

Approximate transformations and robust manipulation of bipartite pure-state entanglement

Guifré Vidal,¹ Daniel Jonathan,² and M. A. Nielsen³

¹*Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, Diagonal 647, E-08028 Barcelona, Spain*

²*Optics Section, the Blackett Laboratory, Imperial College, London SW7 2BZ, United Kingdom*

³*Department of Physics, MC 12-33, California Institute of Technology, Pasadena, California 91125*

(Received 26 October 1999; published 12 June 2000)

We analyze *approximate* transformations of pure entangled quantum states by local operations and classical communication, finding explicit conversion strategies which optimize the fidelity of transformation. These results allow us to determine the most faithful teleportation strategy via an initially shared partially entangled pure state. They also show that procedures for entanglement manipulation such as entanglement catalysis [Jonathan and Plenio, Phys. Rev. Lett. **83**, 3566 (1999)] are robust against perturbation of the states involved, and motivate the notion of *nonlocal fidelity*, which quantifies the difference in the entangled properties of two quantum states.

PACS number(s): 03.67.Hk, 03.65.Bz

I. INTRODUCTION

Entanglement is a *resource* at the heart of quantum mechanics; iron in the classical world's bronze age. It is a key ingredient in effects such as quantum computation [1], quantum teleportation [2], and superdense coding [3]. To better understand entanglement as a resource, we would like to understand what transformations of an entangled state may be accomplished, when only some restricted class of operations is allowed to accomplish this transformation. This paradigm, introduced in Refs. [4–6], has been very successful in identifying many of the fundamental properties of entanglement. The best studied class of operations is local operations and classical communication (LOCC)—that is, the two entangled parties may do whatever they wish to their local system, and may communicate classically, but they cannot use quantum communication.

This class of transformations has been studied in considerable detail in Refs. [7–11]. The purpose of this paper is to generalize earlier results to study *approximate* transformations of one pure state into another. In particular, we obtain a scheme for performing the best possible entanglement transformation, in the sense that the transformation results in a state which is “nearest” the desired target state, with respect to a well-motivated measure of distance. Our results show that existing results about entanglement transformation are robust against the effects of slight noise, and quantify exactly how robust. Our results extend and complement recent and independent work by Barnum [12] on approximate transformations with applications to cryptography.

The paper is structured as follows. In Sec. II we review the relevant background material. Section III proves the main result of the paper, an optimal scheme for performing approximate entanglement transformation. Section IV illustrates our main result by application to some concrete entanglement transformation tasks. In particular, we determine the optimal fidelity of any teleportation scheme that uses a partially entangled pure state as its quantum channel. Section V introduces the concept of *nonlocal fidelity* between two entangled states, and studies some elementary properties of

this measure of distance between two entangled states. Section VI concludes the paper.

II. BACKGROUND

Suppose $|\psi\rangle$ is a pure state of a bipartite system shared by Alice and Bob, and let

$$|\psi\rangle = \sum_{i=1}^n \sqrt{\alpha_i} |i_A i_B\rangle, \quad \alpha_i \geq \alpha_{i+1} \geq 0, \quad \sum_{i=1}^n \alpha_i = 1, \quad (1)$$

be its Schmidt decomposition [13]. (Throughout this paper we switch back and forth between the bra-ket notation $|\psi\rangle$ and the notation ψ without comment.) Without loss of generality we may suppose Alice and Bob have state spaces of equal dimension n . All results extend trivially to the case of unequal dimensions. Suppose the parties wish to transform this initial state into a second pure state $|\phi\rangle$ with Schmidt decomposition

$$|\phi\rangle = \sum_{i=1}^n \sqrt{\beta_i} |i'_A i'_B\rangle, \quad \beta_i \geq \beta_{i+1} \geq 0, \quad \sum_{i=1}^n \beta_i = 1, \quad (2)$$

that we shall call the *target* state, by just acting locally on their subsystems and communicating classically.

Necessary and sufficient conditions for this *deterministic* local transformation to be possible, along with an explicit protocol for the conversion, were presented in Ref. [8]. It was shown there that ψ is locally convertible into ϕ in a deterministic manner if and only if the vector $\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$ is *majorized* by the vector $\vec{\beta} = (\beta_1, \dots, \beta_n)$, $\vec{\alpha} < \vec{\beta}$:

$$\psi \rightarrow \phi \Leftrightarrow \sum_{i=1}^k \alpha_i \leq \sum_{i=1}^k \beta_i, \quad k=1, \dots, n, \quad (3)$$

with equality holding when $k=n$. Condition (3) can be given an equivalent description in terms of the *entanglement monotones* E_l , $l=1, \dots, n$, introduced in Ref. [9],

$$E_l^\psi \equiv \sum_{i=1}^n \alpha_i, \quad E_l^\phi \equiv \sum_{i=1}^n \beta_i, \quad (4)$$

which are quantities that do not increase, on average, under any local transformation [14]. The state ψ can be locally transformed into ϕ with certainty if and only if none of these entanglement monotones are increased during the conversion, that is,

$$E_l^\psi \geq E_l^\phi, \quad l=1, \dots, n. \quad (5)$$

We suppose from now on that condition (3) is not satisfied, and that therefore the parties cannot locally convert ψ into ϕ deterministically, that is, $\psi \not\rightarrow \phi$. What options do they have?

In some cases, namely, when ψ has at least as many nonvanishing Schmidt coefficients as ϕ , the parties can still locally transform ψ into ϕ with some nonvanishing probability of success, performing what we shall call a *conclusive* conversion. The optimal *conclusive* protocol is the one with the maximal probability $P(\psi \rightarrow \phi)$ that the conversion is successful. This probability can be shown to be [9]

$$P(\psi \rightarrow \phi) = \min_{l \in [1, n]} \frac{E_l(\psi)}{E_l(\phi)}, \quad (6)$$

and thus it is the greatest quantity compatible with the non-increasing character of the entanglement monotones E_l .

An appealing feature of *conclusive* conversions is that when the protocol succeeds the parties end up sharing exactly the target state ϕ they wanted. This is useful in any situation where Alice and Bob need the target state *exactly* and do not wish to accept a merely *similar* outcome, say another state ξ with a reasonably high overlap with ϕ . One may conceive, for instance, that the parties want to perform fully reliable teleportation [2]. In order to do so they may try to conclusively convert the initial pure state ψ into an m -state [7]—a state of the form

$$|\psi_m\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^m |i_A i_B\rangle. \quad (7)$$

In the present work we consider, on the contrary, that the parties allow for the final outcome ξ of the conversion to be just an approximated version of the target state ϕ . We shall call this alternative type of transformations *faithful* (see Fig. 1). More specifically, we present here faithful conversions $\psi \rightarrow \xi$ such that the fidelity between the final state ξ and the target state ϕ , which we define as

$$F(\xi, \phi) \equiv \langle \xi | \phi \rangle^2, \quad (8)$$

is the greatest locally achievable. (Note that our nomenclature differs from that used, e.g., in Ref. [19], whose definition of “fidelity” corresponds to the square root of ours.)

