Symmetric extension of two-qubit states

Jianxin Chen,[1,2,3] Zhengfeng Ji,[2,4] David Kribs,[1,2] Norbert Lütkenhaus,[2,5] and Bei Zeng[1,2,5]
[1]*Department of Mathematics and Statistics, University of Guelph, Guelph, Ontario, Canada*
[2]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada*
[3]*UTS-AMSS Joint Research Laboratory for Quantum Computation and Quantum Information Processing, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China*
[4]*State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, China*
[5]*Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada*
(Received 3 January 2014; published 17 September 2014)

A bipartite state ρ_{AB} is symmetric extendible if there exists a tripartite state $\rho_{ABB'}$ whose AB and AB' marginal states are both identical to ρ_{AB}. Symmetric extendibility of bipartite states is of vital importance in quantum information because of its central role in separability tests, one-way distillation of Einstein-Podolsky-Rosen pairs, one-way distillation of secure keys, quantum marginal problems, and antidegradable quantum channels. We establish a simple analytic characterization for symmetric extendibility of any two-qubit quantum state ρ_{AB}; specifically, $\mathrm{tr}(\rho_B^2) \geqslant \mathrm{tr}(\rho_{AB}^2) - 4\sqrt{\det \rho_{AB}}$. As a special case we solve the bosonic three-representability problem for the two-body reduced density matrix.

DOI: 10.1103/PhysRevA.90.032318 PACS number(s): 03.67.Mn, 03.65.Ud, 03.67.Dd

I. INTRODUCTION

The notion of *symmetric extendibility* for a bipartite quantum state ρ_{AB} was introduced in [1] as a test for entanglement. A bipartite density operator ρ_{AB} is symmetric extendible if there exists a tripartite state $\rho_{ABB'}$ such that $\mathrm{tr}_{B'}(\rho_{ABB'}) = \mathrm{tr}_B(\rho_{ABB'})$. A state ρ_{AB} without symmetric extension is evidently entangled, and to decide such an extendibility ρ_{AB} can be formulated in terms of semidefinite programming (SDP) [2]. Although this leads to numerical tests and bounds [3–6] that allow for entanglement detection [7–11], an analytic formula provides greater insight.

States with symmetric extension also have a clear operational meaning for quantum information processing [12]. One simple idea is that if a bipartite state ρ_{AB} is symmetric extendible, then one cannot distill any entanglement from ρ_{AB} by protocols only involving local operations and one-way classical communication (from A to B) [13] because of entanglement monogamy [14]. Furthermore, using the Choi-Jamiolkowski isomorphism, symmetric extendibility of bipartite states also provides a test for antidegradable quantum channels [15] and one-way quantum capacity of quantum channels [13].

A similar idea applies to the protocols for quantum key distribution (QKD), which aim to establish a shared secret key between two parties (for a review, see [16]). The corresponding QKD protocols can be viewed as having two phases: in the first phase, the two parties establish joint classical correlations by performing measurements on an untrusted bipartite quantum state, while in the second phase a secret key is distilled from these correlations by a public discussion protocol (via authenticated classical channels) which typically involves classical error correction and privacy amplification [17–20]. If the underlying bipartite state ρ_{AB} is symmetric extendible, then no secret key can be distilled by a process involving only one-way communication. Therefore, the foremost task of the public discussion protocol is to break this symmetric extendibility by some bidirectional postselection process. Failure to find such a protocol means that no secret key can be established [15,21,22].

From each of these perspectives then, we draw motivation for finding a simple characterization of all bipartite quantum states that possess symmetric extensions.

For the simplest case in which ρ_{AB} is a two-qubit state, it was conjectured in [22] that the set ρ_{AB} is symmetric extendible if and only if the spectra condition $\mathrm{tr}(\rho_B^2) \geqslant \mathrm{tr}(\rho_{AB}^2) - 4\sqrt{\det \rho_{AB}}$ is satisfied. This elegant inequality is arrived at by studying several examples both analytically and numerically, for example, the Bell diagonal states and the ZZ-invariant states. Unfortunately, [22] fails to prove in general either the necessity or the sufficiency of the conjecture, an unusual situation as typically one of the directions would be easy to establish. This hints at an intrinsic hardness to the problem, whose solution may require new physical insight.

It has been observed that the symmetric extension problem is a special case of the quantum marginal problem [15], which asks for the conditions under which some set of density matrices $\{\rho_{A_i}\}$ for subsets $A_i \subset \{1,2,\ldots,n\}$ is reduced density matrices of some state ρ of the whole n-particle system [23]. The related problem in fermionic (bosonic) systems is the so-called N-representability problem, which has a long history in quantum chemistry [24,25].

Despite recent progress [23,24,26], most quantum marginal problems are notoriously difficult. It was shown that the quantum marginal problem belongs to the complexity class of QMA(Quantum Merlin Arthur)-complete, even for the relatively simple case where the marginals $\{\rho_{A_i}\}$ are two-particle density matrices [27–29]. Nevertheless, the solution to small systems would provide insight on developing approximation or numerical methods for larger systems, although on the analytical side only a handful partial results are known [30,31].

