Entanglement sharing through noisy qubit channels: One-shot optimal singlet fraction

Rajarshi Pal[*]
Optics and Quantum Information Group, The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India

Somshubhro Bandyopadhyay[†]
Department of Physics and Center for Astroparticle Physics and Space Science, Bose Institute, Block EN, Sector V, Bidhan Nagar, Kolkata 700091, India

Sibasish Ghosh[‡]
Optics and Quantum Information Group, The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India
(Received 13 January 2014; published 5 November 2014)

Maximally entangled states—a resource for quantum information processing—can only be shared through noiseless quantum channels, whereas in practice channels are noisy. Here we ask: Given a noisy quantum channel, what is the maximum attainable purity (measured by singlet fraction) of shared entanglement for single channel use and local trace preserving operations? We find an exact formula of the maximum singlet fraction attainable for a qubit channel and give an explicit protocol to achieve the optimal value. The protocol distinguishes between unital and nonunital channels and requires no local postprocessing. In particular, the optimal singlet fraction is achieved by transmitting part of an appropriate pure entangled state, which is maximally entangled if and only if the channel is unital. A linear function of the optimal singlet fraction is also shown to be an upper bound on the distillable entanglement of the mixed state dual to the channel.

DOI: 10.1103/PhysRevA.90.052304 PACS number(s): 03.67.Hk, 03.65.Ud, 03.65.Yz, 03.67.Mn

I. INTRODUCTION

Shared entanglement between two separated observers (Alice and Bob) is a critical resource for quantum information processing (QIP) tasks such as dense coding [1], cryptography [2], distributed quantum computation [3], and quantum teleportation [4]. Faithful implementation of QIP tasks require maximally entangled states, which can only be shared through noiseless quantum channels, where Alice prepares a maximally entangled state of two particles (say, qubits) and sends one of them to Bob through the channel. In practice, available channels are noisy resulting in mixed states. Entanglement distillation [5–9] provides a solution by converting these mixed states to fewer almost-perfect entangled states of purity close to unity while requiring many uses of the channel and joint measurements on many copies of the output. Clearly, the yield in an entanglement distillation protocol depends on the purity of the mixed states, which in turn is a function of the amount of noise present in the quantum channel. Thus, in the simplest case of entanglement sharing, a basic question is: Given a noisy quantum channel what is the maximum achievable purity for single use of the channel?

In this work, we answer the above question for qubit channels within the paradigm of trace-preserving local operations (TP-LOCC). By restricting to this class of operations, where no subsystem is thrown away, our results provide the conditions and an explicit protocol when every single use of the channel is maximally efficient. Our result also characterizes qubit channels by quantifying reliable transmission of quantum information via teleportation for single channel use and TP-LOCC.

In the simplest scenario, the general protocol of sharing entanglement works as follows: Alice prepares a bipartite pure entangled state $|\psi\rangle$ and sends one half of it to Bob through a quantum channel, say Λ (which, throughout the present paper, is assumed to be nonentanglement breaking). This results, in general, in a mixed entangled state $\rho_{\psi,\Lambda} = (I \otimes \Lambda)(\rho_\psi)$, where $\rho_\psi = |\psi\rangle\langle\psi|$. The *purity* of this state is characterized by its singlet fraction [5,7,9,10] defined as

$$F(\rho_{\psi,\Lambda}) = \max_{|\Phi\rangle} \langle\Phi|\rho_{\psi,\Lambda}|\Phi\rangle, \tag{1}$$

where $|\Phi\rangle$ is a maximally entangled state. The singlet fraction quantifies how close the state $\rho_{\psi,\Lambda}$ is to a maximally entangled state, and therefore how useful the state is for QIP tasks. For example, it is related to the teleportation fidelity f for teleportation of a qudit via the following relation:

$$f(\rho_{\psi,\Lambda}) = \frac{dF(\rho_{\psi,\Lambda}) + 1}{d+1}. \tag{2}$$

In this work we are interested in the *optimal singlet fraction* for the channel Λ defined as

$$F(\Lambda) = \max_{|\psi\rangle} \max_{L} F(L(\rho_{\psi,\Lambda})), \tag{3}$$

where the maximum is taken over all pure state transmissions and trace-preserving LOCCs L. Note that, by virtue of Eq. (2) $F(\Lambda)$ also quantifies reliable transmission of quantum states via teleportation, albeit for single channel use, where the optimal teleportation fidelity for the channel is expressed as $f(\Lambda) = \frac{dF(\Lambda)+1}{d+1}$. This is in contrast with the known measures such as channel fidelity [9], which quantifies, on an average, how close the output state is to the input state, and entanglement fidelity [11,12], which captures how well

[*]rajarshi@imsc.res.in
[†]som@jcbose.ac.in
[‡]sibasish@imsc.res.in

the channel preserves entanglement [13] of the transmitted system with other systems.

For qubit channels such as depolarizing [9] and amplitude damping [14] the value of $F(\Lambda)$ is known, but no general expression has been found yet for a generic qubit channel. In this work, we obtain an exact formula of $F(\Lambda)$ for a qubit channel and give an explicit protocol to achieve this value. Surprisingly, we also find that to attain the optimal value no local postprocessing is required, even though it is known that local postprocessing can increase the singlet fraction of a state. In particular, we show that the optimal value is attained by sending part of a maximally entangled state down the channel if and only if the channel is unital. This means that for nonunital channels one must necessarily transmit part of an appropriate nonmaximally entangled state. We also prove that the optimal singlet fraction is equal to a linear function of the negativity [10] of the mixed state $\rho_{\Phi^+,\Lambda}$, where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Thus a linear function of $F(\Lambda)$ is an upper bound on the distillable entanglement of the mixed state $\rho_{\Phi^+,\Lambda}$.

Let us note a couple of implications of our results. As noted earlier, an entanglement distillation [5–9] protocol uses many copies of the mixed state $\rho_{\psi,\Lambda}$ (for some transmitted pure state $|\psi\rangle$) of purity $F(\rho_{\psi,\Lambda})$ and converts them to a fewer number of near-perfect entangled states of purity close to unity. Following the prescription in this paper, for a given noisy qubit channel Alice and Bob can now prepare states with maximum achievable purity for each channel use so as to maximize the yield in their distillation protocol. Second, by virtue of Eq. (2) we are able to provide the optimal teleportation fidelity for any qubit channel, albeit for single channel use.

The paper is organized as follows: In Sec. II we provide an analytical expression for the optimal singlet fraction of any qubit channel and a recipe for obtaining the optimal value by sharing a pure entangled state across the channel. We also prove that this pure entangled state is maximally entangled if and only if the channel is unital. In Sec. III we relate the optimal singlet fraction with the maximum output negativity of a state that can be shared across the channel. In Sec. IV we show that for a nonunital qubit channel the singlet fraction obtained by postprocessing the output of any maximally entangled state is strictly less than the optimal value. We conclude in Sec. V.