This *approximate* approach is more suitable than conclusive transformations in a number of contexts. First, it allows us to consider local conversions when the conclusive ones

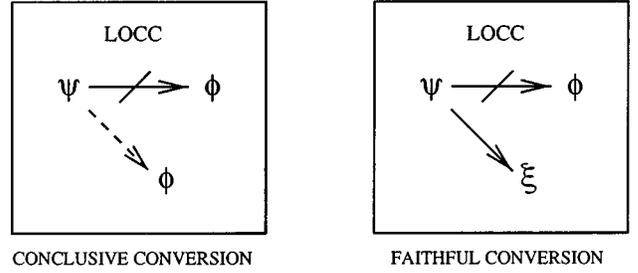


FIG. 1. Suppose local operations on the subsystems and classical communication between Alice and Bob (LOCC) are not sufficient for a *deterministic* conversion of the initial state ψ into their target state ϕ , i.e., $\psi \not\rightarrow \phi$. A *conclusive* local conversion may then do the job with some prior probability of success, i.e., sometimes the protocol will lead to the target state ϕ and sometimes will fail to do so. Alternatively, a *faithful* conversion will deterministically lead to a final state ξ which is only (but often reasonably) similar to the target state ϕ .

are not possible at all. For example, this is the case whenever the target state has more nonvanishing Schmidt coefficients than the initial state [7]. This is relevant to the problem of diluting the entanglement of a finite set of pure, maximally entangled states into a larger set of other pure, partially entangled ones. Such a problem can be well posed from the point of view of faithful conversions, and we will address here the question of which are the optimal (that is, most faithful) dilution protocols for the finite case.

Entanglement distillation—the extraction of pure state entanglement from mixed states—is a second context where faithful conversions are highly relevant. It is known [16] that the conclusive local conversion of N copies of a mixed state ρ into any entangled pure state ϕ is in general impossible, that is the probability of making the transformation $\rho^{\otimes N} \rightarrow \phi$ is typically equal to 0 for any finite N , whereas distillation of pure state entanglement is often possible in the limit $N \rightarrow \infty$ [6]. Thus faithful conversions of mixed states into pure states appear as a more adequate framework for the study of approximate entanglement distillation.

A third reason for interest in faithful transformation protocols is that, as we will show here, in general they differ from the conclusive protocols with the highest probability of success. Finally, the study of approximate conversions allows us to quantify how robust exact transformations are, a problem of direct relevance to applications of entanglement transformation such as entanglement catalysis [17] and certain cryptographic protocols [12,18].

III. OPTIMAL CONVERSIONS BETWEEN PURE STATE ENTANGLEMENT

We consider here the most general local transformations of the initial state ψ , namely, those that convert ψ into an ensemble of possible final states ρ_k with corresponding probabilities p_k (see Fig. 2). In the case of *pure* final states, it has been shown in Ref. [10] that such a *probabilistic* transformation can be performed by local means if, and only if, the entanglement monotones E_l do not increase on average, that is,

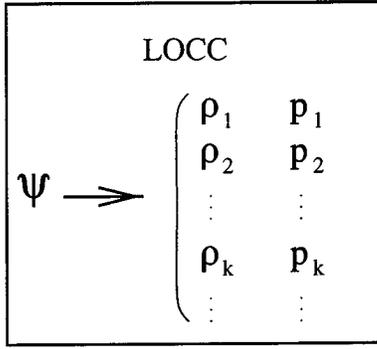


FIG. 2. The most general local transformation a bipartite pure state ψ can undergo may be *probabilistic* in nature, and its outgoing states may be *mixed*. Lemma 1 allows us to restrict our considerations to *deterministic* transformations of ψ into a final *pure* state ξ , when searching for the most *faithful* local conversion into a target state ϕ .

$$\psi \rightarrow \{p_k, \xi_k\} \Leftrightarrow E_l^\psi \geq \sum_k p_k E_l^{\xi_k}, \quad l=1, \dots, n. \quad (9)$$

We can extend this result to the case where the final states may be mixed states ρ_k . Notice that *any* local protocol generating an ensemble $\{p_k, \rho_k\}$ of final mixed states from the pure state ψ can be (nonuniquely) viewed as the outcome of a two-step procedure of the following form: first, an ensemble of pure states $\{p_k q_{k,j}, \xi_{k,j}\}$ such that

$$\rho_k = \sum_j q_{k,j} |\xi_{k,j}\rangle \langle \xi_{k,j}| \quad (10)$$

is locally produced; then the information concerning the index j is discarded. Therefore the transformation $\psi \rightarrow \{p_k, \rho_k\}$ can be performed locally if, and only if, there exists an ensemble $\{p_k q_{k,j}, \xi_{k,j}\}$ satisfying Eq. (10) and such that

$$E_l^\psi \geq \sum_{k,j} p_{k,j} E_l^{\xi_{k,j}}, \quad l=1, \dots, n. \quad (11)$$

We can now proceed to the main results of this work. In lemma 1, we determine the most faithful strategy for converting between pure states when only local unitary transformations are allowed. In lemma 2, we show that among all possible local transformations of the initial pure state ψ , $\psi \rightarrow \{p_k, \rho_k\}$ (see Fig. 2), the maximal average fidelity with respect to the target state ϕ , $\sum_k p_k \langle \phi | \rho_k | \phi \rangle$, can always be obtained in a local and deterministic conversion of the state ψ into a final pure state ξ . These results are then used to prove theorem 3, which provides the value of the optimal fidelity and the identity of the best possible final state ξ , while also constructing an explicit local protocol for the conversion. It is worth noting that the pure state fidelity is equivalent to the ‘‘trace distance,’’ a quantity with a well-defined *operational meaning* as the probability of making an error distinguishing two states [19]. The state ξ is in this sense the best possible physical approximation to the state ϕ that may be achieved using LOCC. We note that results

closely related to lemma 1 and lemma 2 have recently been obtained independently by Barnum [12], however, he does not provide the general solution to the approximation problem, theorem 3.

Lemma 1. Let $\tau, \omega \in \mathcal{C}^n \otimes \mathcal{C}^n$ be two normalized states with ordered Schmidt decompositions in the same local basis, that is,

$$|\tau\rangle = \sum_{i=1}^n \sqrt{\tau_i} |i_A i_B\rangle, \quad \tau_i \geq \tau_{i+1} \geq 0, \quad (12)$$

$$|\omega\rangle = \sum_{i=1}^n \sqrt{\omega_i} |i_A i_B\rangle, \quad \omega_i \geq \omega_{i+1} \geq 0, \quad (13)$$

and let us consider the overlap or fidelity $F_{U,V} \equiv |\langle \tau | \omega_{U,V} \rangle|^2$ between τ and a third vector $\omega_{U,V} \equiv (U \otimes V)\omega$, where U and V are any two local unitaries on Alice’s and Bob’s subsystems, respectively. Then

$$\max_{U \otimes V} F_{U,V} = \left(\sum_{i=1}^n \sqrt{\tau_i \omega_i} \right)^2, \quad (14)$$

the maximal overlap corresponding precisely to the case $U = V = I$, $\omega_{U,V} = \omega$.

