Optimal entanglement generation from quantum operations

M. S. Leifer,* L. Henderson, and N. Linden
Department of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW, United Kingdom
(Received 14 May 2002; published 13 January 2003)

We consider how much entanglement can be produced by a nonlocal two-qubit unitary operation, U_{AB}—the *entangling capacity* of U_{AB}. For a single application of U_{AB}, with no ancillas, we find the entangling capacity and show that it generally helps to act with U_{AB} on an entangled state. Allowing ancillas, we present numerical results from which we can conclude, quite generally, that allowing initial entanglement typically increases the optimal capacity in this case as well. Next, we show that allowing collective processing does not increase the entangling capacity if initial entanglement is allowed.

DOI: 10.1103/PhysRevA.67.012306 PACS number(s): 03.67.−a

I. INTRODUCTION

The fundamental resource used in many quantum information protocols, such as cryptography and teleportation, is the entanglement in a quantum state. A major theme of investigation in quantum information theory is the analysis and characterization of entanglement properties of quantum states under local operations and classical communication (LOCC). One issue is how to extract the entanglement in a quantum state. The simplest protocols involve taking a single copy of the quantum state and using LOCC to extract the entanglement [1]. An important realization is that, in general, collective processing (i.e. processing more than one copy of the state at a time) is more efficient than individual-copy processing. Indeed, for mixed states [2], there are examples where no entanglement can be extracted at all if one only has one copy, but collective processing does allow extraction of entanglement. The fact that *asymptotic* collective processing (i.e., processing of infinitely many copies) is necessary for the *reversible* extraction of entanglement is a key building block in the general theory of entanglement [3,4].

The fundamental resource used in quantum control theory and quantum computing is a nonlocal quantum operation, such as an interaction Hamiltonian or a unitary gate. These can be used, along with local actions, to perform the steps of quantum algorithms and to generate entangled states. Conversely, an entangled state and LOCC can be used to apply a nonlocal operation to an arbitrary state, enabling distributed quantum processing.

Just as for quantum states, it is important to find ways of classifying and quantifying the nonlocal properties of operations. There is a multitude of inter-related problems here. Indeed, there seems to be an even richer structure in the case of quantum operations than there is for states. For example, one can consider how much entanglement an operation can generate, how much classical communication the operation can perform, or the power of the operation to simulate other operations. As with states, we may restrict ourselves to a single application of an operation or we may process multiple copies collectively.

This area has attracted much interest recently and results have been obtained on Hamiltonian simulation [5–17], interconversion of unitary operations [18,19], entanglement generation [20–23], and generating operations from entangled states [24–26]. Most of these results have focused on protocols involving a single application of the operation and little is known about the multiple-copy and asymptotic cases.

In this paper, we focus on the problem of entanglement generation for two-qubit unitary operations acting on pure states. Suppose that Alice and Bob share a state $|\psi\rangle$ in their combined Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ and that they are able to implement an operation $U_{AB} \in U(4)$ on any nonlocal two-qubit subspace. They would like to maximize the amount of entanglement that they generate per application of U_{AB}. We call this maximum the entangling capacity $\mathcal{EC}_E$ of U_{AB}. For single applications of U_{AB}, the entangling capacity is given by

$$\mathcal{EC}_E(U_{AB}) = \max_{|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B} [E(U_{AB}|\psi\rangle) - E(|\psi\rangle)], \quad (1)$$

where E is an entanglement measure and U_{AB} acts on one qubit in $\mathcal{H}_A$ and one in $\mathcal{H}_B$.

In Sec. II, we review the useful decomposition of two-qubit unitaries which was introduced in Refs. [6,21]. Section III of the paper concerns the single-copy entangling capacity. In Sec. III A, we review an argument due to Refs. [27,28] that shows that the single-copy entangling capacity can be achieved when U_{AB} is only allowed to act on pure states. We then extend this argument to show that pure states can still be used if the entangling capacity is to be achieved using the minimal amount of initial entanglement. In Sec. III B and Sec. III C, we show how much entanglement can be created by a single use of a quantum operation when we allow Alice and Bob to share initial entanglement; this work extends Ref. [21] where the authors considered entangling capacities of unitaries but did not allow initial entanglement; it also extends Ref. [20], which allowed initial entanglement but only unitary transformations infinitesimally close to the identity (i.e., Hamiltonians). In the case where ancillas are not allowed (Sec. III B), we are able to derive analytic results about the entangling capacities of unitaries. We find that it generally helps to start with an entangled state, although this is dependent on the entanglement measure. Section III C concerns the case where we allow ancillas; we mostly describe numerical results here, however these numerical re-

*Email address: Matt.Leifer@bristol.ac.uk

sults allow us to conclude, quite generally, that allowing initial entanglement can increase the entangling capacity even when ancillas are available.