II. OPTIMAL SINGLET FRACTION FOR QUBIT CHANNELS

A. Preliminaries

A quantum channel Λ is a trace-preserving completely positive map characterized by a set of Kraus operators $\{A_i\}$ satisfying $\sum A_i^\dagger A_i = I$. Its dual $\hat{\Lambda}$ is described in terms of the Kraus operators $\{A_i^\dagger\}$ (the dual is the adjoint map with respect to the Hilbert-Schmidt inner product). A channel Λ is said to be *unital* if its action preserves identity: $\Lambda(I) = I$, and *nonunital* if it does not, i.e., $\Lambda(I) \neq I$. A dual channel $\hat{\Lambda}$ is trace preserving if and only if Λ is unital. Sending half of a bipartite pure state $|\phi\rangle$ down the channel $\$ \in \{\Lambda, \hat{\Lambda}\}$ gives rise to a mixed state (not necessarily normalized)

$$\rho_{\phi,\$} = (I \otimes \$)(\rho_\phi), \tag{4}$$

where $\rho_\phi = |\phi\rangle\langle\phi|$. For the channel \$ with a set of Kraus operators $\{K_i\}$, the above equation takes the form

$$\rho_{\phi,\$} = \sum_i (I \otimes K_i)\rho_\phi(I \otimes K_i^\dagger). \tag{5}$$

Recall that, by transmitting one half of a pure entangled state $|\psi\rangle$ through a noisy channel Λ results in a mixed state $\rho_{\psi,\Lambda}$ of singlet fraction $F(\rho_{\psi,\Lambda})$. Simply maximizing $F(\rho_{\psi,\Lambda})$ over all transmitted pure states $|\psi\rangle$ may not yield the optimal value we are looking for because it is known [15–17] that TP-LOCC can enhance the singlet fraction of two qubit states. Thus for a given $\rho_{\psi,\Lambda}$, the maximum achievable singlet fraction is defined as [17]

$$F^*(\rho_{\psi,\Lambda}) = \max_L F(L(\rho_{\psi,\Lambda})), \tag{6}$$

where the maximization is over all TP-LOCC L carried out by Alice and Bob on their respective qubits. Note that, unlike F, which can increase under TP-LOCC, F^* is an entanglement monotone [17] and can be exactly computed [17] by solving a convex semidefinite program for any given two-qubit density matrix. Maximizing F^* over all transmitted pure states $|\psi\rangle$ yields the *optimal singlet fraction* defined earlier in Eq. (3):

$$F(\Lambda) = \max_{|\psi\rangle} F^*(\rho_{\psi,\Lambda}). \tag{7}$$

It is clear from the above definitions that for any shared pure state $|\psi\rangle$, the following inequalities hold:

$$F(\Lambda) \geqslant F^*(\rho_{\psi,\Lambda}) \geqslant F(\rho_{\psi,\Lambda}). \tag{8}$$

B. Results

Our first result gives an exact formula for the optimal singlet fraction defined in Eq. (7) and an explicit protocol by which the optimal value can be achieved. We show that for any qubit channel Λ there exists an "optimal" two-qubit pure state $|\psi_0\rangle$, not necessarily maximally entangled, such that all the inequalities in (8) become equalities.

Theorem 1. The optimal singlet fraction of a qubit channel Λ is given by

$$F(\Lambda) = \lambda_{\max}(\rho_{\Phi^+,\Lambda}), \tag{9}$$

where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and $\lambda_{\max}(\rho_{\Phi^+,\Lambda})$ is the maximum eigenvalue of the density matrix $\rho_{\Phi^+,\Lambda}$. Moreover, the following equalities hold:

$$F(\Lambda) = F^*(\rho_{\psi_0,\Lambda}) = F(\rho_{\psi_0,\Lambda}), \tag{10}$$

where $|\psi_0\rangle$ is the eigenvector corresponding to the maximum eigenvalue of the density matrix $\rho_{\Phi^+,\hat{\Lambda}}$.

Proof. We begin by obtaining an exact expression of the maximum preprocessed singlet fraction. It is defined as

$$F_1(\Lambda) = \max_{|\psi\rangle} F(\rho_{\psi,\Lambda}) \tag{11}$$

$$= \max_{|\psi\rangle} \max_{|\Phi\rangle} \langle\Phi|\rho_{\psi,\Lambda}|\Phi\rangle, \tag{12}$$

where $|\Phi\rangle$ is maximally entangled. Noting that every maximally entangled state $|\Phi\rangle$ can be written as $(U \otimes V)|\Phi^+\rangle$, for some $U, V \in \mathrm{SU}(2)$, we can rewrite Eq. (12) as

$$F_1(\Lambda) = \max_{|\psi\rangle,U,V} \langle\Phi^+|(U^\dagger \otimes V^\dagger)\rho_{\psi,\Lambda}(U \otimes V)|\Phi^+\rangle. \tag{13}$$

Let, $\rho_\psi = |\psi\rangle\langle\psi|$ and $\rho_{\Phi^+} = |\Phi^+\rangle\langle\Phi^+|$. Using the fact that $(I\otimes V)|\Phi^+\rangle = (V^T \otimes I)|\Phi^+\rangle$, we now simplify the above equation:

$$\begin{aligned} F_1(\Lambda) &= \max_{|\psi\rangle,U,V} \langle\Phi^+|(U^\dagger \otimes V^\dagger)\rho_{\psi,\Lambda}(U\otimes V)|\Phi^+\rangle \qquad (14)\\ &= \max_{|\psi\rangle,U,V} \langle\Phi^+|(U^\dagger \otimes V^\dagger)\sum_i (I\otimes A_i)\rho_\psi(I\otimes A_i^\dagger)(U\otimes V)|\Phi^+\rangle \\ &= \max_{|\psi\rangle,U,V} \langle\psi|\sum_i (I\otimes A_i^\dagger)(U\otimes V)\rho_{\Phi^+}(U^\dagger\otimes V^\dagger)(I\otimes A_i)|\psi\rangle \\ &= \max_{|\psi\rangle,U,V} \langle\psi|\sum_i (I\otimes A_i^\dagger)(UV^T\otimes I)\rho_{\Phi^+}(V^*U^\dagger\otimes I)(I\otimes A_i)|\psi\rangle \\ &= \max_{|\psi\rangle,U,V} \langle\psi|(UV^T\otimes I)\rho_{\Phi^+,\hat{\Lambda}}(V^*U^\dagger\otimes I)|\psi\rangle \\ &= \max_{|\psi\rangle}\langle\psi|\rho_{\Phi^+,\hat{\Lambda}}|\psi\rangle. \qquad (15)\end{aligned}$$

From Eqs. (14) and (15) it immediately follows that

$$F_1(\Lambda) = F(\rho_{\psi_0,\Lambda}) = \lambda_{\max}(\rho_{\Phi^+,\hat{\Lambda}}), \qquad (16)$$

where $\lambda_{\max}(\rho_{\Phi^+,\hat{\Lambda}})$ denotes the maximum eigenvalue of $\rho_{\Phi^+,\hat{\Lambda}}$ and $|\psi_0\rangle$ the corresponding eigenvector. Using the result,

$$\lambda_{\max}(\rho_{\Phi^+,\hat{\Lambda}}) = \lambda_{\max}(\rho_{\Phi^+,\Lambda}), \qquad (17)$$

proved in Lemma 5 (Sec. 1 of the Appendix), we have therefore proven that

$$F(\Lambda) \geqslant F_1(\Lambda) = \lambda_{\max}(\rho_{\Phi^+,\Lambda}). \qquad (18)$$

The following lemma now gives an upper bound on the optimal singlet fraction $F(\Lambda)$.