Proof. Let us begin by reexpressing τ, ω in the form [20]

$$|\tau\rangle = I \otimes \sigma^\tau |\alpha\rangle; |\omega\rangle = I \otimes \sigma^\omega |\alpha\rangle, \quad (15)$$

where $\sigma^\tau, \sigma^\omega$ are the diagonal $n \times n$ matrices constructed from the ordered Schmidt coefficients of τ, ω (i.e., $\sigma_i^\tau = \sqrt{\tau_i}$) and $\alpha = \sum_{i=1}^n |i_A i_B\rangle$ is the unnormalized maximally entangled state. The overlap between τ and any vector $\omega_{U,V}$ obtained from ω by local unitary rotations is then

$$\begin{aligned} |\langle \tau | U \otimes V | \omega \rangle|^2 &= |\langle \alpha | (U \otimes \sigma^\tau V \sigma^\omega) | \alpha \rangle|^2 \\ &= |\langle \alpha | (I \otimes \sigma^\tau V \sigma^\omega U^T) | \alpha \rangle|^2 \\ &= |\text{Tr}(\sigma^\tau V \sigma^\omega U^T)|^2, \end{aligned} \quad (16)$$

where we have used the easily verified observations that $U \otimes I |\alpha\rangle = I \otimes U^T |\alpha\rangle$ and $\langle \alpha | (I \otimes A) | \alpha \rangle = \text{Tr}[A]$. The desired result follows directly from problem III.6.12 in Ref. [15]. Alternatively, a sketch of the remainder of the proof is as follows. First, rewrite

$$|\text{Tr}(\sigma^\tau V \sigma^\omega U^T)| = |\text{Tr}(\sqrt{\sigma^\tau} V \sqrt{\sigma^\omega} \sqrt{\sigma^\omega} U^T \sqrt{\sigma^\tau})|. \quad (17)$$

By the Cauchy-Schwarz inequality $|\text{Tr}(A^\dagger B)| \leq \sqrt{\text{Tr}(A^\dagger A) \text{Tr}(B^\dagger B)}$, we then have

$$|\text{Tr}(\sigma^\tau V \sigma^\omega U^T)| \leq \sqrt{\text{Tr}(\sigma^\omega V^\dagger \sigma^\tau V) \text{Tr}(\sigma^\tau U^* \sigma^\omega U^T)}. \quad (18)$$

Define $C \equiv V^\dagger \sigma^\tau V$. Since σ^ω is diagonal, we have $\text{Tr}(\sigma^\omega C) = \text{Tr}[\sigma^\omega \text{diag}(C)]$, where $\text{diag}(C)$ is obtained by retaining only the diagonal elements of C . Now, since σ^τ diagonalizes C , Schur’s theorem (Ref. [21], theorem 9.B.1) implies that there exist permutation operators P_i such that

$$\text{diag}(C) = \sum_i p_i P_i \sigma^\tau P_i^\dagger. \quad (19)$$

It follows that

$$\begin{aligned} \text{Tr}(\sigma^\omega C) &= \sum_i p_i \text{Tr}(\sigma^\omega P_i \sigma^\tau P_i^\dagger) \leq \sum_i p_i \text{Tr}(\sigma^\omega \sigma^\tau) \\ &= \text{Tr}(\sigma^\omega \sigma^\tau), \end{aligned} \quad (20)$$

where the inequality follows from the observation that $x_1 \leq x_2$ and $y_1 \leq y_2$ imply that $x_1 y_2 + x_2 y_1 \leq x_1 y_1 + x_2 y_2$, and so $\text{Tr}(\sigma^\omega P_i \sigma^\tau P_i^\dagger) \leq \text{Tr}(\sigma^\omega \sigma^\tau)$. Similarly, $\text{Tr}(\sigma^\tau U^* \sigma^\omega U^T) \leq \text{Tr}(\sigma^\omega \sigma^\tau)$. Substituting these results in Eq. (18) and then into Eq. (16), we finally obtain

$$|\langle \tau | U \otimes V | \omega \rangle|^2 \leq \text{Tr}^2(\sigma^\omega \sigma^\tau) \quad (21)$$

which is precisely the overlap between τ and ω given in Eq. (14).

Lemma 2. Among all possible local transformations of the bipartite pure state ψ , $\psi \rightarrow \{p_k, \rho_k\}$, a deterministic one, $\psi \rightarrow \xi$, into some pure state ξ can always be found which achieves the most faithful transformation with respect to the target state ϕ .

Proof. Because of the linearity of the trace $\text{Tr}[\dots]$, the overlap $\text{Tr}[|\phi\rangle\langle\phi|\rho]$ between ϕ and a mixed state ρ equals the average overlap between ϕ and any ensemble realizing ρ . Therefore we can consider, without loss of generality [compare the discussion around Eq. (10)], just local transformations $\psi \rightarrow \{p_k, \xi_k\}$ into pure states ξ_k , with squared Schmidt coefficients $\gamma_i^k \geq \gamma_{i+1}^k \geq 0$. By lemma 1, the average fidelity \bar{F} with the target state ϕ of Eq. (2) satisfies

$$\bar{F} \leq \sum_k p_k \left(\sum_{i=1}^n \sqrt{\gamma_i^k \beta_i} \right)^2. \quad (22)$$

Moreover, it follows from Eqs. (5) and (9) that the pure state $\bar{\xi}$, defined as

$$|\bar{\xi}\rangle \equiv \sum_{i=1}^n \sqrt{\sum_k p_k \gamma_i^k} |i'_A i'_B\rangle, \quad (23)$$

with the same Schmidt basis as the target state ϕ , can be obtained deterministically from ψ in Eq. (1). The concavity of Uhlmann's fidelity $F(\rho_1, \rho_2) \equiv (\text{Tr} \sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}})^2$ [22] implies that the overlap between $\bar{\xi}$ and the target state ϕ is an upper bound on \bar{F} ,

$$\bar{F} \leq \sum_k p_k \left(\sum_{i=1}^n \sqrt{\gamma_i^k \beta_i} \right)^2 \leq \left(\sum_{i=1}^n \sqrt{\sum_k p_k \gamma_i^k \beta_i} \right)^2. \quad (24)$$

More precisely, define diagonal $n \times n$ matrices σ^ϕ , σ^{ξ_k} , and $\sigma^{\bar{\xi}}$, constructed from the square of the ordered Schmidt coefficients of ϕ , ξ_k and $\bar{\xi}$, respectively (e.g., $\sigma_{ii}^\phi = \beta_i$). Then the second inequality in Eq. (24) is equivalent to

$$\sum_k p_k F(\sigma^{\xi_k}, \sigma^\phi) \leq F(\sigma^{\bar{\xi}}, \sigma^\phi), \quad (25)$$

which corresponds to concavity of the fidelity since by construction $\sigma^{\bar{\xi}} = \sum_k p_k \sigma^{\xi_k}$.