In this work, we prove the conjecture that a two-qubit state ρ_{AB} is symmetric extendible if and only if $\mathrm{tr}(\rho_B^2) \geqslant \mathrm{tr}(\rho_{AB}^2) - 4\sqrt{\det \rho_{AB}}$. Our main insight for obtaining this result relies largely on the physical pictures from the study of the quantum marginal problem. Besides providing a better understanding for various quantum information protocols related to symmetric extension, our result also gives an analytic necessary and sufficient condition for a special case of the quantum marginal problem, which could lead to some insight into more general situations.

II. SYMMETRIC EXTENSION

For any two-qubit state ρ_{AB}, we denote its symmetric extension by $\rho_{ABB'}$ (which may be nonunique); hence $\rho_{AB} = \rho_{AB'}$. Consider the following set:

$$\mathcal{A} = \{\rho_{AB} : \vec{\lambda}(\rho_{AB}) = \vec{\lambda}(\rho_B)\}, \tag{1}$$

where $\vec{\lambda}(\rho)$ denotes the nonzero eigenvalues of ρ in decreasing order. It is shown in [22] that $\mathcal{A}$ fully characterizes the set of two-qubit states which admit pure symmetric extension $\rho_{ABB'} = |\psi_{ABB'}\rangle\langle\psi_{ABB'}|$ for some pure state $|\psi_{ABB'}\rangle$. This follows from the Schmidt decomposition of $|\psi_{ABB'}\rangle$, which gives the same nonzero spectra for ρ_{AB} and ρ_B.

The convex hull of $\mathcal{A}$ is given by

$$\mathcal{B} = \left\{\rho_{AB} : \rho_{AB} = \sum_j p_j \rho_{AB}^j;\right.$$
$$\left. 0 \leqslant p_j \leqslant 1; \sum_j p_j = 1; \rho_{AB}^j \in \mathcal{A}\right\},$$

which completely characterizes the set of two-qubit states that admit symmetric extension.

It is conjectured in [22] that set $\mathcal{B}$ may be equal to another analytically tractable set $\mathcal{C}$ given by

$$\mathcal{C} = \left\{\rho_{AB} : \mathrm{tr}\left(\rho_B^2\right) \geqslant \mathrm{tr}\left(\rho_{AB}^2\right) - 4\sqrt{\det \rho_{AB}}\right\}. \tag{2}$$

Our main result is to show that the conjecture $\mathcal{B} = \mathcal{C}$ is indeed valid.

Theorem 1. A two-qubit state ρ_{AB} admits a symmetric extension if and only if $\mathrm{tr}(\rho_B^2) \geqslant \mathrm{tr}(\rho_{AB}^2) - 4\sqrt{\det \rho_{AB}}$.

Our key insight for obtaining this result relies largely on the structure of $\mathcal{B}$. Since $\mathcal{B}$ is a convex set, for any point $\sigma_{AB} \in \partial\mathcal{B}$, where $\partial\mathcal{B}$ denotes the boundary of $\mathcal{B}$, there exists a supporting hyperplane through σ_{AB}, which is associated with an observable $H_{AB}(\sigma_{AB})$. That is, $\mathrm{tr}[H_{AB}(\sigma_{AB})\rho_{AB}] \geqslant 0$ holds for any $\rho_{AB} \in \mathcal{B}$. This induces a Hamiltonian $H = H_{AB} + H_{AB'}$ for the three-qubit system ABB', which has the symmetric extension $\rho_{ABB'}$ supported on the ground-state space of H.

If it is true that $\mathcal{B} = \mathcal{C}$, then $\mathcal{C}$ must inherit all the above-mentioned properties of the convex body $\mathcal{B}$. These observations then hint at the structure of the intersection of $\partial\mathcal{C}$ with the supporting hyperplane associated with $H_{AB}(\sigma_{AB})$, which are faces of the convex body $\mathcal{C}$.

III. THE NECESSARY CONDITION

We first prove the necessary condition of Theorem 1, which, as observed below, will follow if we prove $\mathcal{C}$ is convex. A natural approach here would be to assume that for any $\rho_{AB},\sigma_{AB} \in \mathcal{C}$, the convex combination $p\rho_{AB} + (1-p)\sigma_{AB}$ for any $p \in [0,1]$ is also in $\mathcal{C}$. However, the characterization of $\mathcal{C}$ by Eq. (2) involves the square root of a determinant, which is not easy to handle directly.

We therefore take another slightly different approach based on the fact that a closed set with a nonempty interior is convex if every point on its boundary has a supporting hyperplane [32]. Thus our goal is to find such a supporting hyperplane for any $\sigma_{AB} \in \partial\mathcal{C}$.

To achieve our goal, we will need to characterize the boundary of $\mathcal{C}$ (i.e., $\partial\mathcal{C}$). Let $f(\sigma_{AB}) = \mathrm{tr}(\sigma_B^2) - \mathrm{tr}(\sigma_{AB}^2) + 4\sqrt{\det \sigma_{AB}}$. We have the following result.