Lemma 1. For a qubit channel Λ,

$$F(\Lambda) \leqslant \lambda_{\max}(\rho_{\Phi^+,\Lambda}), \qquad (19)$$

where $\lambda_{\max}(\rho_{\Phi^+,\Lambda})$ denotes the maximum eigenvalue of the density matrix $\rho_{\Phi^+,\Lambda}$.

Proof. Recall that by definition, $F(\Lambda) = \max_\psi F^*(\rho_{\psi,\Lambda})$; in particular,

$$F^*(\rho_{\psi,\Lambda}) = \max_L F(L(\rho_{\psi,\Lambda})) = F(\rho^*_{\psi,\Lambda}), \qquad (20)$$

where $\rho^*_{\psi,\Lambda}$ is the state obtained from $\rho_{\psi,\Lambda}$ by *optimal* TP-LOCC associated to $\rho_{\psi,\Lambda}$. It was shown in Ref. [17] that the optimal TP-LOCC is a one-way LOCC protocol, where any of the parties apply a state dependent filter. In the case of success the other party does nothing, and in the case of failure, Alice and Bob simply prepare a separable state. We have, therefore,

$$\rho^*_{\psi,\Lambda} = p\rho_1 + (1-p)\rho_s, \qquad (21)$$

where $\rho_1 = \frac{1}{p}(A\otimes I)\rho_{\psi,\Lambda}(A^\dagger\otimes I)$ with A being the optimal filter, is the state arising with probability $p = \mathrm{Tr}[(A^\dagger A\otimes I)\rho_{\psi,\Lambda}]$ when filtering is successful and ρ_s is a separable state which Alice and Bob prepare when the filtering operation is not successful. F^* is given by [17]

$$F^*(\rho_{\psi,\Lambda}) = F(\rho^*_{\psi,\Lambda}) = pF(\rho_1) + \frac{1-p}{2} \qquad (22)$$

$$= p\langle\Phi^+|\rho_1|\Phi^+\rangle + \frac{1-p}{2}. \qquad (23)$$

Observe that the filter is applied at Alice's end, that is, on the qubit she holds and not on the qubit that was sent through the channel to Bob. In Eqs. (22) and (23), the separable state ρ_s is chosen so that $\langle\Phi^+|\rho_s|\Phi^+\rangle = \frac{1}{2}$ and optimality of the filter A implies that $F(\rho_1) = \langle\Phi^+|\rho_1|\Phi^+\rangle$ (if the latter is not the case we will get another filter unitarily connected with A which yields a higher singlet fraction). We will now show that $F(\rho_1) \leqslant \lambda_{\max}(\rho_{\Phi^+,\Lambda})$. First we observe that

$$\begin{aligned} F(\rho_1) &= \frac{1}{p}\langle\Phi^+|(A\otimes I)(I\otimes\Lambda)(|\psi\rangle\langle\psi|)(A^\dagger\otimes I)|\Phi^+\rangle \\ &= \frac{1}{p}\langle\Phi^+|(I\otimes\Lambda)[(A\otimes I)|\psi\rangle\langle\psi|(A^\dagger\otimes I)]|\Phi^+\rangle. \end{aligned} \qquad (24)$$

On the other hand, because Λ is a trace-preserving map, we also observe that

$$\begin{aligned} p &= \mathrm{Tr}[(A^\dagger A\otimes I)\rho_{\psi,\Lambda}] \\ &= \mathrm{Tr}\{(I\otimes\Lambda)[(A^\dagger A\otimes I)|\psi\rangle\langle\psi|]\} \\ &= \mathrm{Tr}[(A^\dagger A\otimes I)|\psi\rangle\langle\psi|]. \end{aligned} \qquad (25)$$

We thus have $\rho_1 = (I\otimes\Lambda)(|\psi'\rangle\langle\psi'|)$ and thereby from Eqs. (24) and (25) we get

$$\begin{aligned} F(\rho_1) &= \langle\Phi^+|(I\otimes\Lambda)(|\psi'\rangle\langle\psi'|)|\Phi^+\rangle \\ &= F(\rho_{\psi',\Lambda}), \end{aligned} \qquad (26)$$

where $|\psi'\rangle = \frac{1}{\sqrt{q}}(A\otimes I)|\psi\rangle$ is a normalized vector with $q = p = \langle\psi|(A^\dagger A\otimes I)|\psi\rangle$. Hence from Eqs. (11), (18), and (26) we have,

$$F(\rho_1) \leqslant F_1(\Lambda) = \lambda_{\max}(\rho_{\Phi^+,\Lambda}). \qquad (27)$$

Thus from Eq. (23) we have

$$\begin{aligned} F^*(\rho_{\psi,\Lambda}) &\leqslant p\lambda_{\max}(\rho_{\Phi^+,\Lambda}) + \frac{1-p}{2} \\ &\leqslant \lambda_{\max}(\rho_{\Phi^+,\Lambda}). \end{aligned} \qquad (28)$$

The last inequality follows from the fact that $\lambda_{\max}(\rho_{\Phi^+,\Lambda}) > 1/2$ [as the channel is not entanglement breaking, this follows by applying Lemma 6 (Sec. 2 of the Appendix) on $\sigma_{AB} = \rho_{\Phi^+,\Lambda}$].

Since inequality (28) holds for any transmitted pure state $|\psi\rangle$, we therefore conclude that

$$F(\Lambda) \leqslant \lambda_{\max}(\rho_{\Phi^+,\Lambda}). \tag{29}$$

This completes the proof of Lemma 1. ∎

From Eqs. (18) and (19) we have, $F(\Lambda) = \lambda_{\max}(\rho_{\Phi^+,\Lambda})$. Now, as $F(\Lambda) \geqslant F^*(\rho_{\psi_0,\Lambda}) \geqslant F(\rho_{\psi_0,\Lambda})$ from Eqs. (16) and (18) we have

$$F(\Lambda) = F^*(\rho_{\psi_0,\Lambda}) = F(\rho_{\psi_0,\Lambda}). \tag{30}$$

This completes the proof of Theorem 1. ∎

What can we say about $|\psi_0\rangle$? The evidence so far is mixed: $|\psi_0\rangle$ can be either maximally entangled (e.g., for depolarizing channel [9]) or nonmaximally entangled (e.g., for amplitude damping channel [14]), but the answer for a generic qubit channel is not known. The following result completely characterizes the channels for which $|\psi_0\rangle$ is maximally entangled and for which it is not.

Theorem 2. The state $|\psi_0\rangle$, as defined in Theorem 1, is maximally entangled if and only if the channel Λ is unital.