Lemma 2 implies that we need focus only on deterministic conversions into a final pure state ξ . We assume, without loss of generality, that n (the dimension of the local Hilbert spaces) is the greatest of the number of nonvanishing Schmidt coefficients of the initial state ψ and the target state ϕ . We need to introduce some notation before we finally present the most faithful local conversion. Let us then call l_1 the smallest integer $\in [1, n]$ such that

$$\frac{E_{l_1}^\psi}{E_{l_1}^\phi} = \min_{l \in [1, n]} \frac{E_l^\psi}{E_l^\phi} \equiv r_1 \quad (\leq 1). \quad (26)$$

It may happen that $l_1 = r_1 = 1$. If not, it follows from the equivalence

$$\frac{a}{b} < \frac{a+c}{b+d} \Leftrightarrow \frac{a}{b} < \frac{c}{d} \quad (a, b, c, d > 0) \quad (27)$$

that for any integer $k \in [1, l_1 - 1]$

$$\frac{E_k^\psi - E_{l_1}^\psi}{E_k^\phi - E_{l_1}^\phi} > r_1. \quad (28)$$

Let us then define l_2 as the smallest integer $\in [1, l_1 - 1]$ such that

$$r_2 \equiv \frac{E_{l_2}^\psi - E_{l_1}^\psi}{E_{l_2}^\phi - E_{l_1}^\phi} = \min_{l \in [1, l_1 - 1]} \frac{E_l^\psi - E_{l_1}^\psi}{E_l^\phi - E_{l_1}^\phi} \quad (> r_1). \quad (29)$$

Repeating this process until $l_k = 1$ for some k , we obtain a series of $k+1$ integers $l_0 > l_1 > l_2 > \dots > l_k$ ($l_0 \equiv n+1$) and k positive real numbers $0 < r_1 < r_2 < \dots < r_k$, by means of which we define our final state

$$|\xi\rangle \equiv \sum_{i=1}^n \sqrt{\gamma_i} |i'_A i'_B\rangle, \quad (30)$$

where $|i'_A\rangle$, $|i'_B\rangle$ are the same as in Eq. (2), and

$$\gamma_i \equiv r_j \beta_i \quad \text{if } i \in [l_j, l_{j-1} - 1], \quad (31)$$

that is,

$$\vec{\gamma} = \begin{bmatrix} r_k \begin{bmatrix} \beta_{l_k} \\ \vdots \\ \beta_{l_{k-1}-1} \end{bmatrix} \\ \vdots \\ r_2 \begin{bmatrix} \beta_{l_2} \\ \vdots \\ \beta_{l_1-1} \end{bmatrix} \\ \vdots \\ r_1 \begin{bmatrix} \beta_{l_1} \\ \vdots \\ \beta_{l_0-1} \end{bmatrix} \end{bmatrix}. \quad (32)$$

By construction $\gamma_i \geq \gamma_{i+1}$ and

$$E_i^\psi \geq E_i^\xi \quad \forall i \in [1, n], \quad (33)$$

so the vector $\vec{\alpha}$ is majorized by the vector $\vec{\gamma}$, $\vec{\alpha} < \vec{\gamma}$. According to condition (3) the local strategy presented in Ref. [8] will indeed allow the parties to obtain the state ξ from ψ with certainty. Now, let us define positive quantities

$$A_j \equiv E_{l_j}^\psi - E_{l_{j-1}}^\psi = \sum_{i=l_j}^{l_{j-1}-1} \alpha_i \quad (E_{l_0}^\psi \equiv 0), \quad (34)$$

$$B_j \equiv E_{l_j}^\phi - E_{l_{j-1}}^\phi = \sum_{i=l_j}^{l_{j-1}-1} \beta_i \quad (E_{l_0}^\phi \equiv 0). \quad (35)$$

Then the fidelity between the final state ξ and the target state ϕ reads, in terms of the initial and target states

$$|\langle \xi | \phi \rangle|^2 = \left(\sum_{j=1}^k \sqrt{A_j B_j} \right)^2. \quad (36)$$

Without loss of generality, lemma 1 allows us to assume that any other possible final state ξ' has the same Schmidt basis as the target state ϕ and squared Schmidt coefficients $\gamma'_i \geq \gamma'_{i+1} \geq 0$, so by the Cauchy-Schwarz inequality $(\sqrt{x_1 y_1} + \sqrt{x_2 y_2})^2 \leq (x_1 + x_2)(y_1 + y_2)$, $(x_1, x_2, y_1, y_2 \geq 0)$,

$$F_{\xi'} \equiv F(\xi', \phi) \equiv \left(\sum_{i=1}^n \sqrt{\gamma'_i \beta_i} \right)^2 \quad (37)$$

$$\leq \left[\sum_{j=1}^k \left(\sum_{i=l_j}^{l_{j-1}-1} \gamma'_i \right)^{1/2} \sqrt{B_j} \right]^2, \quad (38)$$

where l_j ($j = 1, \dots, k$) have been defined in Eqs. (26)–(29). Now, recall that $\sum_{i=l_j}^{l_{j-1}-1} \gamma'_i = E_{l_j}^{\xi'} - E_{l_{j-1}}^{\xi'}$, and that the local and deterministic character of the conversion $\psi \rightarrow \xi'$ implies that $E_l^\psi \geq E_l^{\xi'}$ ($l = 1, \dots, n$). We can therefore define a_j as

$$a_j \equiv E_{l_j}^\psi - E_{l_j}^{\xi'}; \quad a_0 \equiv 0. \quad (39)$$

The condition $\alpha < \gamma'$ implies that $a_j \geq 0$ for each j . We may rewrite Eq. (38) in terms of the a_j and the A_j introduced in Eq. (34) as

$$F_{\xi'} \leq \left(\sum_{j=1}^k \sqrt{A_j - a_j + a_{j-1}} \sqrt{B_j} \right)^2 \equiv f(\vec{a}). \quad (40)$$

Our interest is in the behavior of $f(\vec{a})$ as a function of \vec{a} . We will show that in the allowed parameter region $f(\vec{a})$ is maximized when $\vec{a} = \vec{0}$. A direct computation shows that the (tridiagonal) matrix of second derivatives of $f(\vec{a})$, $(M_n)_{ij} \equiv \partial^2 f / \partial a_i \partial a_j$, is negative definite in the region $\mathcal{A} \subset \mathcal{R}^n$ defined by the constraints $a_j \geq 0$ and $A_j - a_j + a_{j-1} \geq 0$, which contains all relevant situations compatible with $\gamma'_i \geq \gamma'_{i+1} \geq 0$. Next, note that

$$\left. \frac{\partial f(\vec{a})}{\partial a_j} \right|_{\vec{a}=\vec{0}} = \sqrt{f(\vec{0})} \left(\sqrt{\frac{B_{j+1}}{A_{j+1}}} - \sqrt{\frac{B_j}{A_j}} \right). \quad (41)$$

By construction $A_j/B_j < A_{j+1}/B_{j+1}$ [compare Eqs. (26)–(29) and (34),(35)], so

$$\left. \frac{\partial f(\vec{a})}{\partial a_j} \right|_{\vec{a}=\vec{0}} < 0. \quad (42)$$

It follows that the maximum of $f(\vec{a} \in \mathcal{A})$ occurs at $\vec{a} = \vec{0}$, that is, when the final state ξ' is precisely the state ξ as defined in Eqs. (30)–(32). Therefore, we can conclude the following.