Lemma 1. $\partial\mathcal{C}$ contains all states $\sigma_{AB} \in \mathcal{C}$ without full rank (i.e., has rank <4) and all full-rank states $\sigma_{AB} \in \mathcal{C}$ satisfying $f(\sigma_{AB}) = 0$.

To prove Lemma 1, we first consider the case where σ_{AB} is without full rank. Consider the polynomial $\det(y\rho_{AB} + \sigma_{AB}) = \sum_{k=0}^{4} c_k(\rho_{AB})y^k$ for $\rho_{AB} \in \mathcal{C}$. Define $h(\rho_{AB}) = c_1(\rho_{AB})$. Notice that $c_0(\rho_{AB}) = 0$ and $\det(y\rho_{AB} + \sigma_{AB}) \geqslant 0$ when $y \to 0^+$. Furthermore, $h(\sigma_{AB}) = 0$. This implies that $\{X : h(X) = 0\}$ is a supporting hyperplane at σ_{AB}. Hence it follows that any $\sigma_{AB} \in \mathcal{C}$ without full rank is in $\partial\mathcal{C}$, and furthermore there is always a supporting hyperplane at σ_{AB}.

We then discuss the case where $\sigma_{AB} \in \partial\mathcal{C}$ is of full rank (i.e., rank 4). In this case, we show that all $\sigma_{AB} \in \partial\mathcal{C}$ are characterized by $f(\sigma_{AB}) = 0$. To see this, notice that σ_{AB} lies on the boundary if every neighborhood of σ_{AB} contains at least one point in $\mathcal{C}$ and at least one point not in $\mathcal{C}$.

For any Hermitian operator M_{AB}, we have the following expansion by Jacobi's formula (see, e.g., [33]):

$$f(\sigma_{AB} + \epsilon M_{AB}) - f(\sigma_{AB}) = 2\,\mathrm{tr}[H_{AB}(\sigma_{AB})M_{AB}]\epsilon + O(\epsilon^2), \tag{3}$$

where

$$H_{AB}(\sigma_{AB}) = \sqrt{\det \sigma_{AB}}\sigma_{AB}^{-1} - \sigma_{AB} + \sigma_B. \tag{4}$$

Now for any full-rank state σ_{AB} satisfying the strict inequality $f(\sigma_{AB}) > 0$, we can always find an open ball centered at σ_{AB} over which the strict inequality always holds; i.e., σ_{AB} is an interior point. On the other hand, if $f(\sigma_{AB}) = 0$, then we can always choose suitable Hermitian operators M_{AB}, M'_{AB} such that $\mathrm{tr}[H_{AB}(\sigma_{AB})M_{AB}] > 0$ and $\mathrm{tr}[H_{AB}(\sigma_{AB})M'_{AB}] < 0$ unless $H_{AB}(\sigma_{AB}) = 0$. The latter cannot occur, as it would imply $\sqrt{\det \sigma_{AB}}\mathbb{I}_{AB} = \sigma_{AB}^2 - \sigma_{AB}^{\frac{1}{2}}\sigma_B\sigma_{AB}^{\frac{1}{2}} \leqslant \sigma_{AB}^2$. The last inequality holds only if $\sigma_{AB} \propto \mathbb{I}_{AB}$, which immediately contradicts $f(\frac{\mathbb{I}}{4}) = \frac{1}{2}$. Hence any full-rank states satisfying $f(\sigma_{AB}) = 0$ are boundary points of $\mathcal{C}$.

Given the full characterization of $\partial\mathcal{C}$ given by Lemma 1, especially the form of Eqs. (3) and (4), our main result in this section is then the following theorem.

Theorem 2. For any full-rank state $\sigma_{AB} \in \partial\mathcal{C}$ and $H_{AB}(\sigma_{AB})$ as given in Eq. (4), the inequality

$$\mathrm{tr}[H_{AB}(\sigma_{AB})\rho_{AB}] \geqslant 0 \tag{5}$$

holds for any $\rho_{AB} \in \mathcal{C}$.

Note that the equality of Eq. (5) holds when $\rho_{AB} = \sigma_{AB}$. Equality (5) then means that for any full-rank $\sigma_{AB} \in \partial\mathcal{C}$, there is a supporting hyperplane of $\mathcal{C}$ which can be characterized by

$$\mathcal{L}(\sigma_{AB}) := \{X : \mathrm{tr}[H_{AB}(\sigma_{AB})X] = 0\}. \tag{6}$$

In order to prove Eq. (5), we will need another characterization of the set $\mathcal{C}$ and follow a straightforward step-by-step optimization procedure that involves a lengthy calculation. We provide the technical details in Appendixes A and B.

To summarize, we have thus shown that for any $\sigma_{AB} \in \partial\mathcal{C}$, with or without full rank, there exists a supporting hyperplane at σ_{AB}. This implies that $\mathcal{C}$ is convex.

