i\rangle\}_{i=1}^{d}$ an orthonormal basis. In definition (4) the map $\mathcal{E}$ is understood to act as the identity on the operators acting on $\mathcal{H}_{A_2}$ and $\mathcal{H}_{B_2}$. The operator E has a clear interpretation since it is proportional to the density operator resulting from the operation $\mathcal{E}$ on systems A_1 and B_1 when both of them are prepared in a maximally entangled state with two ancillary systems, respectively.

On the other hand, we have

$$\mathcal{E}(\rho_{A_1B_1}) = d^4 \operatorname{tr}_{A_2A_3B_2B_3}(E_{A_1A_2,B_1B_2}\rho_{A_3B_3}P_{A_2A_3}P_{B_2B_3}). \tag{6}$$

This can be proved as follows. First, we can write $d^2 \operatorname{tr}_{A_3B_3}(\rho_{A_3B_3}P_{A_2A_3}P_{B_2B_3}) = \rho_{A_2B_2}^{T}$, where T means transpose in the basis $S_{A_2} \otimes S_{B_2}$. Now, using (4) one can readily show that $\mathcal{E}(\rho_{A_1B_1}) = d^2 \operatorname{tr}_{A_2B_2}(E_{A_1A_2,B_1B_2}\rho_{A_2B_2}^{T})$. Equation (6) has a very simple interpretation. It reflects the fact that, if we have the state $E_{A_1A_2,B_1B_2}$ at our disposal, we can always produce the map $\mathcal{E}$ on any state of systems A_3 and B_3 by performing a joint measurement locally such that both systems A_2A_3 and B_2B_3 are projected onto the maximally entangled state (5). Of course, this will happen with certain probability. Below we will show how to implement CPM with unit probability using this method.

The relations (4) and (6) induce a one-to-one correspondence between CPM acting on tensor product spaces and positive operators. In fact, this correspondence can be viewed as an extension of the isomorphism introduced by Jamiolkowski [5] to tensor product spaces. Using these relations it is very easy to show the following: (i) $\mathcal{E}$ is separable iff $E_{A_1A_2,B_1B_2}$ is separable with respect to the systems (A_1A_2) and (B_1B_2). Thus, we can study the separability of CPM by studying the problem of separability of positive operators. This immediately implies that we can use all the results derived for the latter problem [13]. (ii) $\mathcal{E}$ can create nonlocal entanglement between A and B iff $E_{A_1A_2,B_1B_2}$ is nonseparable with respect to the systems (A_1A_2) and (B_1B_2). In particular, we can always obtain a state whose density operator is proportional to $E_{A_1A_2,B_1B_1}$ out of separable states by entangling our systems locally with ancillas [20]. (iii) Let us assume that $E_{A_1A_2,B_1B_2}^{T_{A_1A_2}} \geq 0$, where $T_{A_1A_2}$ denotes transposition with respect to A_1 and A_2 in the basis S_A. Then, if $\rho^{T_{A_1}} \geq 0$ we have that $\mathcal{E}(\rho_{A_1B_1})^{T_{A_1}} \geq 0$. If additionally $E_{A_1A_2,B_1B_2}$ is entangled (i.e., bound entangled [21]), then we can always produce bound entangled states out of nonentangled states by using the map $\mathcal{E}$ (see ii). (iv) If $\mathcal{E}$ corresponds to a unitary action, the corresponding operator has rank one, i.e., it can be written as $E = |\Psi\rangle\langle\Psi|$, where $|\Psi\rangle \in \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$ is a normalized state.

We illustrate some of the above results with some simple examples concerning qubits ($d = 2$). First, let us assume that $E_{A_1A_2,B_1B_2}$ is an entangled state with positive partial transposition. According to (i) the corresponding completely positive map $\mathcal{E}$ is nonseparable and according to (iii) $[\mathcal{E}(\rho)]^{T_{A_1}} \geq 0$ for all ρ separable. But in this case, positive partial transposition is equivalent to separability [14,15], and therefore $\mathcal{E}(\rho)$ is separable for all ρ separable. However, if we allow for input states that are locally entangled with ancillas, the final state will be (bound) entangled according to (ii). As for another example, we consider a family of phase gates of the form

$$U(\alpha_N) \equiv e^{-i\alpha_N \sigma_x^{A_1} \otimes \sigma_x^{B_1}}, \qquad \alpha_N \equiv \pi/2^N, \qquad (7)$$

where the σ's are Pauli operators. These gates are of the same kind as the ones used in the discrete Fourier transform [23]. The corresponding operator $E_{A_1A_2,B_1B_2} = |\psi_{\alpha_N}\rangle\langle\psi_{\alpha_N}|$, where

$$|\psi_{\alpha_N}\rangle = \cos(\alpha_N)\,|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2} - i\sin(\alpha_N)\,|\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}\,, \qquad (8)$$

and $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and $|\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$ are Bell states.