Theorem 3. The maximal fidelity F_{opt} achievable in a faithful local transformation of the initial pure state ψ into the target pure state ϕ is given by Eq. (36),

$$F_{\text{opt}} = \left(\sum_{j=1}^k \sqrt{A_j B_j} \right)^2. \quad (43)$$

The most faithful protocol consists in a deterministic conversion of ψ into the pure state ξ as defined in Eqs. (30)–(32).

IV. DISCUSSION AND APPLICATIONS

The next few sections apply theorem 3 to several problems of entanglement transformation. Section IV A finds the most faithful protocol for performing a special type of entanglement transformation known as entanglement concentration, in which a large number of partially entangled states are transformed into Bell pairs. This result is then applied to determine the most faithful teleportation protocol via any given pure quantum state. Section IV B finds the most faithful protocol for performing the reverse procedure to concentration, entanglement dilution. Section IV C compares the most faithful transformation with the optimal conclusive transformation, and concludes that in general they are different. Section IV D explains how our results can be used to demonstrate the robustness against noise of entanglement transformation protocols for pure states and Sec. IV E explains this in the special case of entanglement catalysis.

A. Concentration of entanglement and optimal teleportation fidelity

An entanglement concentration protocol [5] is a strategy for obtaining maximally entangled states from some partially entangled initial (pure) state ψ using only LOCC. In the original formulation of this concept, due to Bennett, Bernstein, Popescu, and Schumacher [5], many (N) copies of an $(n \times n)$ -dimensional state ψ are available, and the goal is to obtain the largest number of n -states in the asymptotic limit where $N \rightarrow \infty$. More recently, the optimal way to conclusively concentrate the entanglement of a *single copy* of ψ has also been obtained [7,10,11].

In this section we solve the same problem from the point of view of faithful conversions. In this case, the goal is to determine the local strategy that maximizes the fidelity between the single copy of ψ and the maximally entangled n -state ψ_n . It turns out that the optimal strategy in this case is essentially to do nothing at all. The only requirement is to apply the local unitary rotations that align the Schmidt components of ψ to those of ψ_n , in the manner implied by lemma 1. This result can be shown using Eqs. (26)–(32). However, a simpler derivation can be obtained from the following argument. First, for any pure state ψ with Schmidt coefficients $\sqrt{\alpha_1} \geq \dots \geq \sqrt{\alpha_n}$, consider the function

$$F_{\max}(\psi) = \frac{1}{n} \left(\sum_{i=1}^n \sqrt{\alpha_i} \right)^2. \quad (44)$$

As has been pointed out by Horodecki [23], F_{\max} is a unitarily invariant, concave function of the reduced density matrix $\rho_A = \text{Tr}_B |\psi\rangle\langle\psi|$. Following theorem 2 in Ref. [14], it is therefore an entanglement monotone for pure states. In fact, lemma 1 shows that $F_{\max}(\psi)$ is the greatest fidelity with respect to ψ_n that is achievable from ψ by local unitary rotations. Now, following lemma 2, let ξ be the most faithful approximation of ψ_n obtainable from ψ by LOCC. By definition then, $F_{\max}(\psi) \leq F_{\max}(\xi)$. On the other hand, since F_{\max} is an entanglement monotone, we must also have $F_{\max}(\psi) \geq F_{\max}(\xi)$. These quantities are therefore equal, which implies that the optimally faithful strategy can be achieved using only local unitary rotations.

It is interesting to note that F_{\max} can also have another interpretation. It is equivalent to the robustness of entanglement $R(\psi)$, an entanglement monotone that was comprehensively studied in Ref. [14]. $R(\psi)$ is defined as the minimal amount of separable noise that has to be mixed with state ψ in order to wash out its quantum correlations completely. For pure states, its value reads $R(\psi) = nF_{\max}(\psi) - 1$.

An important consequence of determining F_{\max} is that it also allows us to determine the optimal fidelity of teleportation via ψ . Recall that perfect teleportation of an unknown n -dimensional state can be realized only if an “ n state” is shared between Alice and Bob [2]. For a more general initially shared state ψ , one must admit some imperfection in the procedure. As with entanglement transformations, it is possible to consider two approaches to imperfect teleportation: on the one hand, conclusive teleportation strategies seek to maximize the likelihood of achieving ideal teleportation,

but also allow for the possibility of failure [24]. On the other hand, faithful strategies seek to maximize the so-called fidelity of teleportation. For any given teleportation strategy \mathcal{T} , this quantity is naturally defined [25] as the average overlap between Alice’s initial state ϕ and the final teleported state obtained by Bob

$$f(\Lambda_{\mathcal{T},\psi}) = \int d\phi \langle \phi | \Lambda_{\mathcal{T},\psi} (|\phi\rangle\langle\phi|) | \phi \rangle, \quad (45)$$

where $\Lambda_{\mathcal{T},\psi}$ is the trace-preserving quantum operation that maps the initial state onto the teleported one (a construction for this operation may be found in Ref. [26]).

Recently, a connection has been found between this quantity and faithful entanglement concentration procedures [25]. It has been shown that, for any given initial state ρ (pure or mixed) in $(n \times n)$ -dimensional Hilbert space, the maximum value of f over *all possible* teleportation protocols implemented using LOCC is given by

$$f_{\max}(\rho) = \frac{F_{\max}(\rho)n + 1}{n + 1}. \quad (46)$$

Here, $F_{\max}(\rho)$ is precisely the maximum fidelity that can be achieved between ρ and an n -state under a trace-preserving quantum operation implemented via local operations and classical communication. In general, it is not yet known how to calculate this quantity. However, in the case of a pure initial state $\rho = \psi$, its value is the one found in Eq. (44) above. The maximum fidelity of teleportation via ψ is then also immediately determined via Eq. (46):

$$f_{\max}(\psi) = \frac{\left(\sum_{i=1}^n \sqrt{\alpha_i} \right)^2 + 1}{n + 1}. \quad (47)$$

A “most faithful” teleportation protocol that achieves this limit has also been described in Ref. [25]. For any initial state ρ , its first step requires transforming ρ into the most faithful achievable approximation of an n state. In the case of a pure state ψ , we now know that this is done merely by the Schmidt-basis alignment described above. The remainder of the protocol requires then only a so-called “ $U \otimes U^*$ twirling” [25] of the state (resulting in a Werner state [27]), followed by applying the standard teleportation procedure [2]. We therefore have now an explicit protocol for realizing optimally faithful teleportation via pure states.