A direct consequence of the convexity of $\mathcal{C}$ is that $\mathcal{B} \subseteq \mathcal{C}$. To see why, we can easily verify that $\mathcal{A} \subset \mathcal{C}$. Additionally, $\mathcal{B}$ is the convex hull of $\mathcal{A}$. Therefore the convex hull of $\mathcal{A}$ is a subset of the convex hull of $\mathcal{C}$, which is again $\mathcal{C}$, and thus we have $\mathcal{B} \subseteq \mathcal{C}$, as required.

IV. THE SUFFICIENT CONDITION

To prove the sufficiency of Theorem 1, we will need to show that any state in $\mathcal{C}$ can be represented as a convex combination of some states in $\mathcal{A}$. In fact, given the convexity of $\mathcal{C}$, it suffices to show this for $\sigma_{AB} \in \partial\mathcal{C}$.

Furthermore, we only need to deal with the cases where $\sigma_{AB} \in \partial\mathcal{C}$ is of full rank or rank 3. The rank-1 case is obvious, and the rank-2 case has already been solved in [22]. That is, any rank-2 state $\rho_{AB} \in \mathcal{C}$ can be written as a convex combination of two states in $\mathcal{A}$; hence ρ_{AB} is symmetric extendible.

For the full rank case, let us first build up some intuition by imagining what should happen if $\mathcal{B} = \mathcal{C}$. According to Eq. (5), for any $\sigma_{AB} \in \partial\mathcal{C}$, there exists a supporting hyperplane $\mathcal{L}(\sigma_{AB})$ given by all the X satisfying $\mathrm{tr}[H_{AB}(\sigma_{AB})X] = 0$, where $H_{AB}(\sigma_{AB})$ given in Eq. (4) is a Hermitian operator acting on qubits A and B.

Now let us consider the following operator H acting on the three-qubit system ABB':

$$H = H_{AB} + H_{AB'}. \tag{7}$$

Note that H can be viewed as a Hamiltonian of the system ABB'. The symmetric extension of σ_{AB}, denoted by $\sigma_{ABB'}$, should have zero energy as $\mathrm{tr}(H\sigma_{ABB'}) = \mathrm{tr}(H_{AB}\sigma_{AB}) + \mathrm{tr}(H_{AB'}\sigma_{AB'})$.

Furthermore, we show that H is positive. Since H is symmetric when swapping BB', we can always find a complete set of eigenstates $\{|\psi_i\rangle\}_{i=1}^{8}$ of H, such that for each $|\psi_i\rangle$, $\mathrm{tr}_B(|\psi_i\rangle\langle\psi_i|) = \mathrm{tr}_{B'}(|\psi_i\rangle\langle\psi_i|)$. This is because if there is any eigenstate $|\phi\rangle$ of H with energy E_ϕ which does not satisfy $\mathrm{tr}_B(|\phi\rangle\langle\phi|) = \mathrm{tr}_{B'}(|\phi\rangle\langle\phi|)$, then the state $|\phi'\rangle = S|\phi\rangle$ is also an eigenstate of H with the same energy E_ϕ, where $S := \mathrm{SWAP}_{BB'}$ is the swap operation acting on the qubits BB'. Therefore we can rechoose the eigenstates with energy E_ϕ as $\varphi = 1/\sqrt{2}(|\phi\rangle + |\phi'\rangle)$ and $\varphi' = 1/\sqrt{2}(|\phi\rangle - |\phi'\rangle)$; then we will have $\mathrm{tr}_B(|\varphi\rangle\langle\varphi|) = \mathrm{tr}_{B'}(|\varphi\rangle\langle\varphi|)$ and $\mathrm{tr}_B(|\varphi'\rangle\langle\varphi'|) = \mathrm{tr}_{B'}(|\varphi'\rangle\langle\varphi'|)$.

It then directly follows from Eq. (5) that for this complete set of eigenstates $\{|\psi_i\rangle\}_{i=1}^{8}$ with $\mathrm{tr}_B(|\psi_i\rangle\langle\psi_i|) = \mathrm{tr}_{B'}(|\psi_i\rangle\langle\psi_i|)$, $\mathrm{tr}(H|\psi_i\rangle\langle\psi_i|) \geqslant 0$. That is, H is positive. Therefore, $\sigma_{ABB'}$ with zero energy is supported on the ground-state space of H (for a general discussion on supporting hyperplanes and the ground-state space, see, e.g., [25,34,35]).

Because H is symmetric when swapping BB', generically, the ground-state space of H should be doubly degenerate. To see this, if $|\psi_0\rangle$ is a ground state of H, $S|\psi_0\rangle$ is also a ground state of H. Generically, $S|\psi_0\rangle$ should be linear independent of $|\psi_0\rangle$.