The final part of this paper (Sec. IV) concerns collective processing of quantum operations. As described above, collective processing is a key idea in understanding entanglement properties of quantum states. Our main result, essentially that collective processing of quantum operations does not help in generating quantum entanglement, is in stark contrast to the situation for processing of quantum states. We conclude with a discussion of the implications of these results for the interconvertibility of quantum operations and the classification of their entanglement properties.

II. DECOMPOSITION OF TWO-QUBIT UNITARY OPERATORS

The entanglement properties of a unitary operation are invariant under local unitary operations applied before or after the operation. This gives a notion of local equivalence of operations

$$U_{AB} \sim U'_{AB} \text{ iff } U'_{AB} = V_A \otimes V_B U_{AB} W_A \otimes W_B, \tag{2}$$

where V_A, V_B, W_A, W_B are local unitaries acting on the systems indicated. In order to simplify our calculations, we make use of the following decomposition of two-qubit unitary operators. Any two-qubit unitary, $U_{AB} \sim U_d$; where

$$U_d = \exp\left(i \sum_{j=1}^{3} \alpha_j \sigma_j^A \otimes \sigma_j^B \right), \tag{3}$$

$\pi/4 \geqslant \alpha_1 \geqslant \alpha_2 \geqslant |\alpha_3| \geqslant 0$ and $\sigma_{1,2,3}$ are the Pauli matrices. Since U_d has the same entangling capacity as U, we always work with this form [31]. Note that the eigenvalues of U_d are given by $e^{i\lambda_j}$, where

$$\begin{aligned} \lambda_1 &= -\alpha_1 + \alpha_2 + \alpha_3, \\ \lambda_2 &= +\alpha_1 - \alpha_2 + \alpha_3, \\ \lambda_3 &= +\alpha_1 + \alpha_2 - \alpha_3, \\ \lambda_4 &= -\alpha_1 - \alpha_2 - \alpha_3. \end{aligned} \tag{4}$$

The corresponding eigenbasis is given by $U_d|\Phi_j\rangle = e^{i\lambda_j}|\Phi_j\rangle$ which is the Bell basis. For later convenience, we choose the following phase convention:

$$\begin{aligned} |\Phi_1\rangle &= \frac{-i}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\Phi_2\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ |\Phi_3\rangle &= \frac{-i}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\Phi_4\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{5}$$

In Ref. [21], an explicit method is given for calculating α_j, V_A, V_B, W_A, and W_B for any unitary. However, since we are only interested in the values α_j, the following method can be used.

First, we define

$$\tilde{U} = \sigma_2 \otimes \sigma_2 U^T \sigma_2 \otimes \sigma_2, \tag{6}$$

where T indicates the transpose in the computational basis. The eigenvalues of $\tilde{U}U$ are local invariants of U, equivalent to those found in Ref. [29]. From, Eq. (3) one can see that these invariants are in fact squares of the eigenvalues of U_d. Thus, solving Eq. (4) gives the unique decomposition.

III. SINGLE-COPY ENTANGLING CAPACITY

A. Purity of states in the optimal protocol

In this section we determine whether optimal protocols can be found for generating entanglement using one application of U_{AB}, which only involve pure states at every stage. We use an argument of Refs. [27,28] to establish that this is the case. Further, we extend this argument to show that optimal pure state protocols can be found, which start with the minimum possible amount of initial entanglement. Thus, all the important details of the single-copy entangling capacity of U_{AB} can be established by considering pure states only.

Making a suitable definition of the entangling capacity over mixed states is not quite as straightforward as the pure state case. In particular, the choice of entanglement measure for the initial and final states may be different. For the initial state, it seems natural to use a measure of the minimum average amount of entanglement required to generate it (i.e., the entanglement of formation). However, for the final state it makes more sense to measure the maximum amount of entanglement that can be extracted from it (i.e., the distillable entanglement).

To make this more specific, consider an initial mixed state ρ_0. Let $\rho_0 = \Sigma_j p_j |\psi_j\rangle\langle\psi_j|$ be the decomposition of ρ_0 with minimal ensemble-average entanglement. To generate an ensemble of n states described by ρ_0, we may prepare $|\psi_j\rangle$ with probability p_j and then discard the information about which state was prepared. As $n \to \infty$, the amount of entanglement per state used in this procedure will be $E_f(\rho_0)$, where E_f is the entanglement of formation. The operation U_{AB} can then be applied to each state individually, yielding n copies of the state $\rho_1 = U_{AB}\rho_0 U_{AB}^\dagger$. These states can then be distilled to singlets by LOCC, and as $n \to \infty$ the yield of singlets per copy of ρ_1 will be $D(\rho_1)$, where D is the distillable entanglement. Note that, although this protocol involves collective processing of the states, the fact that U_{AB} is applied to each copy of ρ_0 individually means that it can still be re-

garded as a single-copy protocol with respect to the nonlocal operation.