Proof. Recall that $|\psi_0\rangle$ is the eigenvector corresponding to the maximum eigenvalue of $\rho_{\Phi^+,\hat{\Lambda}}$. Let $|\psi_0'\rangle$ be the eigenvector corresponding to the maximum eigenvalue of $\rho_{\Phi^+,\Lambda}$. The following lemma establishes the correspondence between the vectors $|\psi_0\rangle$ and $|\psi_0'\rangle$.

Lemma 2. Let V be the swap operator defined by the action $V|\eta\rangle|\chi\rangle = |\chi\rangle|\eta\rangle$. Then $V|\psi_0\rangle^* = |\psi_0'\rangle$.

Proof. Let us now consider the spectral decomposition of $\rho_{\Phi^+,\Lambda}$:

$$\rho_{\Phi^+,\Lambda} = \sum_{k=0}^{3} p_k |\psi_k'\rangle\langle\psi_k'|. \tag{31}$$

From Eq. (A5) in the Appendix we have

$$\rho_{\Phi^+,\hat{\Lambda}} = \sum_{k=0}^{3} \lambda_k (V^\dagger|\psi_k'\rangle\langle\psi_k'|V)^*. \tag{32}$$

For different values of k, $(V^\dagger|\psi_k'\rangle)^*$'s are orthogonal as V is unitary.

Hence we see that Eq. (32) is in fact a spectral decomposition of $\rho_{\Phi^+,\hat{\Lambda}}$ with eigenvectors

$$|\psi_k\rangle = (V^\dagger|\psi_k'\rangle)^*. \tag{33}$$

The Schmidt coefficients of $|\psi_k'\rangle$ are the same as that of $|\psi_k\rangle$. The entanglement of $|\psi_k'\rangle$ is thus also the same as that of $|\psi_\alpha\rangle$.

Let $|\psi_0'\rangle$ be the eigenvector corresponding to the maximum eigenvalue of $\rho_{\Phi^+,\Lambda}$. We have from Eq. (33),

$$|\psi_0\rangle = (V^\dagger|\psi_0'\rangle)^*. \tag{34}$$

This completes the proof of Lemma 2. ∎

Therefore, if $|\psi_0'\rangle$ is maximally entangled, then so is $|\psi_0\rangle$ and vice versa. We will prove the theorem by showing that $|\psi_0'\rangle$ is maximally entangled if and only if Λ is unital.

We first show that if $|\psi_0'\rangle$ is maximally entangled then Λ must be unital. We first note that the Kraus operators of the channel Λ can be obtained from the action of the channel on the maximally entangled state $|\Phi^+\rangle$.

Now for every k, we can write $|\psi_k'\rangle$ [appeared in Eq. (31)] as

$$|\psi_k'\rangle = (I \otimes G_k)|\Phi^+\rangle, \tag{35}$$

where G_k is a 2×2 complex matrix. It was shown in Ref. [9] that the channel Λ can be described in terms of the Kraus operators $\{\sqrt{p_k}G_k\}$. Noting that (a) $\langle\psi_i'|\psi_j'\rangle = \delta_{ij}$, and (b) for any operator O, $\langle\Phi^+|I\otimes O|\Phi^+\rangle = \frac{1}{2}\mathrm{Tr}\, O$, it follows that the Kraus operators $\{\sqrt{p_k}G_k\}$ are trace orthogonal. That is,

$$\mathrm{Tr}\, A_k^\dagger A_l = 2\sqrt{p_k p_l}\,\delta_{kl}, \tag{36}$$

where $A_k = \sqrt{p_k}G_k$. The Kraus operators thus obtained through the spectral decomposition of $\rho_{\Phi^+,\Lambda}$ are trace orthogonal. They also satisfy $\sum A_k^\dagger A_k = I$, as Λ is a trace-perserving completely positive (TPCP) map.

Suppose now the channel Λ is nonunital, i.e., $\Lambda(I) \neq I$. This implies that

$$\sum A_k A_k^\dagger \neq I. \tag{37}$$

None of our considerations change if we consider a channel $U \circ \Lambda$ with Kraus operators UA_k where $U \in \mathrm{SU}(2)$. This is because the eigenvectors of $\rho_{\Phi^+,\Lambda}$ and $\rho_{\Phi^+,U\Lambda}$ are local unitarily connected and eigenvalues are the same. Let us now assume that one of the eigenstates ($|\psi_0'\rangle$, say) in the spectral decomposition of $\rho_{\Phi^+,\Lambda}$ in Eq. (31) is maximally entangled. This necessarily implies one of the Kraus operators (namely, A_0) is proportional to a unitary. Now because of the postprocessing freedom, without any loss of generality we can take A_0 to be $\sqrt{p}I$, with $p \in [0,1]$. Due to trace orthogonality [Eq. (36)] we will have

$$\mathrm{Tr}(A_k) = 0, \qquad \text{for} \quad k = 1,2,3. \tag{38}$$

We can thus take $A_k = \vec{\alpha_k}\cdot\vec{\sigma}$, where $\vec{\alpha_k} \in \mathbb{C}^3$ and $\vec{\sigma} = \{\sigma_x,\sigma_y,\sigma_z\}$, for $k = 1,2,3$. On using $(\vec{\sigma}\cdot\vec{a})(\vec{\sigma}\cdot\vec{b}) = (\vec{a}\cdot\vec{b})I + i\vec{\sigma}\cdot(\vec{a}\times\vec{b})$ the trace preservation condition $\sum A_k^\dagger A_k = I$ now becomes

$$pI + \sum_{k=1}^{3}(\vec{\alpha_k}^*\cdot\vec{\alpha_k})I + i(\vec{\alpha_k}^*\times\vec{\alpha_k})\cdot\vec{\sigma} = I, \tag{39}$$

from which we obtain

$$p + \sum_{k=1}^{3}(\vec{\alpha_k}^*\cdot\vec{\alpha_k}) = 1,$$
$$\sum_{k=1}^{3}\vec{\alpha_k}^*\times\vec{\alpha_k} = 0. \tag{40}$$

On the other hand, the condition for nonunitality [Eq. (37)] of the channel gives us

$$pI + \sum_{k=1}^{3}(\vec{\alpha_k}^*\cdot\vec{\alpha_k})I - i(\vec{\alpha_k}^*\times\vec{\alpha_k})\cdot\vec{\sigma} \neq I, \tag{41}$$

which is clearly in contradiction with Eq. (40). Thus $\rho_{\Phi^+,\Lambda}$ cannot have a maximally entangled eigenvector if Λ is nonunital. Hence, $|\psi_0'\rangle$ is not maximally entangled. Therefore it follows that if $|\psi_0\rangle$ is maximally entangled, then the channel must be unital.