Let us now denote the ground-state space of H by V_H, which is generically two-dimensional and define

$$\mathcal{F} := \{\rho_{AB}|\rho_{AB} = \mathrm{tr}_{B'}\,\rho_{ABB'},\rho_{ABB'} \text{ supported on } V_H\}.$$

Note that $\mathcal{F} \subset \partial\mathcal{C}$ and $\mathcal{F}$ is, in fact, a face of the convex body $\mathcal{C}$. We have that for $\sigma_{AB} \in \mathcal{F}$, the symmetric extension $\sigma_{ABB'}$ is supported on the ground-state space of H. This indicates that $\mathcal{F} = \mathcal{L}(\sigma_{AB}) \bigcap \partial\mathcal{C}$.

Because V_H is generically two-dimensional, any state supported on V_H can be parameterized by a two-dimensional unitary operator U and the two eigenvalues λ_0,λ_1 of any state that is supported on V_H (with $\lambda_0 + \lambda_1 = 1$). That is, any state $\rho_{ABB'}$ supported on V_H is of the form, in some chosen orthonormal basis of $\{|\psi_1\rangle,|\psi_2\rangle\}$ of V_H,

$$\rho_{ABB'}(\lambda_0,\lambda_1,U) = U(\lambda_0|\psi_0\rangle\langle\psi_0| + \lambda_1|\psi_1\rangle\langle\psi_1|)U^\dagger.$$

Consequently, any state $\rho_{AB} = \mathrm{tr}_{B'}\,\rho_{ABB'} \in \mathcal{L}(\sigma_{AB}) \bigcap \partial\mathcal{C}$ can also be parametrized by λ_0,λ_1,U, which we can denote as $\rho_{AB}(\lambda_0,\lambda_1,U)$.

Furthermore, any $\rho_{ABB'}(\lambda_0,\lambda_1,U)$ has the obvious decomposition

$$\rho_{ABB'}(\lambda_0,\lambda_1,U) = \lambda_0\rho_{ABB'}(1,0,U) + \lambda_1\rho_{ABB'}(0,1,U),$$

where both $\rho_{ABB'}(1,0,U)$ and $\rho_{ABB'}(0,1,U)$ are three-qubit pure states. As a result,

$$\rho_{AB}(\lambda_0,\lambda_1,U) = \lambda_0\rho_{AB}(1,0,U) + \lambda_1\rho_{AB}(0,1,U),$$

where both $\rho_{AB}(1,0,U)$ and $\rho_{AB'}(0,1,U)$ are in $\partial\mathcal{C}$ and of rank 2.

Summarizing the discussion above, for a full-rank $\sigma_{AB} \in \partial\mathcal{C}$, we shall expect that, generically, any state in $\mathcal{L}(\sigma_{AB}) \bigcap \partial\mathcal{C}$ can be parameterized by a two-dimensional unitary U and two real parameters λ_0,λ_1, denoted as $\rho_{AB}(\lambda_0,\lambda_1,U)$. Any such $\rho_{AB}(\lambda_0,\lambda_1,U)$ can always be written as a convex combination of two rank-2 states in $\partial\mathcal{C}$. A detailed analysis of $\mathcal{L}(\sigma_{AB}) \bigcap \partial\mathcal{C}$ shows this is not only generically the case but also always the case. This is given as the following theorem. We shall provide the technical details of the proof in Appendix C.

Theorem 3. Every full-rank $\sigma_{AB} \in \partial\mathcal{C}$ can be written as a convex combination of two rank-2 states in $\partial\mathcal{C}$.

Furthermore, because any rank-2 state $\rho_{AB} \in \mathcal{C}$ can be written as a convex combination of two states in $\mathcal{A}$, it follows that any full-rank $\sigma_{AB} \in \partial\mathcal{C}$ can be written as a convex combination of states in $\mathcal{A}$ and hence is symmetric extendible.

Now consider the case where $\sigma_{AB} \in \partial\mathcal{C}$ has rank 3. Let $|\phi\rangle$ be the state in $\ker\sigma_{AB}$. Notice that since any two-qubit state is the local unitary equivalent to state $a|00\rangle + b|11\rangle$ for some a,b, we can always write σ_{AB} in the following form without loss of generality:

$$\sigma_{AB} = \begin{pmatrix} |b|^2 & b^*x^* & b^*y^* & -ab^* \\ bx & |r|^2 & t & -ax \\ by & t^* & |s|^2 & -ay \\ -a^*b & -a^*x^* & -a^*y^* & |a|^2 \end{pmatrix}.$$

Let us choose the Hermitian operator

$$M_{AB} = \begin{pmatrix} 0 & b^*p^* & b^*q^* & bp \\ 0 & 0 & 0 & -ap \\ bq & 0 & 0 & -aq \\ 0 & -a^*p^* & -a^*q^* & 0 \end{pmatrix},$$

where p,q are constants to be fixed later, and define $\sigma(\epsilon) = \sigma_{AB} + \epsilon M_{AB}$.