Let us now consider a basis of maximally entangled states of systems A_1A_2 (and B_1B_2) as $|\Phi_i\rangle = \mathbb{1} \otimes U_i|\Phi\rangle$, where U_i are unitary operators and $|\Phi\rangle$ is defined in (5). If we perform a measurement on that basis and obtain $|\Phi_i\rangle_{A_1A_2}$ and $|\Phi_j\rangle_{B_1B_2}$ the state of our systems will be $\mathcal{E}(U_i \otimes U_j \rho_{A_1B_1} U_i^\dagger \otimes U_j^\dagger)$. Thus, we see that as a result of the measurement we either implement the CPM, $\mathcal{E}$, or local operations followed by the CPM. Below, we will show how to use this effect in order to perform arbitrary nonlocal unitary operations by using entangled states. We will restrict ourselves to the case of qubits, but our results can be easily generalized. We will first show how to perform gates of the form (7) with probability 1/2. If we fail, we will show that by using other entangled states and performing more measurements of the same kind, we can make the probability of success equal to one. Then we will show how we can use these results to implement $U(\alpha)$ for arbitrary α. Finally, we will show that any arbitrary unitary operation can be implemented using the method described above.

Let us start considering the gates $U(\alpha_N)$ (7). The amount of entanglement of the corresponding state $|\psi_{\alpha_N}\rangle$ (8) is given by its entropy of entanglement

$$E(\psi_{\alpha_N}) = -x\log_2(x) - (1-x)\log_2(1-x)\,, \qquad (9)$$

where $x = \cos^2(\alpha_N) = \cos^2(\pi/2^N)$. On the one hand, $E(\psi_{\alpha_2}) = 1$, i.e., according to our discussion $U(\pi/4)$ is capable of creating 1 ebit of entanglement. On the other hand, $E(\psi_{\alpha_1}) = 0$, i.e., $U(\pi/2) = -i\sigma_x \otimes \sigma_x$ is a *local* gate. For $N \geq 2$, we have that $E(\psi_{\alpha_N})$ is monotonically decreasing with N. Note that for N sufficiently large, we can regard (7) as an infinitesimal transformation and use the results of Ref. [2] to show that the gate can optimally create an entanglement proportional to α_N. We will show that in that limit $U(\alpha_N)$ can be implemented with unit probability by using an average amount of entanglement also proportional to α_N, assisted by classical communication of approximately 2 bits in both directions.

We want to perform the gate on systems A_3B_3 and obtain the output state in systems A_1B_1. We assume that both systems A_1A_2 and B_1B_2 are in the state $|\psi_{\alpha_N}\rangle$ and we measure systems A_2A_3 and B_2B_3 in the Bell basis $|\Psi_{i_1,i_2}\rangle = \mathbb{1} \otimes \sigma_{i_1,i_2}|\Phi^+\rangle$, where $\sigma_{1,1} = \mathbb{1}, \sigma_{1,2} = \sigma_x, \sigma_{2,1} = \sigma_y$, and $\sigma_{2,2} = \sigma_z$. Note that all outcomes of the measurement are equally probable. If the outcome for A_2A_3 is $|\Psi_{i_1,i_2}\rangle$, we apply σ_{i_1,i_2} to A_1 and proceed analogously with B_2B_3. One can readily see that the resulting operation on A_1B_1 after this procedure will be (i) $U(\alpha_N)$ if $i_1 = j_1$, and (ii) $U(\alpha_N)^\dagger = U(-\alpha_N)$ if $i_1 \neq j_1$. Thus, with probability 1/2 we obtain the desired gate, whereas with probability 1/2 we apply $U(-\alpha_N)$ instead, and so we fail. In order to apply the desired gate with probability one, we proceed as follows. If we fail, we repeat the procedure but with systems A_1A_2 and B_1B_2 prepared in the state $|\psi_{2\alpha_N}\rangle$. With a probability 1/2 we will succeed, and otherwise we will have applied $U(-\alpha_N)^3$ to the original state. We continue in the same vein; that is, in the kth step we use systems A_1A_2 and B_1B_2 in the state $|\psi_{2^{k-1}\alpha_N}\rangle$ so that if we fail altogether we will have applied $U(-\alpha_N)^{2^k-1}$. For $k = N$ we have that $U(-\alpha_N)^{2^N-1} = -U(\alpha_N)$, and therefore even if we fail we will have applied the right gate, so that the procedure ends.