B. Entanglement dilution

We now consider the reverse process to entanglement concentration, entanglement dilution [5]. In this case, the parties start out with some m -state ψ_m and aim at obtaining a final, less entangled state ϕ , constituted of N copies of some smaller-dimensional state χ , i.e., $\phi = \chi^{\otimes N}$. If the number of nonvanishing Schmidt coefficients of χ is greater than $\sqrt[N]{m}$, then this exact transformation is not possible at all — not even with only some probability of success — since ϕ has

fewer Schmidt components than $\psi, m < n$ [7]. In this case, it is interesting to consider the most faithful approximation to $\chi^{\otimes N}$ that can be achieved.

Let $|\phi\rangle = \sum_{i=1}^n \sqrt{\beta_i} |i_A i_B\rangle$. The most faithful approximation ξ to ϕ that can be obtained from ψ_m by LOCC is determined using Eqs. (26)–(32) as follows: from Eq. (26), we have $r_1=0$, $l_1=m+1$. Equation (29) gives $r_2 = (m \sum_{i=1}^m \beta_i)^{-1}$, $l_2=1$. It follows that

$$|\xi\rangle = \frac{1}{\sqrt{\sum_{i=1}^m \beta_i}} \sum_{i=1}^m \sqrt{\beta_i} |i_A i_B\rangle, \quad (48)$$

and the corresponding optimal fidelity (43) simply reads

$$F_{\text{opt}} = \sum_{i=1}^m \beta_i. \quad (49)$$

In other words, the best approximation to the target state ϕ is the state of highest norm that can be obtained by projecting ϕ onto an $(m \times m)$ -dimensional subspace.

In Ref. [5] the problem of optimal entanglement dilution was solved in the asymptotic limit $m, N \rightarrow \infty$. In this regime, the dilution procedure can actually be realized with 100% efficiency. The protocol realizing this is well-defined for any finite values of m, N . It consists essentially in identifying the subspace of ϕ spanned by its m largest Schmidt components and then using the m -state ψ_m to teleport half of this over to Bob. It can be easily verified that the resulting fidelity with respect to ϕ is given precisely by the expression above. This then shows that not only does this protocol approach fidelity 1 as $m, N \rightarrow \infty$, but it is also optimal for any finite values of these quantities.

C. Faithful versus conclusive transformations

Suppose Alice and Bob's aim is to transform the state ψ into the state ϕ . We have found the optimal fidelity with which this transformation can be accomplished. A natural question to ask is how this faithful conversion strategy compares with the optimal conclusive strategy—the one that maximizes the probability of successful conversion [9]. A first observation is that the latter is in general *not* also the most faithful strategy. This follows since the optimal conclusive strategy will not usually succeed with 100% probability, whereas lemma 2 shows that the fidelity with respect to ϕ is always maximized by means of a deterministic transformation. A simple example is the case of a two-qubit system initially in a partially entangled state $a|00\rangle + b|11\rangle$, with $a > b > 0$. As we have seen above, the most faithful strategy for converting it into the maximally entangled two state is simply to do nothing, which corresponds to a fidelity of $\frac{1}{2} + ab$. On the other hand, the optimal conclusive transformation, which succeeds with probability $2b^2$ [7,9], results in an average fidelity of $\frac{1}{2} + b^2$, which is strictly less than was achieved by the most faithful transformation.

We also note the surprising fact that, in all cases, realizing the most faithful conversion does not diminish in any way

Alice and Bob's chances of conclusively obtaining the target state. This follows since the final state ξ in Eqs. (30)–(32) is precisely the same as the intermediate state Ω in the optimal conclusive protocol presented in Ref. [9], Eqs. (9)–(13). This means then that no probability of success is lost during a most faithful conversion, that is,

$$P(\psi \rightarrow \phi) = P(\xi \rightarrow \phi). \quad (50)$$

In other words, the parties may postpone their decision on whether or not they wish to risk their initial state in a conclusive transformation into ϕ , while obtaining already the most faithful approximation to ϕ .

D. Robustness of transformations

Up to this point, our discussion has assumed that the initial state ψ shared by Alice and Bob is pure. Suppose, however, that ψ is corrupted a little before it is made available to Alice and Bob, so they receive a density matrix ρ instead. What can we say about the possibility of transforming ρ into a target state ϕ ? This section establishes upper and lower bounds on the fidelity with which the transformation $\rho \rightarrow \phi$ may be accomplished, and the next section explains how these results may be used to analyze the robustness of effects such as entanglement catalysis [17].

Our results are most easily presented using the trace distance, a metric on Hermitian operators defined by $T(A, B) \equiv \text{Tr}(|A - B|)$, where $|X|$ denotes the positive square root of the Hermitian matrix X^2 . Ruskai [28] has shown that the trace distance contracts under physical processes. More precisely, if ρ and σ are any two density operators, and if $\rho' \equiv \mathcal{E}(\rho)$ and $\sigma' \equiv \mathcal{E}(\sigma)$ denote states after some physical process represented by the (trace-preserving) quantum operation \mathcal{E} occurs, then

$$T(\rho', \sigma') \leq T(\rho, \sigma). \quad (51)$$

We will use $T(\psi, \phi)$ to denote the trace distance between the density matrices $|\psi\rangle\langle\psi|$ and $|\phi\rangle\langle\phi|$. For pure states the trace distance and the fidelity are related by the simple formula

$$T(\psi, \phi) = 2\sqrt{1 - F(\psi, \phi)}. \quad (52)$$

Returning to the problem of entanglement transformation, suppose ψ is a pure state that we wish to transform into a pure state ϕ . Let $T(\psi \rightarrow \phi)$ denote the minimal trace distance that can be achieved by such a transformation; this is easily found by substituting Eq. (43) into Eq. (52). We will provide upper and lower bounds on $T(\rho \rightarrow \phi)$, the minimal trace distance to ϕ that may be achieved by a protocol starting with the state ρ , and using local operations and classical communication.

Suppose we start with the state ρ , and apply the protocol that most faithfully transforms ψ into ϕ . Define ρ' to be the result of applying this protocol to ρ , and ψ' the result of applying the protocol to ψ . Then since this is just one possible protocol, not necessarily optimal, for transforming ρ into ϕ , we must have

$$T(\rho \rightarrow \phi) \leq T(\rho', \phi). \quad (53)$$

By the metric property of the trace distance

$$T(\rho', \phi) \leq T(\rho', \psi') + T(\psi', \phi). \quad (54)$$

But by the contractivity property (51) we have $T(\rho', \psi') \leq T(\rho, \psi)$, and the choice of protocol ensures that $T(\psi', \phi) = T(\psi \rightarrow \phi)$. Thus Eq. (54) implies

$$T(\rho \rightarrow \phi) \leq T(\rho, \psi) + T(\psi \rightarrow \phi), \quad (55)$$

which is an upper bound on $T(\rho \rightarrow \phi)$ in terms of the easily calculated quantities $T(\rho, \psi)$ and $T(\psi \rightarrow \phi)$.