Then

$$\begin{aligned} &\mathrm{tr}\left[\sigma(\epsilon)_B^2\right] - \mathrm{tr}\left[\sigma(\epsilon)_{AB}^2\right] \\ &\quad = \mathrm{tr}[(\sigma_B + \epsilon M_B)^2] - \mathrm{tr}[(\sigma_{AB} + \epsilon M_{AB})^2] \\ &\quad = \mathrm{tr}\left(\sigma_B^2\right) - \mathrm{tr}\left(\sigma_{AB}^2\right) + \epsilon^2\left[\mathrm{tr}\left(M_B^2\right) - \mathrm{tr}\left(M_{AB}^2\right)\right] \\ &\qquad + 2\epsilon[\mathrm{tr}(\sigma_B M_B) - \mathrm{tr}(\sigma_{AB} M_{AB})] \\ &\quad = -2|ap + b^*q^*|^2\epsilon^2 - 4\mathrm{Re}[(ap + b^*q^*)(a^*x^* + by)]\epsilon, \end{aligned}$$

where Re stands for the real part of a complex number.

By choosing suitable p,q such that $ap + b^*q^* = 0$, we will have $\mathrm{tr}[\sigma(\epsilon)_B^2] = \mathrm{tr}[\sigma(\epsilon)_{AB}^2]$, which implies $\sigma(\epsilon) \in \partial\mathcal{C}$ if $\sigma(\epsilon)$ is a density operator. M_{AB} is a traceless operator whose kernel also contains $|\phi\rangle$; therefore with growing ϵ in either direction, we will have positive ϵ_+ and negative ϵ_- such that $\sigma(\epsilon_i) = \sigma_{AB} + \epsilon_i M_{AB} \in \partial\mathcal{C}$ and $\mathrm{rank}[\sigma(\epsilon_i)] \leqslant 2$ for any $i \in \{+,-\}$. Hence, σ_{AB} of rank 3 can be written as a convex combination of, at most, two states from $\mathcal{A}$.

This concludes the proof of the sufficiency condition of Theorem 1.

V. EXAMPLE

To better understand the physical picture, let us look at an example. Consider the two-qubit Werner state

$$\rho_W(p) = (1-p)\frac{\mathbb{I}}{4} + p|\phi\rangle\langle\phi|,$$

where $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $p \in [0,1]$. The equation

$$\mathrm{tr}\left[\rho_W^2(p)\right] = \mathrm{tr}\{[\mathrm{tr}_B\, \rho_W(p)]^2\} + 4\sqrt{\det \rho_W(p)}$$

provides a unique solution of $p = \frac{2}{3}$; i.e., $\rho_W(\frac{2}{3}) \in \partial\mathcal{C}$. Further, Eq. (4) gives

$$H_{AB}\left(\rho_W\left(\frac{2}{3}\right)\right) = \begin{pmatrix} \frac{2}{9} & 0 & 0 & -\frac{4}{9} \\ 0 & \frac{2}{3} & 0 & 0 \\ 0 & 0 & \frac{2}{3} & 0 \\ -\frac{4}{9} & 0 & 0 & \frac{2}{9} \end{pmatrix}.$$

The ground-state space of the Hamiltonian $H(\rho_W(\frac{2}{3})) = H_{AB}(\rho_W(\frac{2}{3})) + H_{AB'}(\rho_W(\frac{2}{3}))$ is indeed twofold degenerate and is spanned by

$$|\psi_0\rangle = \frac{1}{\sqrt{6}}\left(2|000\rangle + |101\rangle + |110\rangle\right),$$

$$|\psi_1\rangle = \frac{1}{\sqrt{6}}\left(2|111\rangle + |010\rangle + |001\rangle\right).$$

Therefore any state $\rho_{ABB'}$ supported on this ground-state space can be written as $\rho_{ABB'}(\lambda_0,\lambda_1,U) = U(\lambda_0|\psi_0\rangle\langle\psi_0| + \lambda_1|\psi_1\rangle\langle\psi_1|)U^\dagger$ for some 2×2 unitary operator U acting on the two-dimensional space spanned by $|\psi_0\rangle,|\psi_1\rangle$. And any state ρ_{AB} in $\mathcal{L}(\rho_W(\frac{2}{3}))\bigcap\partial\mathcal{C}$ has the form $\rho_{AB}(\lambda_0,\lambda_1,U) = \mathrm{tr}_{B'}[U(\lambda_0|\psi_0\rangle\langle\psi_0| + \lambda_1|\psi_1\rangle\langle\psi_1|)U^\dagger]$.

It is straightforward to check that $\rho_W(\frac{2}{3}) = \rho_{AB}(\frac{1}{2},\frac{1}{2},\mathbb{I})$. In other words, the symmetric extension of $\rho_W(\frac{2}{3})$, given by $\rho_{ABB'}(\frac{1}{2},\frac{1}{2},\mathbb{I})$, is the maximally mixed state of the ground-state space of $H(\rho_W(\frac{2}{3}))$. Also, $\rho_W(\frac{2}{3})$ can clearly be written as the convex combination of two rank-2 states which are also in $\mathcal{L}(\rho_W(\frac{2}{3}))\bigcap\partial\mathcal{C}$: $\rho_W\left(\frac{2}{3}\right) = \frac{1}{2}\rho_{AB}(1,0,\mathbb{I}) + \frac{1}{2}\rho_{AB}(0,1,\mathbb{I})$.