The total average entanglement which is consumed during this procedure is given by

$$\overline{E}[U(\alpha_N)] = \sum_{k=1}^{N}\left(\frac{1}{2}\right)^{k-1} E(\psi_{\alpha_{N-k+1}}) = \alpha_N f_N\,, \qquad (10)$$

where

$$f_N = \frac{1}{\pi}\sum_{k=1}^{N} 2^k E(\psi_{\alpha_k}) < f_\infty = 5.97932\,. \qquad (11)$$

In (10), the weight factor of $p_k = (1/2)^{k-1}$ gives the probability that the kth step has to be performed. Thus, we obtain $\overline{E}[U(\alpha_N)] < \alpha_N f_\infty$. Because of the fact that in each step of this procedure one bit of classical communication in each direction is necessary [24], the average amount of classical communication is given by $2 - (1/2)^{N-2}$ bits.

Although the procedure described above allows one only to implement gates with "binary phases" $\alpha_N = \pi/2^N$, any gate $U(\alpha)$ with arbitrary phase α can be approximated with arbitrarily high accuracy by a sequence of gates of the form $U(\alpha_N)$, consuming on average $\overline{E} \leq f_\infty\alpha$ ebits of entanglement. Furthermore, this procedure allows one to implement any arbitrary two-qubit unitary operation U. We can write any such operation as $U = e^{-iHt} = \lim_{n\to\infty}(\mathbb{1} - iHt/n)^n$, where H is a self-adjoint operator. We can thus apply infinitesimal gates $U_n = (\mathbb{1} - iHt/n)$ sequentially using an extension of the scheme described above. Note that after such an infinitesimal operation we can perform local operations without consuming entanglement. This allows us to restrict the form of the Hamiltonians to those that can be written as

$$H_0 = \sum_{k=x,y,z}^{3} \mu_k \sigma_k^A \otimes \sigma_k^B \equiv \sum_{k=1}^{3} H_k\,. \qquad (12)$$

This can be viewed as follows. First, let us write H in terms of Pauli operators for systems A and B as $H = \vec{\alpha}\cdot\vec{\sigma}^A + \vec{\beta}\cdot\vec{\sigma}^B + \vec{\sigma}^A\cdot\gamma\vec{\sigma}^B$, where γ is a matrix and $\vec{\sigma}$ is the Pauli vector. If we apply an infinitesimal local transformation in A and B with Hamiltonians $-\vec{\alpha} \cdot \vec{\sigma}^A$ and $-\vec{\beta} \cdot \vec{\sigma}^B$, respectively, this will be equivalent to having H with $\alpha = \beta = 0$. Moreover, prior to this operation and after the application of U_n we can always perform local operations such that we obtain an evolution given by H_0 (12), where the μ's are the singular values of γ. Since the H_k commute, we have that the corresponding unitary operation is given by

$$\tilde{U}_n = e^{-iH_1 t/n} e^{-iH_2 t/n} e^{-iH_3 t/n}, \tag{13}$$

a sequence of operations of the form (7), for which we already have provided a protocol. The required amount of entanglement is therefore given by $\overline{E}_U = f_\infty t(\mu_1 + \mu_2 + \mu_3)$ ebits.

Using the results of Ref. [2], one can compare for small α_N (large N) the average amount of entanglement used up to implement the gate (7) with the maximal amount of entanglement which can be produced with the help of a single application of the gate [25]. One finds that for $\alpha_N \to 0$, that the ratio $\overline{E}[U(\alpha_N)]/E_{\text{create}}[U(\alpha_N)]$ is given by ≈ 3.1268.