With this in mind, we define the mixed state single-copy entangling capacity as

$$C_E^{mixed} = \max_{\rho_0}[D(\rho_1) - E_f(\rho_0)]. \tag{7}$$

Then

$$D(\rho_1) - E_f(\rho_0) \leqslant E_f(\rho_1) - E_f(\rho_0) \leqslant \sum_j p_j [E_f(U_{AB}|\psi_j\rangle \times \langle\psi_j|U_{AB}^\dagger) - E_f(|\psi_j\rangle\langle\psi_j|)] \tag{8}$$

$$\leqslant \max_{\psi_j}[E_f(U_{AB}|\psi_j\rangle) - E_f(|\psi_j\rangle)]. \tag{9}$$

This demonstrates that, for every mixed state, there is a pure state for which the action of U_{AB} generates at least as much entanglement.

Next we show that any mixed state that achieves the entangling capacity cannot be formed using less entanglement than there is in a pure state that achieves the entangling capacity with minimal initial entanglement. Let $|\psi\rangle$ be a pure state that achieves the entangling capacity with the minimal possible initial entanglement. Let ρ be a mixed state that also achieves the entangling capacity. From Eqs. (8) and (9) it is clear that the optimal decomposition of ρ must be a mixture of pure states that achieve the entangling capacity. Since this is the optimal decomposition of ρ, $E_f(\rho)$ is just the weighted average of the entanglements of these pure states. Thus, $E_f(\rho) \geqslant E_f(|\psi\rangle)$ because $|\psi\rangle$ has the minimal entanglement of any possible state in this ensemble.

B. Single application with no ancillas

We now determine the entangling capacity of two-qubit unitaries of the form of Eq. (3) when no ancillas are allowed. This depends on the entanglement measure we choose to optimize over. In Sec. III B 1 we optimize over the square of concurrence and then in Sec. III B 2 we show how our results can be extended to other measures of entanglement.

1. Square of concurrence

One entanglement measure that is particularly convenient to optimize is the square of the concurrence [30], C, defined by

$$C(|\psi\rangle) = |\langle\psi|\sigma_2 \otimes \sigma_2|\psi^*\rangle|, \tag{10}$$

where $|\psi^*\rangle$ is the state vector obtained by taking the complex conjugates of the components of $|\psi\rangle$ in the computational basis. We can adapt an argument from Ref. [21] to perform the optimization here.

Writing $|\psi\rangle = \Sigma_j b_j |\Phi_j\rangle$ gives

$$\Delta C^2 = C_f^2 - C_0^2 = \left|\sum_j e^{2i\lambda_j} b_j^2\right|^2 - \left|\sum_j b_j^2\right|^2 = \sum_{j,k} (e^{2i(\lambda_j - \lambda_k)} - 1) b_j^2 b_k^{*2}, \tag{11}$$

where C_0 is the initial concurrence and C_f is the final concurrence after applying U_{AB}.

This can be optimized by imposing the normalization condition $\Sigma_j |b_j|^2 = 1$ with a Lagrange multiplier, 2μ, i.e., we maximize

$$L = \sum_{j,k} (e^{2i(\lambda_j - \lambda_k)} - 1) b_j^2 b_k^{*2} - 2\mu\left(\sum_j b_j b_j^* - 1\right). \tag{12}$$

Differentiating gives

$$\frac{\partial L}{\partial b_j} = 2 b_j e^{2i\lambda_j} \sum_k e^{-2i\lambda_k} b_k^{*2} - 2 b_j \sum_k b_k^{*2} - 2\mu b_j^* = 0; \tag{13}$$

multiplying by b_j and summing over j gives

$$\sum_{j,k} (e^{2i(\lambda_j - \lambda_k)} - 1) b_j^2 b_k^{*2} - \mu \sum_j |b_j|^2 = 0, \tag{14}$$

which yields

$$\mu = C_f^2 - C_0^2. \tag{15}$$

Substituting Eqs. (15) and (11) into Eq. (13) gives

$$b_j e^{2i\lambda_j} e^{2i\eta} C_f - b_j e^{2i\epsilon} C_0 - C_f^2 b_j^* + C_0^2 b_j^* = 0, \tag{16}$$

where ϵ, η are phases depending on all of the b_j's. One possible solution is $b_j = 0$. To find the other solutions we write $b_j = \beta_j e^{i\gamma_j}$ where $\beta_j, \gamma_j \in \mathbb{R}$. These solutions must have $\beta_j \neq 0$ and so Eq. (16) reduces to

$$C_f^2 - e^{2i(\lambda_j + \gamma_j + \eta)} C_f - C_0^2 + e^{2i(\gamma_j + \epsilon)} C_0 = 0. \tag{17}$$

There are as many equations (17) as there are nonzero b_j's. For generic λ_j's, we will show that at most two of these equations can be satisfied simultaneously.