We remark that $p = \frac{2}{3}$ corresponds to a fidelity $\frac{3}{4}$ with $|\phi\rangle$. This is consistent with the result that Werner states with fidelity $\leqslant\frac{3}{4}$ have zero one-way distillable entanglement [36,37].

VI. DISCUSSION

We have fully solved the symmetric extension problem for the two-qubit case. An immediate application of our result is a full characterization for antidegradable qubit channels, as it is known that a channel $\mathcal{N}$ is antidegradable if and only if its Choi-Jamiolkowski representation $\rho_{\mathcal{N}}$ has a symmetric extension [15]. Previously, analytic necessary and sufficient conditions were only known for antidegradable unital qubit channels [38–40].

We can also apply our result to the three-boson system of two modes, i.e., the states supported on the symmetric subspaces of the three-qubit space. Our result then leads to a complete solution to the three-representability problem: the set of all three-representable two-boson densities can be characterized by $\{\rho_2 : \mathrm{tr}(\rho_1^2) \geqslant \mathrm{tr}(\rho_2^2)\}$, where ρ_i is the i-boson density matrix for $i = 1,2$.

A natural question to ask is how to generalize the result to higher-dimensional systems. Unfortunately, for any higher dimensions a full characterization involving only spectra is highly unlikely [22]. There have been some efforts made for special cases, but no general results have been found [41–43]. It is also possible to generalize this result to k-symmetric extension [3,6], i.e., to characterize the states ρ_{AB} with an extension to k copies of B that is symmetric under the interchange of the copies of B. We believe our physical picture based on the convexity of $\mathcal{B}$ and the symmetry of the system may shed light on the understanding of symmetric extendibility for higher-dimensional systems or multicopies.

ACKNOWLEDGMENTS

The authors thank J. Watrous and D. Leung for helpful discussions. J.C. and B.Z. are supported by NSERC, CIFAR, and NSF of China (Grant No. 61179030). Z.J. acknowledges support from NSERC and ARO. D.K. was supported by NSERC and a University Research Chair at Guelph. N.L. acknowledges support from NSERC and ORF. J.C. and Z.J. also acknowledge the hospitality of UTS-AMSS Joint Research Laboratory for Quantum Computation and Quantum Information Processing where parts of the work were done.

APPENDIX A: A USEFUL CHARACTERIZATION OF $\mathcal{C}$

To prove our main result, we will provide another useful characterization of $\mathcal{C} = \{\rho_{AB} : \mathrm{tr}(\rho_B^2) \geqslant \mathrm{tr}(\rho_{AB}^2) - 4\sqrt{\det \rho_{AB}}\}$, the set we are mainly interested in.

For simplicity, we use $\mathbb{M}_2$ to denote the set of 2×2 matrices.

Lemma 2.

$$\mathcal{C}=\left\{\begin{pmatrix}Q & R\\ P & 0\end{pmatrix}\begin{pmatrix}Q^\dagger & P\\ R & 0\end{pmatrix}: P,Q,R\in\mathbb{M}_2 \text{ such that}\right.$$

$$\left. P,R\geqslant 0,\ \|PR\|_{\mathrm{tr}}^2\geqslant \|PQ^\dagger\|_{\mathrm{tr}}^2-\|PQ\|_{\mathrm{tr}}^2\right\}.$$

Proof. Any mixed state ρ_{AB} satisfying $\mathrm{tr}(\rho_B^2)\geqslant \mathrm{tr}(\rho_{AB}^2)-4\sqrt{\det\rho_{AB}}$ can be written in the matrix form $\begin{pmatrix}A & C\\ C^\dagger & B\end{pmatrix}$, where B and A are 2×2 positive semidefinite matrices and C is another 2×2 matrix. We first assume B is invertible; then A can be written as $CB^{-1}C^\dagger+D$, where D is another $2\times\ 2$ positive semidefinite matrix.

Employing the identity

$$\begin{pmatrix}CB^{-1}C^\dagger+D & C\\ C^\dagger & B\end{pmatrix}=\begin{pmatrix}\mathbb{I} & CB^{-1}\\ 0 & \mathbb{I}\end{pmatrix}\begin{pmatrix}D & 0\\ C^\dagger & B\end{pmatrix}$$

leads to $\det\rho_{AB}=\det(BD)$.

It is not hard to verify that $\mathrm{tr}(\rho_B^2)\geqslant\mathrm{tr}(\rho_{AB}^2)-4\sqrt{\det\rho_{AB}}$ is equivalent to the condition that $\mathrm{tr}(BD)+2\sqrt{\det BD}\geqslant \mathrm{tr}(CC^\dagger)-\mathrm{tr}(CB^{-1}C^\dagger B)$.

Observe that $\mathrm{tr}(BD)+2\sqrt{\det BD}=(\mathrm{tr}\sqrt{B^{\frac12}DB^{\frac12}})^2$; we can further let $D=B^{-\frac12}X^2B^{-\frac12}$, where X is a positive semidefinite matrix.