We will now show that if Λ is unital, then $|\psi_0'\rangle$ is maximally entangled. In [18] it was proved that that for any unital qubit channel Λ, $\rho_{\Phi^+,\Lambda}$ is local unitarily connected to the Bell-diagonal state $\sum_{i=0}^{3} p_i(I\otimes\sigma_i)|\Phi^+\rangle\langle\Phi^+|(I\otimes\sigma_i)$ with $\sigma_0 = I$, $1 \geqslant p_i \geqslant 0$, and $\sum_i p_i = 1$. It immediately follows that $|\psi_0'\rangle$ is maximally entangled. This completes the proof of Theorem 2. ■

III. OPTIMAL SINGLET FRACTION AND THE MAXIMUM OUTPUT NEGATIVITY

Here we show that $F(\Lambda)$ is related to the negativity of the density matrix $\rho_{\Phi^+,\Lambda}$. We first note that an upper bound on $F^*(\rho_{\psi,\Lambda})$ can be given in terms of its negativity [10] $N(\rho_{\psi,\Lambda})$:

$$F^*(\rho_{\psi,\Lambda}) \leqslant \tfrac{1}{2}[1 + N(\rho_{\psi,\Lambda})], \tag{42}$$

where $N(\rho_{\psi,\Lambda}) = \max\{0, -2\lambda_{\min}(\rho^{\Gamma}_{\psi,\Lambda})\}$ and $\rho^{\Gamma}_{\psi,\Lambda}$ is the partially transposed matrix obtained from $\rho_{\psi,\Lambda}$. Maximizing over all input states $|\psi\rangle$ we get

$$F(\Lambda) \leqslant \tfrac{1}{2}[1 + N(\Lambda)], \tag{43}$$

where $N(\Lambda) = \max_{\psi} N(\rho_{\psi,\Lambda})$. An interesting question here is, does the optimal singlet fraction always reach the above upper bound for all channels Λ? In order to answer this question, we first prove the following:

Lemma 3. For a qubit channel Λ, the optimal singlet fraction $F(\Lambda)$ is related to the negativity $N(\rho_{\Phi^+,\Lambda})$ of the state $\rho_{\Phi^+,\Lambda}$ by the following relation:

$$F(\Lambda) = \tfrac{1}{2}[1 + N(\rho_{\Phi^+,\Lambda})]. \tag{44}$$

Proof. The proof follows by using the formula of negativity, simple application of Lemma 6 (see Sec. 2 of the Appendix) and Theorem 1:

$$\begin{aligned}\tfrac{1}{2}[1 + N(\rho_{\Phi^+,\Lambda})] &= \tfrac{1}{2}\left[1 - 2\lambda_{\min}\left(\rho^{\Gamma}_{\Phi^+,\Lambda}\right)\right]\\ &= \lambda_{\max}(\rho_{\Phi^+,\Lambda}) = F(\Lambda).\end{aligned} \tag{45}$$

This completes the proof of Lemma 3. ■

Next we show that $F(\Lambda)$ does not reach the upper bound in Eq. (43) for all nonunital channels as there are examples for which $N(\Lambda) > N(\rho_{\Phi^+,\Lambda})$. Thus, even though the ordering of negativity may change under one-sided channel action, $I\otimes\Lambda$ the optimal singlet fraction obeys the bound in Eq. (42) for maximally entangled input. For unital channels, however, as the next lemma shows, we have $N(\Lambda) = N(\rho_{\Phi^+,\Lambda})$.

Lemma 4. For unital qubit channels we have $N(\Lambda) = N(\rho_{\Phi^+,\Lambda})$.

Proof. The most general two-qubit pure state in the Schmidt form is given by $|\alpha\rangle = \sqrt{\lambda}|e_1 f_1\rangle + \sqrt{1-\lambda}|e_2 f_2\rangle = (U\otimes V)[\sqrt{\lambda}|00\rangle + \sqrt{(1-\lambda)}|11\rangle]$, with $\lambda\in[0,1]$ and the 2×2 unitary matrices U and V being given by $U|0\rangle = |e_1\rangle$, $V|0\rangle = |f_1\rangle$, $U|1\rangle = |e_2\rangle$, and $V|1\rangle = |f_2\rangle$.

For $\lambda\in[0,1]$, let

$$W_\lambda = \sqrt{\lambda}|0\rangle\langle 0| + \sqrt{(1-\lambda)}|1\rangle\langle 1|. \tag{46}$$

Now using the fact that Λ is a trace-preserving map it is easy to show that

$$\begin{aligned}\rho_{\alpha,\Lambda} &= (I\otimes\Lambda)(|\alpha\rangle\langle\alpha|)\\ &= \frac{(A_1\otimes I)\rho_{\Phi^+,\Lambda}(A_1^\dagger\otimes I)}{\mathrm{Tr}[(A_1^\dagger A_1\otimes I)\rho_{\Phi^+,\Lambda}]},\end{aligned} \tag{47}$$

with the filter $A_1 = UW_\lambda V^T$.

For a unital channel Λ, $\rho_{\Phi^+,\Lambda}$ is locally unitarily connected to a Bell-diagonal state (see proof of Theorem 2). In Ref. [19] it was shown that negativity of a Bell-diagonal state (and hence, any state locally unitarily connected to it) cannot be increased by local filtering. Hence, from Eq. (47) for a unital qubit channel Λ we have

$$N(\Lambda) = N(\rho_{\Phi^+,\Lambda}). \tag{48}$$

This completes the proof of Lemma 4. ■

Example of channel for which $N(\Lambda) > N(\rho_{\Phi^+,\Lambda})$

Let us consider the amplitude damping channel, with Kraus operators

$$K_0 = \begin{pmatrix}1 & 0\\ 0 & \sqrt{1-p}\end{pmatrix} \quad\text{and}\quad K_1 = \begin{pmatrix}0 & \sqrt{p}\\ 0 & 0\end{pmatrix}$$

with $1\geqslant p\geqslant 0$. The channel is nonunital.

It was shown in [14] that the optimal input state for attaining the optimal singlet fraction of the channel is given by $|\chi\rangle = \frac{1}{\sqrt{(2-p)}}|00\rangle + \sqrt{\frac{1-p}{2-p}}|11\rangle$.

Using Theorem 1 for the amplitude damping channel Λ, we therefore get $F(\Lambda) = \lambda_{\max}(\rho_{\Phi^+,\Lambda}) = F^*(\rho_{\chi,\Lambda}) = F(\rho_{\chi,\Lambda})$. Now from Eq. (42) we get $F^*(\rho_{\chi,\Lambda}) \leqslant \frac{1}{2}[1 + N(\rho_{\chi,\Lambda})]$, while from Lemma 3 we get $F(\Lambda) = \frac{1}{2}[1 + N(\rho_{\Phi^+,\Lambda})]$. Hence we must have $N(\rho_{\Phi^+,\Lambda}) \leqslant N(\rho_{\chi,\Lambda})$.

For the amplitude damping channels for input states $|\phi(\lambda)\rangle = \sqrt{\lambda}|00\rangle + \sqrt{(1-\lambda)}|11\rangle$ ($\lambda\in[0,1]$) we have

$$N(\rho_{\phi(\lambda),\Lambda}) = \sqrt{p^2(1-\lambda)^2 + 4\lambda(1-\lambda)(1-p)} - (1-\lambda)p. \tag{49}$$

Thus,

$$N(\rho_{\Phi^+,\Lambda}) = \sqrt{\left(\frac{p^2}{4} + 1 - p\right)} - \frac{p}{2}$$

and

$$N(\rho_{\phi(1/(2-p)),\Lambda}) = \frac{1-p}{2-p}(\sqrt{p^2+4} - p).$$

It is easy to see that $N(\rho_{\Phi^+,\Lambda}) < N(\rho_{\phi(1/(2-p)),\Lambda})$ for all $1 > p > 0$ and hence $N(\rho_{\Phi^+,\Lambda}) < N(\Lambda)$.