A lower bound on $T(\rho \rightarrow \phi)$ may be obtained by a similar technique. Suppose ρ'' and ψ'' are the states obtained from ρ and ψ , respectively, by applying the optimal transformation protocol for obtaining ϕ from ρ . Then we must have

$$T(\psi \rightarrow \phi) \leq T(\psi'', \phi). \quad (56)$$

By the metric property, $T(\psi'', \phi) \leq T(\psi'', \rho'') + T(\rho'', \phi)$. By contractivity, $T(\psi'', \rho'') \leq T(\psi, \rho)$, and by the choice of protocol, $T(\rho'', \phi) = T(\rho \rightarrow \phi)$. Thus

$$T(\psi \rightarrow \phi) \leq T(\rho, \psi) + T(\rho \rightarrow \phi), \quad (57)$$

which provides a lower bound on $T(\rho \rightarrow \phi)$. Combining upper and lower bounds on $T(\rho \rightarrow \phi)$ into a single equation we have the useful inequality

$$|T(\rho \rightarrow \phi) - T(\psi \rightarrow \phi)| \leq T(\rho, \psi). \quad (58)$$

We note in passing that the same method may be used to prove that for any quadruple of quantum states $\rho_1, \rho_2, \sigma_1, \sigma_2$ the following more general inequality holds:

$$|T(\rho_1 \rightarrow \sigma_1) - T(\rho_2 \rightarrow \sigma_2)| \leq T(\rho_1, \rho_2) + T(\sigma_1, \sigma_2). \quad (59)$$

This inequality is of special use in the case where, for example, ρ_2 and σ_2 are pure states, since then theorem 3 allows $T(\rho_2 \rightarrow \sigma_2)$ to be calculated explicitly, and Eq. (59) then bounds the quantity $T(\rho_1 \rightarrow \sigma_1)$, which we do not know how to calculate exactly in general.

E. Example: robustness of entanglement catalysis

As an illustration of the usefulness of the inequality (58), we study the robustness of the phenomenon of *entanglement catalysis* [17] under the presence of initial noise. First let us recall the nature of this effect: it is sometimes the case that, although Alice and Bob cannot deterministically transform ψ into ϕ by local operations and classical communication, there exist *catalyst* entangled states η such that $\psi \otimes \eta$ can be transformed into $\phi \otimes \eta$ by local operations and classical communication. More generally, partial catalyst states may exist that improve the efficiency of the conversion from ψ into ϕ , although not to 100%. In Ref. [17] this effect was studied from the point of view of conclusive conversions: partial catalysts were seen to improve the probability of conclusively obtaining ϕ from ψ . Another point of view, along

the lines of the present work, is to regard them as reducing the minimal trace distance achievable in a faithful conversion:

$$T(\psi \otimes \eta \rightarrow \phi \otimes \eta) < T(\psi \rightarrow \phi). \quad (60)$$

We can now ask whether this improvement survives in the presence of a distortion of the states involved. Suppose for instance that the initial state and catalyst are subject to some noise, so that instead of $\psi \otimes \eta$ we have in fact a mixed state ρ which is merely close to $\psi \otimes \eta$. Taking the trace distance $\varepsilon = T(\rho, \psi \otimes \eta)$ as a measure of the magnitude of the noise, we can then ask how small ε has to be if the catalytic effect is to be preserved.

From Eq. (58) we have

$$T(\rho \rightarrow \phi \otimes \eta) - T(\psi \otimes \eta \rightarrow \phi \otimes \eta) \leq T(\rho, \psi \otimes \eta) = \varepsilon. \quad (61)$$

Now let $\Delta T_\eta = T(\psi \rightarrow \phi) - T(\psi \otimes \eta \rightarrow \phi \otimes \eta)$ be the reduction in the trace distance achievable using the catalyst η when there is no initial error. Then as long as

$$\varepsilon < \Delta T_\eta, \quad (62)$$

we still obtain $T(\rho \rightarrow \phi \otimes \eta) < T(\psi \rightarrow \phi)$, and therefore a catalytic enhancement of the fidelity obtainable via LOCC is still present.

V. NONLOCAL DISTANCE MEASURES

We can use the optimality result of theorem 3 to define notions of fidelity and distance on the space of quantum states that measures how different the ‘‘nonlocal’’ properties of those states are. For example, we define the *nonlocal fidelity* between pure states $|\psi\rangle$ and $|\phi\rangle$ by

$$F_{\text{nl}}(\psi, \phi) \equiv \min(F(\psi \rightarrow \phi), F(\phi \rightarrow \psi)), \quad (63)$$

where $F(\psi \rightarrow \phi)$ is the optimal fidelity for transforming ψ into ϕ by LOCC, and $F(\phi \rightarrow \psi)$ is the optimal fidelity, in general different, for transforming ϕ into ψ by LOCC. The nonlocal fidelity quantifies the similarity in quantum correlations present in ψ and ϕ . The nonlocal fidelity can be turned into a metric by using the *trace distance*. Recall that the trace distance between density matrices ρ and σ is defined by $T(\rho, \sigma) \equiv \text{Tr}|\rho - \sigma|$. For pure states ψ and ϕ the trace distance is related to the fidelity by the formula (52), which we reproduce here for convenience:

$$T(\psi, \phi) = 2\sqrt{1 - F(\psi, \phi)}. \quad (64)$$

Analogous to the nonlocal fidelity we may define the nonlocal trace distance

$$T_{\text{nl}}(\psi, \phi) \equiv 2\sqrt{1 - F_{\text{nl}}(\psi, \phi)}. \quad (65)$$

This is a metric on the space of pure states of a bipartite system, where we agree to identify two states if they have the same Schmidt coefficients. To see the metric property, note that the nonlocal distance is manifestly symmetric, and that $T_{\text{nl}}(\psi, \phi) = 0$ if and only if $F(\psi \rightarrow \phi) = 1$ and $F(\phi \rightarrow \psi)$

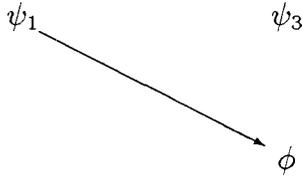


FIG. 3. ϕ is the best approximation to ψ_3 that may be obtained from ψ_1 by local operations and classical communication.