First, consider the case when the optimal starting state has $C_0 = 0$. Then we have

$$C_f(C_f - e^{2i(\lambda_j + \gamma_j + \eta)}) = 0. \tag{18}$$

Since C_f is real and we are looking for the maximum, we must have $C_f = 1$. This shows that it is only best to start in a product state if U_{AB} can generate one *e*-bit of entanglement when no ancillas are present. The conditions for this were found in Ref. [21] to be

$$\alpha_1 + \alpha_2 \geqslant \frac{\pi}{4} \text{ and } \alpha_2 + \alpha_3 \leqslant \frac{\pi}{4}, \tag{19}$$

so here we will focus on the cases where Eq. (19) is violated and the optimal starting state must have nonzero C_0.

Subtracting any two of Eqs. (17) gives

$$\sin(\lambda_j-\lambda_k+\gamma_j-\gamma_k)C_f=e^{i(2\epsilon-2\eta-\lambda_j-\lambda_k)}\sin(\gamma_j-\gamma_k)C_0. \tag{20}$$

This gives consistency conditions for the simultaneous solution of any pair of Eqs. (17). In particular, since C_f and C_0 are both real, we have that

$$2(\epsilon-\eta)-\lambda_j-\lambda_k=n\pi, \quad n\in\mathbb{Z}. \tag{21}$$

For generic λ_j's this condition cannot be satisfied for more than one pair of equations in Eqs. (17). Thus, at most two b_j's can be nonzero [32]. This means that the optimal starting state will always be in a subspace spanned by two of the eigenvectors of U_{AB}. We will choose the two eigenvectors and the coefficients b_j that maximize ΔC^2. Reexpressing Eq. (11) in terms of β_j,γ_j gives

$$\Delta C^2=4\sum_{j<k}\beta_j^2\beta_k^2\{\sin[2(\gamma_j-\gamma_k)+\lambda_j-\lambda_k]\sin(\lambda_k-\lambda_j)\}. \tag{22}$$

Only one term in this sum can be nonzero, and for this term we may choose γ_j,γ_k so that $\Delta C^2=4\beta_j^2\beta_k^2|\sin(\lambda_k-\lambda_j)|$. This is maximized by $\beta_j=\beta_k=1/\sqrt{2}$. Thus the entangling capacity is given by

$$\mathcal{E}C_{C^2}=\max_{j<k}|\sin(\lambda_k-\lambda_j)|. \tag{23}$$

Note that this is greater than the corresponding result of $\max_{j<k}|\sin(\lambda_k-\lambda_j)|^2$ found in Ref. [21] when the starting state is restricted to be a product. This shows that when Eq. (19) is violated, initial entanglement is always required to achieve the optimal capacity when no ancillas are allowed. There are two parameter regions where Eq. (19) does not hold.

(1) $\alpha_1+\alpha_2<\pi/4$, $\alpha_2+\alpha_3<\pi/4$. In this region, the maximum is given by making the $j=3,k=4$ term nonzero. We find that $\mathcal{E}C_{C^2}=\sin[2(\alpha_1+\alpha_2)]$ and the optimal starting state is $|\psi\rangle=(\sin[(\alpha_1+\alpha_2)/2-\pi/8]|01\rangle-i\cos[(\alpha_1+\alpha_2)/2-\pi/8]|10\rangle)$. This gives an optimal initial entanglement of $C_0^2=\frac{1}{2}[1-\sin2(\alpha_1+\alpha_2)]$.

(2) $\alpha_1+\alpha_2>\pi/4$, $\alpha_2+\alpha_3>\pi/4$. In this region, the maximum is given by making the $j=1,k=4$ term nonzero. We find that $\mathcal{E}C_{C^2}=\sin[2(\alpha_2+\alpha_3)]$ and the optimal starting state is $|\psi\rangle=1/\sqrt{2}(|\Phi_1\rangle+e^{i(\pi/4+\alpha_2+\alpha_3)}|\Phi_4\rangle)$.