IV. NONUNITAL CHANNELS AND MAXIMALLY ENTANGLED INPUT

It is important to recognize that Theorems 1 and 2 put together only prescribes a method to attain the optimal singlet fraction. It does not, however, rule out the possibility that the optimal singlet fraction for a nonunital channel may still be attained by sending part of a maximally entangled state followed by local postprocessing. As it turns out this is not the case.

Theorem 3. For a nonunital qubit channel Λ,

$$F^*(\rho_{\Phi^+,\Lambda}) < F(\Lambda). \tag{50}$$

Proof. Using the bound in Eq. (42) for the density matrix $\rho_{\Phi^+,\Lambda}$ we have

$$F^*(\rho_{\Phi^+,\Lambda}) \leqslant \tfrac{1}{2}[1 + N(\rho_{\Phi^+,\Lambda})]. \tag{51}$$

It follows from Lemma 3 that to prove Theorem 3 it suffices to show that for a nonunital channel Λ,

$$F^*(\rho_{\Phi^+,\Lambda}) < \tfrac{1}{2}[1 + N(\rho_{\Phi^+,\Lambda})]. \tag{52}$$

As shown in [17], for any two-qubit density matrix ρ the optimal fidelity $F^*(\rho)$ can be found by solving the following convex semidefinite program:

$$\text{maximize} \quad F^* = \tfrac{1}{2} - \mathrm{Tr}(X\rho^\Gamma), \tag{53}$$

under the constraints

$$0 \leqslant X \leqslant I_4, \tag{54}$$

$$-\frac{I_4}{2} \leqslant X^\Gamma \leqslant \frac{I_4}{2}, \tag{55}$$

with X^Γ being the partial transpose of X. In addition, the optimal X is known to be of rank one.

The proof is now by contradiction. Suppose that $F^*(\rho_{\Phi^+,\Lambda}) = \frac{1}{2}[1 + N(\rho_{\Phi^+,\Lambda})]$; thus to achieve this equality we must necessarily have

$$\tfrac{1}{2} - \mathrm{Tr}(X_{\mathrm{opt}}\rho^\Gamma_{\Phi^+,\Lambda}) = \tfrac{1}{2}[1 + N(\rho_{\Phi^+,\Lambda})], \tag{56}$$

from which it follows that

$$\mathrm{Tr}(X_{\mathrm{opt}}\rho^\Gamma_{\Phi^+,\Lambda}) = -\frac{N(\rho_{\Phi^+,\Lambda})}{2} = \lambda_{\min}(\rho^\Gamma_{\Phi^+,\Lambda}). \tag{57}$$

Using the facts that X_{opt} is a positive rank-one operator (proved in [17]) and there is only one negative eigenvalue for $\rho^\Gamma_{\Phi^+,\Lambda}$ (which means $\lambda_{\min}$ is negative), we obtain

$$X_{\mathrm{opt}} = |\alpha\rangle\langle\alpha|, \tag{58}$$

where $\rho^\Gamma|\alpha\rangle = \lambda_{\min}(\rho^\Gamma)|\alpha\rangle$. Clearly X_{opt} in the above equation is of rank one and satisfies $0 \leqslant X \leqslant I_4$. As eigenvalues of X and X^Γ are invariant under local unitaries it is sufficient to take

$$X = \mathbf{P}[\sqrt{\lambda}|00\rangle + \sqrt{(1-\lambda)}|11\rangle], \tag{59}$$

with $\mathbf{P}[|a\rangle]$ denoting projector on $|a\rangle$ and $\lambda \in (0,1)$.

The spectrum of X^Γ for X in Eq. (59) is given by

$$\lambda(X^\Gamma) = \lambda, (1-\lambda), \pm\sqrt{\lambda(1-\lambda)}. \tag{60}$$

Thus the constraint (55) is only satisfied for $\lambda = \frac{1}{2}$, i.e, if $|\alpha\rangle$ is maximally entangled. Therefore, under the assumption $F^*(\rho_{\Phi^+,\Lambda}) = \frac{1}{2}[1 + N(\rho_{\Phi^+,\Lambda})]$, the eigenvector $|\alpha\rangle$ corresponding to the negative eigenvalue $\lambda_{\min}(\rho^\Gamma_{\Phi^+,\Lambda})$ is maximally entangled.

But then this implies that

$$F(\rho_{\Phi^+,\Lambda}) = \tfrac{1}{2}[1 + N(\rho_{\Phi^+,\Lambda})] = \lambda_{\max}(\rho_{\Phi^+,\Lambda}) \tag{61}$$

because for any two-qubit entangled density matrix σ, $F(\sigma) = \frac{1}{2}[1 + N(\sigma)]$ if and only if the eigenvector corresponding to the negative eigenvalue of σ^Γ is maximally entangled [10]. The last equality in Eq. (61) follows from Eq. (45).

Now from Theorem 1 we have

$$F(\Lambda) = F(\rho_{\psi_0,\Lambda}) = \lambda_{\max}(\rho_{\Phi^+,\Lambda}), \tag{62}$$

where $|\psi_0\rangle$ is the eigenvector corresponding to the maximum eigenvalue of $\rho_{\Phi^+,\hat{\Lambda}}$. Now from Theorem 2 we know that $|\psi_0\rangle$ is necessarily nonmaximally entangled when the channel Λ is nonunital. Thus for a nonunital channel Λ,

$$F(\rho_{\Phi^+,\Lambda}) < F(\Lambda) = \lambda_{\max}(\rho_{\Phi^+,\Lambda}), \tag{63}$$

which contradicts Eq. (61). This completes the proof of Theorem 3. ■

V. CONCLUSIONS

Shared entanglement is a critical resource for quantum information processing tasks such as quantum teleportation. Typically, quantum entanglement is shared by sending part of a pure entangled state through a quantum channel which, in practice, is noisy. This results in mixed entangled states, purity of which is characterized by a singlet fraction. Because faithful implementation of quantum information processing tasks require near-perfect entangled states (states with very high purity), a basic question is the following: What is the optimal singlet fraction attainable for a single use of a quantum channel Λ and trace-preserving local operations?

In this paper, we obtained an exact expression of the optimal singlet fraction for a qubit channel and prescribed a protocol to attain the optimal value. The protocol consists of sending part of a pure entangled state $|\psi_0\rangle$ through the channel, where $|\psi_0\rangle$ is given by the eigenvector corresponding to the maximum eigenvalue of the density matrix $\rho_{\Phi^+,\hat{\Lambda}}$ ($\hat{\Lambda}$ is the channel dual to the qubit channel Λ). We have also shown that this "best" state $|\psi_0\rangle$ is maximally entangled for unital channels but must be nonmaximally entangled if the channel is nonunital. Interestingly, we find that in the optimal case no local postprocessing is required even though it is known that TP-LOCC can increase the singlet fraction of a density matrix.