As an aside, let us mention that we have restricted ourselves here to the implementation of nonlocal unitary operations. In fact, with the formalism introduced here one can extend the analysis to nonunitary operations and even to the implementation of nonlocal measurements. All these results indicate that the entanglement properties of a physical operation $\mathcal{E}$ are directly related to the entanglement of the corresponding operator E.

In summary, we have shown that the problem of separability of nonlocal actions can be connected to the one for states via an isomorphism. The methods introduced here also allow to show how one can implement certain nonlocal operations if one shares a small amount of entanglement and is allowed to perform local operations and classical communication. These local operations require, in principle, Bell measurement between the two particles in one location which may be difficult in practice. However, in experiments one can substitute these pairs of particles by a single one with more levels [19], which implies that only single particle operations are needed. Note that those measurements can then be easily performed with ions or atoms [4]. On the other hand, since with photons it is possible both to create entangled states and to perform Bell measurements (with certain probability) [26] our method allows us to perform probabilistic nonlocal gates between photons without having to use controlled nonlinear interactions [27].

This work was supported by the Austrian SF, the DFG, the European Community under the TMR network ERB-FMRX-CT96-0087 and project EQUIP (Contract No. IST-1999-11053), the ESF, and the Institute for Quantum Information GmbH.

[1] P. Zanardi, C. Zalka, and L. Faoro, quant-ph/0005031.
[2] W. Dür *et al.,* quant-ph/0006034.
[3] Special issue, edited by S. Braunstein and Hoi-Kwang Lo [Fortschr. Phys. **48**, Nos. 9–11 (2000)].
[4] C. A. Sackett *et al.,* Nature (London) **404**, 256–259 (2000); A. Rauschenbeutel *et al.,* Science **288**, 2024–2028 (2000).
[5] A. Jamiolkowski, Rep. Math. Phys. **3**, 275–278 (1972).
[6] J. I. Cirac *et al.,* Phys. Rev. A **59**, 4249 (1999).
[7] A. Chefles, C. R. Gilson, and S. M. Barnett, quant-ph/0003062; quant-ph/0006106.
[8] D. Gottesman, quant-ph/9807006.
[9] J. Eisert *et al.,* quant-ph/0005101.
[10] D. Collins, N. Linden, and S. Popescu, quant-ph/0005102.
[11] B. Schumacher and M. Nielsen, Phys. Rev. A **54**, 2629 (1996).
[12] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[13] M. Lewenstein *et al.,* quant-ph/0006064.
[14] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[15] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 8 (1996).
[16] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[17] E. M. Rains, quant-ph/9707002.
[18] Note that this does not contradict the statement given in Ref. [22], in which it is shown that there are certain trace preserving separable completely positive maps that cannot be implemented locally with probability one.
[19] Note that we can always take instead of two particles $A_{1,2}$ a single one with more levels. This is why we are interested in what we call nonlocal entanglement between systems A and B, rather than intrinsic or local entanglement between $A_{1,2}$.
[20] Note that operator E associated to operations like the swap is entangled, although such operator acting on two particles A_1 and B_1 cannot create nonlocal entanglement. However, this is not in contradiction with this statement since, if we allow such particles to be locally entangled with some other two $A_2$and B_2, respectively, the swap operation can indeed produce nonlocal entangled states.
[21] Bound entangled states are nonseparable states that cannot be distilled to maximally entangled states [16].
[22] C. H. Bennett *et al.,* Phys. Rev. A **59**, 1070 (1999).
[23] R. Jozsa, quant-ph/9707033.
[24] In practice, only $(N - 2)$ steps have to be performed, as it happens that the required operation in step $(N - 1)$, $U(\pi/2)$, is a local operation which can be performed with certainty and without classical communication.
[25] As shown in [2], in the limit $\alpha_N \to 0$, the maximal amount of created entanglement is given by $E_{\text{create}}[U(\alpha_N)] = 1.9123\alpha_N$.
[26] D. Bouwmeester *et al.,* Nature (London) **390**, 575 (1997); D. Boschi *et al.,* Phys. Rev. Lett. **80**, 1121 (1998).
[27] W. Dür *et al.* (to be published).