Note that the entangling capacity is always found to be a function of $\alpha_1+\alpha_2$ or $\alpha_2+\alpha_3$, i.e., a sum of only two of the parameters of the unitary. The value of the third parameter does not affect the entangling capacity at all when no ancillas are allowed.

2. Other entanglement measures

All bipartite entanglement measures, E, are monotonic functions of one another and in particular of the concurrence squared [i.e., $E=E(C^2)$]. Generalizing the strategy of Eqs. (11)–(20) to an arbitrary entanglement measure E by making use of $\partial E/\partial b_j=\partial E/\partial(C^2)\partial(C^2)/\partial b_j$ gives

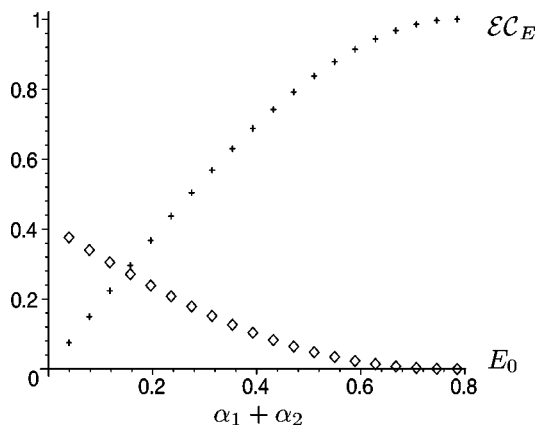

FIG. 1. Single-copy entangling capacity and optimal initial entanglement for a general two-qubit unitary of the form of Eq. (3) when no ancillas are allowed. Crosses show the entangling capacity and diamonds show the minimum initial entanglement of a state that achieves the capacity.

$$\sin(\lambda_j-\lambda_k+\gamma_j-\gamma_k)C_f\frac{dE_f}{d(C_f^2)} =e^{i(2\epsilon-2\eta-\lambda_j-\lambda_k)}\sin(\gamma_j-\gamma_k)C_0\frac{dE}{d(C_0^2)}. \tag{24}$$

This gives the same consistency conditions as Eq. (21) so we still have that at most two b_j's can be nonzero. The only exception is when $dE/d(C^2)\propto 1/C$, which occurs when our entanglement measure is the concurrence itself. In this case, similar methods show that the only consistent solutions are $C_0=0$ and $C_0=1$, meaning that the optimal starting state must always be a product.

For all other entanglement measures we focus on the case where $\alpha_1+\alpha_2<\pi/4,\alpha_2+\alpha_3<\pi/4$. If we choose only b_j and b_k to be nonzero for some choice of $j\neq k=1,2,3,4$, then the resulting optimal ΔE is always a function of the corresponding λ_j and λ_k only. In fact, it must be the same function of λ_j and λ_k for all choices of j and k. For all the measures considered below, we found that the optimal ΔE is always a monotonically increasing function of $|\lambda_j-\lambda_k|$ [33]. As with the square of concurrence, we choose the j and k that give the largest value of $|\lambda_j-\lambda_k|$, namely, $j=3,k=4$. Thus, we can write the optimal starting state in its Schmidt decomposition as

$$|\psi\rangle=\cos(\theta)|01\rangle+e^{i\phi}\sin(\theta)|10\rangle \tag{25}$$

and we simply have to optimize ΔE over the Schmidt parameter θ and relative phase ϕ. We found the following results.

(1) *Concurrence*: $C=|\langle\psi|\sigma_2\otimes\sigma_2|\psi^*\rangle|$. As discussed above, this measure is unusual in that we must always start from a product state. Thus, $\mathcal{E}C_C=\sin[2(\alpha_1+\alpha_2)]$, which coincides with the result of Ref. [21].

(2) *Entropy of entanglement*: $E=-\mathrm{Tr}(\rho^A\log_2\rho^A)$, where ρ^A is Alice's reduced density matrix. We end up with a tran-

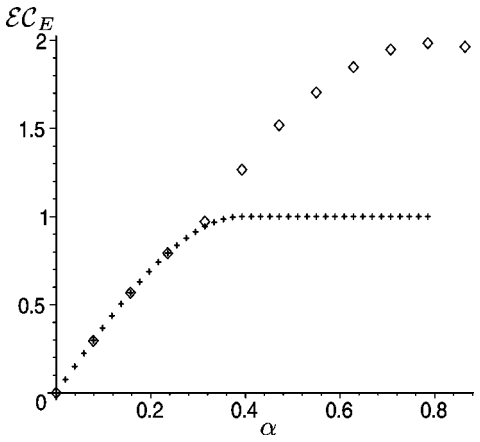

FIG. 2. Single-copy entangling capacity for the DCNOT family. Crosses are for no ancillas and diamonds are for one ancilla on each side.