We would also like to mention that recent results [20–22] have shown that generalized quantum correlations play an essential role in distribution of entanglement via separable states. In this setting, the carrier, which always remains separable with the rest of the system, is transmitted through a noiseless quantum channel, whereas in practice channels are noisy. We therefore expect our results to be useful in a more general treatment of the aforementioned scheme of entanglement distribution involving noisy quantum channels.

ACKNOWLEDGMENT

R.P. thanks Ajit Iqbal Singh for useful discussions.

APPENDIX

1. Technical lemma

Lemma 5. $\lambda_{\max}(\rho_{\Phi^+,\hat{\Lambda}}) = \lambda_{\max}(\rho_{\Phi^+,\Lambda})$.

Proof. We first obtain a relationship between the states $\rho_{\Phi^+,\Lambda}$ and $\rho_{\Phi^+,\hat{\Lambda}}$. Recall that these states are given by

$$\rho_{\Phi^+,\Lambda} = \sum_i (I \otimes A_i)|\Phi^+\rangle\langle\Phi^+|(I \otimes A_i^\dagger), \tag{A1}$$

$$\rho_{\Phi^+,\hat{\Lambda}} = \sum_i (I \otimes A_i^\dagger)|\Phi^+\rangle\langle\Phi^+|(I \otimes A_i). \tag{A2}$$

Equation (A2) can be written as

$$\rho_{\Phi^+,\hat{\Lambda}} = \sum_i [(A_i^\dagger)^T \otimes I]|\Phi^+\rangle\langle\Phi^+|\big(A_i^T \otimes I\big),$$

$$\Rightarrow \rho^*_{\Phi^+,\hat{\Lambda}} = \sum_i (A_i \otimes I)|\Phi^+\rangle\langle\Phi^+|(A_i^\dagger \otimes I), \tag{A3}$$

where the complex conjugation is taken with respect to the computational basis $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$. Now using the SWAP operator V defined by the action $V|ij\rangle = |ji\rangle$, we have

$$(A_i \otimes I)|\Phi^+\rangle = \frac{1}{\sqrt{2}}\sum_{k=0}^{1} A_i|k\rangle \otimes |k\rangle \quad \text{and so,}$$

$$V(A_i \otimes I)|\Phi^+\rangle = \frac{1}{\sqrt{2}}\sum_{k=0}^{1} |k\rangle \otimes A_i|k\rangle$$

$$= (I \otimes A_i)|\Phi^+\rangle. \tag{A4}$$

Hence,

$$\rho^*_{\Phi^+,\hat{\Lambda}} = V^\dagger \rho_{\Phi^+,\Lambda} V,$$

$$\Rightarrow \rho_{\Phi^+,\hat{\Lambda}} = (V^\dagger \rho_{\Phi^+,\Lambda} V)^*. \tag{A5}$$

From the above equation it therefore follows that

$$\lambda_{\max}(\rho_{\Phi^+,\hat{\Lambda}}) = \lambda_{\max}(\rho_{\Phi^+,\Lambda}). \tag{A6}$$

This completes the proof of Lemma 5. ■

Note that Lemma 5 does not assume that Λ is a qubit channel. Also, from Eq. (A5) it is clear that $\rho_{\Phi^+,\hat{\Lambda}}$ is a valid state even for a nonunital channel Λ (and so, the dual channel $\hat{\Lambda}$ is not trace preserving). But we will get unnormalized states if the dual channel acts on one side of some nonmaximally entangled states.

2. Technical lemma

Lemma 6. Let $\sigma_{AB} \in \mathbb{C}^2 \otimes \mathbb{C}^2$ be a bipartite density matrix such that $\mathrm{Tr}_B(\sigma_{AB}) = \frac{1}{2}I$. Then,

$$\lambda_{\min}(\sigma_{AB}^\Gamma) + \lambda_{\max}(\sigma_{AB}) = \tfrac{1}{2}, \tag{A7}$$

where $\lambda_{\min}(X)$ and $\lambda_{\max}(X)$ denote the minimum and maximum eigenvalue of $X \in \{\sigma_{AB},\sigma_{AB}^\Gamma\}$ and Γ denotes partial transposition.

Proof. Let $\sigma_{AB} \in \mathbb{C}^2 \otimes \mathbb{C}^2$ be a bipartite density matrix such that $\mathrm{Tr}_B(\sigma_{AB}) = \frac{1}{2}I$. From the Choi-Jamiolkowski isomorphism ([23,24]) we have that σ_{AB} can be written as

$$\sigma_{AB} = (I \otimes \Lambda)(|\Phi^+\rangle_{AB}\langle\Phi^+|),$$

where Λ is a TPCP map, mapping $\mathscr{B}(\mathbb{C}^2)$ to itself.

In [18] it was shown that any such map Λ can be written as

$$\Lambda(\rho) = (U_1 \circ \Lambda' \circ U_2)(\rho) \quad \text{for all} \quad \rho \in \mathscr{B}(\mathbb{C}^2) \tag{A8}$$

with Λ' being a canonical TPCP map and U_1 and U_2 being unitary maps. If $\rho = \frac{1}{2}(I + x\sigma_1 + y\sigma_2 + z\sigma_3)$ and $\rho' = \Lambda'(\rho) = \frac{1}{2}(I + x'\sigma_1 + y'\sigma_2 + z'\sigma_3)$, then in the Bloch sphere representation the map Λ' is given by

$$\begin{bmatrix} 1 \\ x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ t_1 & \lambda_1 & 0 & 0 \\ t_2 & 0 & \lambda_2 & 0 \\ t_3 & 0 & 0 & \lambda_3 \end{bmatrix} \begin{bmatrix} 1 \\ x \\ y \\ z \end{bmatrix}, \tag{A9}$$

with t_i and λ_i being real for all i.

Now as local unitaries do not affect the eigenvalues of σ_{AB} or σ_{AB}^Γ, for the rest of the proof we can focus on $(I \otimes \Lambda')(|\Phi^+\rangle\langle\Phi^+|) = \rho_{\Phi^+,\Lambda'}$ with the map Λ' given by Eq. (A9). We have

$$\rho_{\Phi^+,\Lambda'} = \frac{1}{2}\begin{bmatrix} a & b & 0 & d \\ b^* & (1-a) & f & 0 \\ 0 & f & c & b \\ d & 0 & b^* & (1-c) \end{bmatrix}, \tag{A10}$$

with $a = \frac{1+t_3+\lambda_3}{2}$, $b = \frac{t_1 - it_2}{2}$, $d = \frac{(\lambda_1+\lambda_2)}{2}$, $f = \frac{(\lambda_1-\lambda_2)}{2}$, and $c = \frac{(1+t_3-\lambda_3)}{2}$. Now complete positivity of Λ' implies positivity of $\rho_{\Phi^+,\Lambda'}$ and hence the spectrum of $\rho_{\Phi^+,\Lambda'}$ is same as that of $\rho^*_{\Phi^+,\Lambda'}$. Now the eigenvalue equation of $\rho^*_{\Phi^+,\Lambda'}$ is

$$\begin{vmatrix} \left(\frac{a}{2} - \lambda\right) & \frac{b^*}{2} & 0 & \frac{d}{2} \\ \frac{b}{2} & \left(\frac{1-a}{2} - \lambda\right) & \frac{f}{2} & 0 \\ 0 & \frac{f}{2} & \left(\frac{c}{2} - \lambda\right) & \frac{b^*}{2} \\ \frac{d}{2} & 0 & \frac{b}{2} & \left(\frac{(1-c)}{2} - \lambda\right) \end{vmatrix} = 0. \tag{A11}$$