$=1$, which we know is true if and only if ψ and ϕ have the same Schmidt coefficients. All that remains is to prove the triangle inequality

$$T_{\text{nl}}(\psi_1, \psi_3) \leq T_{\text{nl}}(\psi_1, \psi_2) + T_{\text{nl}}(\psi_2, \psi_3). \quad (66)$$

To prove this, we use a construction illustrated in Figs. 3 and 4. Without loss of generality, we suppose that

$$T_{\text{nl}}(\psi_1, \psi_3) = T(\psi_3, \phi), \quad (67)$$

where ϕ is the best possible approximation to ψ_3 that may be obtained from ψ_1 by local operations and classical communication. Furthermore, let ϕ_2 be the best approximation to ψ_2 that can be obtained from ψ_1 by local operations and classical communication, and let ϕ_3 be the best approximation to ψ_3 that can be obtained from ψ_2 by local operations and classical communication. Then

$$T(\psi_2, \phi_2) \leq T_{\text{nl}}(\psi_1, \psi_2), \quad T(\psi_3, \phi_3) \leq T_{\text{nl}}(\psi_2, \psi_3). \quad (68)$$

Furthermore, let p_i, ϕ'_i be the ensemble of states that results when the protocol used to transform ψ_2 into ϕ_3 is applied to ϕ_2 instead. Define $\rho \equiv \sum_i p_i |\phi'_i\rangle\langle\phi'_i|$. Then since ρ may be obtained from ψ_1 by local operations and classical communication we have

$$T_{\text{nl}}(\psi_1, \psi_3) \leq T(\rho, \psi_3) \quad (69)$$

$$\leq T(\rho, \phi_3) + T(\phi_3, \psi_3), \quad (70)$$

where we applied the metric property of the trace distance on the second line. We again use the result of Ruskai [28] stating that $T(\dots, \dots)$ never decreases if the same trace-preserving quantum operation is applied to each argument,

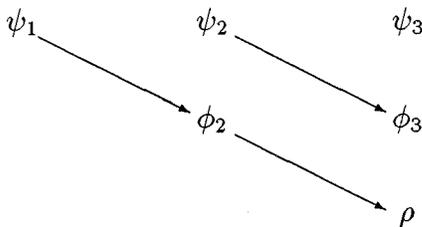


FIG. 4. ϕ_2 is the best approximation to ψ_2 that can be obtained from ψ_1 by local operations and classical communication. ϕ_3 is the best approximation to ψ_3 that can be obtained from ψ_2 by local operations and classical communication. ρ is the (possibly mixed) state that results when the protocol converting ψ_2 to ψ_3 is applied to ϕ_2 .

so $T(\rho, \phi_3) \leq T(\phi_2, \psi_2)$. Combining this observation with Eq. (70) and then applying Eq. (68) gives

$$T_{\text{nl}}(\psi_1, \psi_3) \leq T(\phi_2, \psi_2) + T(\phi_3, \psi_3) \quad (71)$$

$$\leq T_{\text{nl}}(\psi_1, \psi_2) + T_{\text{nl}}(\psi_2, \psi_3), \quad (72)$$

which is the triangle inequality (66).

Analogous constructions may be carried out for the mixed state case. Unfortunately, general conditions for transforming one mixed state to another by local operations and classical communication are not yet known, so we cannot evaluate the nonlocal distance or nonlocal fidelity in this instance. [Note, however, that Eq. (58) does allow one to prove bounds on the general nonlocal distance.] In the case of mixed states there are inequivalent measures of distance available for use in the definition of nonlocal distance, such as the trace distance and the Bures distance [29]. In general, any good measure of distance for quantum states can be used to define a good measure of nonlocal distance, provided it has a contractivity property analogous to that for the trace distance (which, for example, the Bures distance has).

VI. CONCLUSION

We have found the optimal approximate schemes for transforming one pure entangled state into another using local operations and classical communication. These results have been used to determine the best possible schemes for entanglement concentration and dilution, to determine the optimal teleportation fidelity that may be achieved when imperfect pure state entanglement is available, and to obtain bounds on how well entanglement can be transformed in the presence of a small amount of noise in the initial state. This in turn allows us to estimate how robust surprising effects such as entanglement catalysis are against such small perturbations. Furthermore, we defined a nonlocal fidelity to measure the difference in the entanglement present in two quantum states. This quantity is not affected by local unitary changes to the system, and can be used to define interesting nonlocal metrics on the space of entangled states. We believe that these results shed considerable light on the ongoing effort to develop the notion of entanglement as a physical resource that can be employed in a wide variety of information processing tasks. In particular, an understanding of approximation is crucial to the analysis of proposals for tasks of practical interest, such as the cryptographic protocol recently proposed by Barnum [12], whose security depends upon the difficulty of performing certain entanglement transformations.

ACKNOWLEDGMENTS

G.V. acknowledges CIRIT Grant No. 1997FI-00068 PG and financial support from CIRYT Contract No. AEN98-

0431, and CIRIT Contract No. 1998SGR-00026. D.J. thanks the Brazilian agency Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), the Leverhulme Trust, EPSRC, the ORS Award Scheme, and the European Union. M.A.N. was supported by DARPA through the Quantum Information and Computing Institute (QUIC) adminis-

tered through the ARO. Part of this work was completed during the “Complexity, Computation and the Physics of Information” workshop of the Isaac Newton Institute and the ESF-QIT meeting in Cambridge. The authors thank the Institute and the European Science Foundation for support during this period.

-
- [1] J. Preskill, Proc. R. Soc. London, Ser. A **454**, 469 (1998).
 - [2] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
 - [3] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
 - [4] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).
 - [5] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
 - [6] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
 - [7] H.-K. Lo and S. Popescu, e-print quant-ph/9707038.
 - [8] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
 - [9] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999).
 - [10] D. Jonathan and M. B. Plenio, Phys. Rev. Lett. **83**, 1455 (1999).
 - [11] L. Hardy, Phys. Rev. A **60**, 1912 (1999).
 - [12] H. Barnum, e-print quant-ph/9910072.
 - [13] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, 1993).
 - [14] G. Vidal, e-print quant-ph/9807077.
 - [15] R. Bhatia, *Matrix Analysis* (Springer-Verlag, New York, 1997).
 - [16] A. Kent, Phys. Rev. Lett. **81**, 2839 (1998).
 - [17] D. Jonathan and M. B. Plenio, Phys. Rev. Lett. **83**, 3566 (1999).
 - [18] J. Kempe, Phys. Rev. A **60**, 910 (1999).
 - [19] C. A. Fuchs and J. van de Graaf, IEEE Trans. Inf. Theory **45**, 1216 (1999).
 - [20] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).
 - [21] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications* (Academic Press, New York, 1979).
 - [22] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).
 - [23] M. Horodecki (private communication).
 - [24] T. Mor, e-print quant-ph/9608005.
 - [25] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).
 - [26] M. A. Nielsen and C. M. Caves, Phys. Rev. A **55**, 2547 (1997).
 - [27] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
 - [28] M. B. Ruskai, Rep. Math. Phys. **6**, 1147 (1994).
 - [29] D. Bures, Trans. Am. Math. Soc. **135**, 199 (1969).