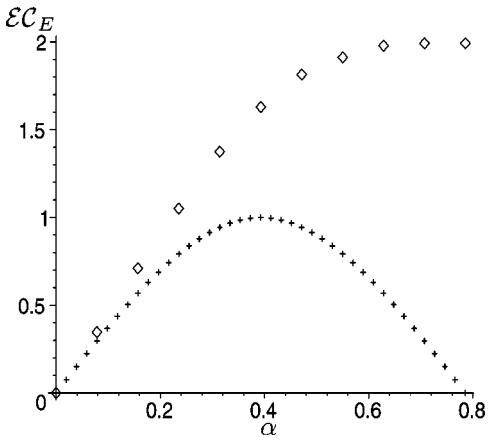

FIG. 3. Single-copy entangling capacity for the SWAP family. Crosses are for no ancillas and diamonds are for one ancilla on each side.

scendental equation in θ, which can be optimized numerically for each $\alpha_1+\alpha_2$. For results see Fig. 1.

(3) *Linearized entropy*: $R=1-\mathrm{Tr}[(\rho^A)^2]$. We find that $\mathcal{EC}_R=\sin[2(\alpha_1+\alpha_2)]$.

C. Ancillas

Next we consider whether adding ancillas can increase the entangling capacity. We have not yet solved this problem analytically; but we present some numerical optimizations, using entropy of entanglement as the measure. Specifically, we use the following definition of entangling capacity when ancillas are present:

$$\mathcal{EC}_E=\max_{|\psi\rangle\in\mathcal{H}_{AA'BB'}}(S\{\mathrm{Tr}_{BB'}[U_{AB}|\psi\rangle\langle\psi|U_{AB}^{\dagger}]\}-S[Tr_{BB'}(|\psi\rangle\langle\psi|)]), \tag{26}$$

where $\mathcal{H}_A$ ($\mathcal{H}_B$) is the Hilbert space of the qubit that Alice (Bob) acts on with U_{AB} and $\mathcal{H}_{A'}$ ($\mathcal{H}_{B'}$) is a finite-dimensional ancillary Hilbert space for Alice (Bob). Only pure states over the Hilbert space $\mathcal{H}_{AA'BB'}=\mathcal{H}_A\otimes\mathcal{H}_{A'}\otimes\mathcal{H}_B\otimes\mathcal{H}_{B'}$ need to be considered because the argument of Sec. III A implies that they are optimal.

Note that, here we are only concerned with the extent to which interaction between Alice and Bob, represented by U_{AB}, can generate entanglement between Alice and Bob. Thus, only the initial and final entanglements between Alice and Bob are relevant and we do not count the entanglement of Alice or Bob with their local ancillas as part of this entanglement.

We chose three different families of operations:

(a) The controlled-NOT(CNOT) family $e^{i\alpha\sigma_1^A\otimes\sigma_1^B}$.

(b) The double CNOT (DCNOT) family $e^{i\alpha(\sigma_1^A\otimes\sigma_1^B+\sigma_2^A\otimes\sigma_2^B)}$.

(c) The SWAP family $e^{i\alpha(\sigma_1^A\otimes\sigma_1^B+\sigma_2^A\otimes\sigma_2^B+\sigma_3^A\otimes\sigma_3^B)}$.

The families are so named because setting $\alpha=\pi/4$ gives operations that are locally equivalent to the CNOT, DCNOT, and SWAP operations.

The simulations were run with both one and two ancillary qubits on each side (i.e., with dimension 2 and 4 for $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$). Adding one ancillary qubit on each side increased the entangling capacity for the DCNOT and SWAP families (see Figs. 2 and 3), but there was no further increase on adding more ancillary qubits. We conjecture that one ancillary qubit on each side is the most general system required to optimize single-copy entangling capacity. Note that, for every α, the SWAP family has a higher entangling capacity than the DCNOT family. This shows that the entangling capacity is generally a function of all three parameters $(\alpha_1,\alpha_2,\alpha_3)$ of the unitary, in contrast to the case considered above where no ancillas are allowed.

For the CNOT family, adding ancillas had no effect at all (see Fig. 4). In Ref. [21], the entangling capacity for the CNOT family starting from a product state with ancillas was found to be $H(\cos^2\alpha)=-\cos^2(\alpha)\log_2[\cos^2(\alpha)]-\sin^2(\alpha)\log_2[\sin^2(\alpha)]$. No ancillas were required to achieve this capacity. Our results exceed this capacity, which demonstrates that allowing initial entanglement can still increase the entangling capacity even if ancillas are present.