Now, the partial transpose with respect to the first party of $\rho_{\Phi^+,\Lambda'}$ is given by

$$\rho^\Gamma_{\Phi^+,\Lambda'} = \frac{1}{2}\begin{bmatrix} a & b & 0 & f \\ b^* & (1-a) & d & 0 \\ 0 & d & c & b \\ f & 0 & b^* & (1-c) \end{bmatrix}. \tag{A12}$$

The eigenvalue equation of $\rho^\Gamma_{\Phi^+,\Lambda'}$ is given by

$$\begin{vmatrix} \left(\frac{a}{2} - \lambda\right) & \frac{b}{2} & 0 & \frac{f}{2} \\ \frac{b^*}{2} & \left(\frac{(1-a)}{2} - \lambda\right) & \frac{d}{2} & 0 \\ 0 & \frac{d}{2} & \left(\frac{c}{2} - \lambda\right) & \frac{b}{2} \\ \frac{f}{2} & 0 & \frac{b^*}{2} & \left(\frac{(1-c)}{2} - \lambda\right) \end{vmatrix} = 0. \tag{A13}$$

Replacing λ by $(\frac{1}{2}-\lambda')$, in Eq. (A13) we have

$$\begin{vmatrix} -\left(\frac{(1-a)}{2}-\lambda'\right) & \frac{b}{2} & 0 & \frac{f}{2} \\ \frac{b^*}{2} & -\left(\frac{a}{2}-\lambda'\right) & \frac{d}{2} & 0 \\ 0 & \frac{d}{2} & -\left(\frac{(1-c)}{2}-\lambda'\right) & \frac{b}{2} \\ \frac{f}{2} & 0 & \frac{b^*}{2} & -\left(\frac{c}{2}-\lambda'\right) \end{vmatrix} = 0. \tag{A14}$$

In Eq. (A14) performing the interchanges, column 1 $\Leftrightarrow$ column 2 and column 3 $\Leftrightarrow$ column 4, we have

$$\begin{vmatrix} \frac{b}{2} & -\left(\frac{(1-a)}{2}-\lambda'\right) & \frac{f}{2} & 0 \\ -\left(\frac{a}{2}-\lambda'\right) & \frac{b^*}{2} & 0 & \frac{d}{2} \\ \frac{d}{2} & 0 & \frac{b}{2} & -\left(\frac{(1-c)}{2}-\lambda'\right) \\ 0 & \frac{f}{2} & -\left(\frac{c}{2}-\lambda'\right) & \frac{b^*}{2} \end{vmatrix} = 0. \tag{A15}$$

In Eq. (A15) performing the interchanges, row 1 $\Leftrightarrow$ row 2 and row 3 $\Leftrightarrow$ row 4, we have

$$\begin{vmatrix} -\left(\frac{a}{2}-\lambda'\right) & \frac{b^*}{2} & 0 & \frac{d}{2} \\ \frac{b}{2} & -\left(\frac{(1-a)}{2}-\lambda'\right) & \frac{f}{2} & 0 \\ 0 & \frac{f}{2} & -\left(\frac{c}{2}-\lambda'\right) & \frac{b^*}{2} \\ \frac{d}{2} & 0 & \frac{b}{2} & -\left(\frac{(1-c)}{2}-\lambda'\right) \end{vmatrix} = 0. \tag{A16}$$

Now multiplying the first row by -1, the second column by -1, the third row by -1 and, the fourth column by -1 successively in Eq. (A16) we get back Eq. (A11). Thus if eigenvalues of $\rho_{\Phi^+,\Lambda'}$ are λ_i with $i=1,2,3,4$, those of $\rho^{\Gamma}_{\Phi^+,\Lambda'}$ are $(\frac{1}{2}-\lambda_i)$. Thus we have

$$\begin{aligned} \lambda_{\min}(\rho^{\Gamma}_{\Phi^+,\Lambda'}) &= \tfrac{1}{2}-\lambda_{\max}(\rho_{\Phi^+,\Lambda'}), \\ \Rightarrow \lambda_{\min}(\rho^{\Gamma}_{\Phi^+,\Lambda'})+\lambda_{\max}(\rho_{\Phi^+,\Lambda'}) &= \tfrac{1}{2}, \\ \Rightarrow \lambda_{\min}(\sigma^{\Gamma}_{AB})+\lambda_{\max}(\sigma_{AB}) &= \tfrac{1}{2}. \end{aligned} \tag{A17}$$

This completes the proof of Lemma 6. ■

[1] C. H. Bennett and Stephen J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] H. Buhrman and H. Röhrig, in *Distributed Quantum Computing*, Lecture Notes in Computer Science Vol. 2747 (Springer, New York, 2003), pp. 1–20.
[4] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[5] C. H. Bennett, D. P. Divincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[6] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[7] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[8] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
[9] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).
[10] F. Verstraete and H. Verschelde, Phys. Rev. A **66**, 022307 (2002).
[11] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).
[12] H. Barnum, M. A. Nielsen, and B. Schumacher, Phys. Rev. A **57**, 4153 (1998).
[13] E. Schrödinger, Naturwissenschaften **23**, 807 (1935); For a recent review, see R. Horodecki, P. Horodecki. M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[14] S. Bandyopadhyay and A. Ghosh, Phys. Rev. A **86**, 020304(R) (2012).
[15] P. Badziag, M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **62**, 012311 (2000).
[16] S. Bandyopadhyay, Phys. Rev. A **65**, 022302 (2002).
[17] F. Verstraete and H. Verschelde, Phys. Rev. Lett. **90**, 097901 (2003).
[18] M. B. Ruskai, S. Szarek, and E. Werner, Linear Algebra Appl. **347**, 159 (2002).
[19] F. Verstraete, K. Audenaert, J. Dehaene, and B. De Moor, J. Phys. A: Math. Gen. **34**, 10327 (2001).
[20] A. Streltsov, H. Kampermann, and D. Bruss, Phys. Rev. Lett. **108**, 250501 (2012).
[21] T. K. Chuan, J. Maillard, K. Modi, T. Paterek, M. Paternostro, and M. Piani, Phys. Rev. Lett. **109**, 070501 (2012).
[22] A. Kay, Phys. Rev. Lett. **109**, 080503 (2012).
[23] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).
[24] M. D Choi, Linear Algebra Appl. **10**, 285 (1975).