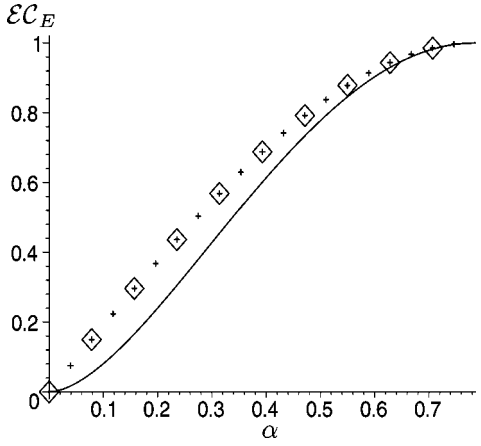

FIG. 4. Single-copy entangling capacity for the CNOT family. Crosses are for no ancillas, diamonds are for one ancilla on each side, and the line shows the equivalent result when the starting state is restricted to be a product between Alice and Bob.

IV. COLLECTIVE PROCESSING

We now turn to the question of whether the entangling capacity is increased by applying n copies of a unitary operation to pairs of qubits in the most general initial state that may be entangled and may contain ancillas. The n-copy entangling capacity is then defined to be the optimal increase in entanglement over Alice and Bob's entire Hilbert space per application of the unitary. In this definition, we again allow Alice and Bob to have arbitrarily large, but finite-dimensional, ancillary Hilbert spaces. We restrict our attention to the case where we have a pure state in the entire Hilbert space at every stage of the protocol, but note that the results also hold for the case where mixed states are allowed [27,28]. In this setting, the unitaries may be applied simultaneously or one after another. Collective LOCC may be performed on all the qubits between applications and each unitary may be applied to arbitrarily chosen pairs of qubits. However, all protocols of this form can be reduced to simpler protocols, which yield the same amount of entanglement.

First, observe that applying unitaries simultaneously is less general than applying them one after the other. Second, because local unitary operations (e.g., local SWAP operations) can be applied as part of the LOCC, all the unitaries can be applied to the same pair of qubits. Thus the problem reduces to a sequence of single-copy problems, where all the qubits that U_{AB} does not act on can be regarded as ancillas. We can do no better than if we have the optimal initial state for a single-copy of U_{AB} available before each application of U_{AB}. Thus, the n-copy entangling capacity can be no greater than the single-copy entangling capacity that can be obtained when ancillas are present. Indeed, this maximum can easily be achieved by acting with U_{AB} on n completely separate copies of the optimal single-copy input state, where each separate state contains the necessary number of ancillas.

If initial entanglement is not available, then collective processing can do better per use of the unitary, since we can make use of the first few copies of the unitary to generate entanglement, which can then be used to make a state with optimal initial entanglement. This can then be used as the starting state for the subsequent copies.

Protocols that start with initial entanglement can outperform protocols that start with product states for all finite n. However, the asymptotic case, where $n\rightarrow\infty$, is more subtle because the operations of entanglement distillation and dilution are available for the states. In the case where we start with product states, we can use some of the first few operations to generate the entanglement required for the optimal initial state. Then we can keep diluting the entanglement of the states at each stage so that we always act on the best initial state. The number of operations required for the first stage of this protocol is fixed and finite, so as $n\rightarrow\infty$ we will achieve the same entangling capacity as if we have started with initial entanglement. This means that asymptotic entangling capacity of a unitary starting with a product state is the same as the capacity that would be obtained starting with initial entanglement.

V. CONCLUSIONS

We have shown that for all finite number of copies of U_{AB}, initial entanglement is required to achieve the optimal entangling capacity. If this initial entanglement and ancillas are available, then collective processing does not help to achieve this maximum.

Our results have implications for the asymptotic interconvertibility of bipartite unitary operations. For example, it is known that the CNOT gate and a singlet state are reversibly interconvertible under LOCC. Thus, one can asymptotically simulate the action of $n\mathcal{E}C_E(U_{AB})$ CNOT gates using n copies of U_{AB} and LOCC by generating entanglement and then distilling or diluting it to singlets. Further, it is impossible to generate more CNOT gates than this, since otherwise one could generate more than $\mathcal{E}C_E(U_{AB})$ e-bits per application of U_{AB} by first converting to CNOT gates and then using them to generate singlet states. More generally, it is not known whether an arbitrary unitary operation is reversibly interconvertible with entangled states under LOCC [i.e., whether one can asymptotically generate n copies of U_{AB} acting on an arbitrary input state given $n\mathcal{E}C_E(U_{AB})$ e-bits]. However, $n\mathcal{E}C_E(U_{AB})$ is a lower bound on how much entanglement is needed to generate n copies of U_{AB}. Also, $\mathcal{E}C_E(U_1)/\mathcal{E}C_E(U_2)$ is an upper bound on how many copies of a bipartite unitary U_2 can be generated asymptotically per application of another bipartite unitary U_1. Whether these bounds can be achieved remains an open question.

ACKNOWLEDGMENTS

We are very grateful to C. H. Bennett, D. Leung, and S. Popescu for many stimulating discussions about nonlocal properties of unitaries and to C. H. Bennett, A. Harrow, D. Leung, and J. Smolin for describing their recent results to us prior to their publication. We gratefully acknowledge funding from the European Union under the project EQUIP (Contract No. IST-1999-11063).

[1] M.A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
[2] N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **81**, 3279 (1998).
[3] C.H. Bennett, H.J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **54**, 4707 (1996).
[4] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, e-print quant-ph/9912039.
[5] C.H. Bennett, J.I. Cirac, M.S. Leifer, D.W. Leung, N. Linden, S. Popescu, and G. Vidal, e-print quant-ph/0107035.
[6] N. Khaneja, R. Brockett, and S.J. Glaser, Phys. Rev. A **63**, 032308 (2001).
[7] J. Dodd, M. Nielsen, M. Bremner, and R. Thew, e-print quant-ph/0106064.
[8] M. Nielsen, M. Bremner, J. Dodd, A. Childs, and C. Dawson, e-print quant-ph/0109064.
[9] P. Wocjan, D. Janzing, and T. Beth, e-print quant-ph/0106077.

[10] D. Janzing, P. Wocjan, and T. Beth, e-print quant-ph/0106085.
[11] P. Wocjan, M. Roetteler, D. Janzing, and T. Beth, e-print quant-ph/0109063.
[12] P. Wocjan, M. Roetteler, D. Janzing, and T. Beth, e-print quant-ph/0109088.
[13] D. Leung, e-print quant-ph/0107041.
[14] H. Chen, e-print quant-ph/0109115.
[15] G. Vidal and J. Cirac, e-print quant-ph/0108076.
[16] G. Vidal and J. Cirac, e-print quant-ph/0108077.
[17] G. Vidal, K. Hammerer, and J. Cirac, e-print quant-ph/0112168.
[18] W. Dür, G. Vidal, and J. Cirac, e-print quant-ph/0112124.
[19] W. Dür and J. Cirac, e-print quant-ph/0201112.
[20] W. Dür, G. Vidal, J. Cirac, N. Linden, and S. Popescu, Phys. Rev. Lett. **87**, 137901 (2001); e-print quant-ph/0006034, Phys. Rev. Lett. (to be published).
[21] B. Kraus and J. Cirac, Phys. Rev. A **63**, 062309 (2001).
[22] P. Zanardi, C. Zalka, and L. Faoro, Phys. Rev. A **62**, 030301 (2000).
[23] P. Zanardi, Phys. Rev. A **63**, 040304(R) (2001).
[24] J. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).
[25] D. Collins, N. Linden, and S. Popescu, Phys. Rev. A **64**, 032302 (2001).
[26] J. Eisert, K.A. Jacobs, P. Papadopoulos, and M.B. Plenio, Phys. Rev. A **62**, 052317 (2000).
[27] D. Leung and C. H. Bennett (private communication).
[28] C.H. Bennett, A. Harrow, D.W. Leung, and J.A. Smolin, e-print quant-ph/0205057.
[29] Y. Makhlin, e-print quant-ph/0002045.
[30] W.K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[31] In fact, when considering the entangling capacity, we can always take $\alpha_3 \geqslant 0$. This is because $\exp(i\Sigma_{j=1}^{2}\alpha_j\sigma_j^A\otimes\sigma_j^B-\alpha_3\sigma_3^A\otimes\sigma_3^B)\sim[\exp(i\Sigma_{j=1}^{3}\alpha_j\sigma_j^A\otimes\sigma_j^B)]^*$ and $\mathcal{E}C_E$ is invariant under conjugation.
[32] This result can be extended to all possible λ_j's by noting that Eq. (20) can only be satisfied for more than one pair if some of the eigenvalues are degenerate. Further, it can be shown that one can choose only one of the corresponding b_j's to be nonzero.
[33] Similarly when $\alpha_1+\alpha_2>\pi/4, \alpha_2+\alpha_3>\pi/4$ we found that, for any choice of j and k, the optimal ΔE is always a monotonically decreasing function of $|\lambda_j-\lambda_k|$.