Then

$$\rho_{AB}=\begin{pmatrix}CB^{-1}C^\dagger+B^{-\frac12}X^2B^{-\frac12} & C\\ C^\dagger & B\end{pmatrix},\qquad\text{(A1)}$$

where B and X are 2×2 positive semidefinite matrices and C is a 2×2 matrix and they satisfy $(\mathrm{tr}\,X)^2\geqslant\mathrm{tr}(CC^\dagger)-\mathrm{tr}(CB^{-1}C^\dagger B)$.

Let us write $C=B^{-\frac12}YB^{\frac12}$; we have

$$\begin{aligned}\rho_{AB}&=\begin{pmatrix}B^{-\frac12}(YY^\dagger+X^2)B^{-\frac12} & B^{-\frac12}YB^{\frac12}\\ B^{\frac12}Y^\dagger B^{-\frac12} & B\end{pmatrix}\\ &=\begin{pmatrix}B^{-\frac12} & 0\\ 0 & B^{\frac12}\end{pmatrix}\begin{pmatrix}Y & X\\ \mathbb{I} & 0\end{pmatrix}\begin{pmatrix}Y^\dagger & \mathbb{I}\\ X & 0\end{pmatrix}\begin{pmatrix}B^{-\frac12} & 0\\ 0 & B^{\frac12}\end{pmatrix}\\ &=\begin{pmatrix}B^{-\frac12}Y & B^{-\frac12}X\\ B^{\frac12} & 0\end{pmatrix}\begin{pmatrix}B^{-\frac12}Y & B^{-\frac12}X\\ B^{\frac12} & 0\end{pmatrix}^\dagger,\end{aligned}$$

where X and B are $2\times\ 2$ positive semidefinite matrices and Y is a $2\times\ 2$ matrix and they satisfy $(\mathrm{tr}\,X)^2\geqslant\mathrm{tr}(B^{-1}YBY^\dagger)-\mathrm{tr}(YY^\dagger)$.

Therefore any $\rho_{AB}\in\mathcal{C}$ can be written as

$$\rho_{AB}=\begin{pmatrix}Q & R\\ P & 0\end{pmatrix}\begin{pmatrix}Q^\dagger & P\\ R^\dagger & 0\end{pmatrix},\qquad\text{(A2)}$$

where Q and R are 2×2 matrices and Q is a 2×2 positive semidefinite matrix and they satisfy $\|PR\|_{\mathrm{tr}}^2=(\mathrm{tr}\sqrt{PRR^\dagger P})^2\geqslant\mathrm{tr}[PP(Q^\dagger Q-QQ^\dagger)]$.

Furthermore, we can even choose R to be a positive semidefinite matrix since R only appears in the term $RR^\dagger$ in the top left 2×2 submatrix of ρ_{AB}.

Now let's look at the case where B is singular. B is thus a rank-1 positive operator; without loss of generality, let's assume it is a rank-1 projection $|u\rangle\langle u|$. From the positivity of ρ_{AB}, C can be written as $|u\rangle\langle v|$. Hence

$$\rho_{AB}=\begin{pmatrix}D+|v\rangle\langle v| & |v\rangle\langle u|\\ |u\rangle\langle v| & |u\rangle\langle u|\end{pmatrix},$$

where $|u\rangle$ is a unit vector but $|v\rangle$ is unnormalized.

We can simply choose $P=|u\rangle\langle u|$, $Q=|v\rangle\langle u|$, and $R=\sqrt{D}$ to satisfy our requirement. ■

APPENDIX B: PROOF OF THEOREM 2

As we have shown in the main text, to prove the convexity of $\mathcal{C}$, it suffices to prove Theorem 2; that is, for any full-rank state $\sigma_{AB}\in\partial\mathcal{C}$ and any state $\rho_{AB}\in\mathcal{C}$,

$$\mathrm{tr}\left[\left(\sqrt{\det\sigma_{AB}}\sigma_{AB}^{-1}-\sigma_{AB}+\sigma_B\right)\rho_{AB}\right]\geqslant 0.$$

To prove Theorem 2, our main strategy is as follows: we first restate Theorem 2 as the non-negativity of a multivariable function on some specified region and then apply a step-by-step optimization procedure to the objective function. In each step, we fix several variables and think of objective function as a one-variable function whose minimum point can easily be computed. Thus one variable will be eliminated within each step. By repeating this procedure several times, we could greatly simplify the objective function as well as the constraints.

Proof. As we have seen in Appendix A, we can parametrize points in $\mathcal{C}$ by using three 2×2 matrices.

Thus we can write

$$\rho_{AB}=\begin{pmatrix}Q_1 & R_1\\ P_1 & 0\end{pmatrix}\begin{pmatrix}Q_1^\dagger & P_1\\ R_1 & 0\end{pmatrix}\qquad\text{(B1)}$$

and

$$\sigma_{AB}=\begin{pmatrix}Q_2 & R_2\\ P_2 & 0\end{pmatrix}\begin{pmatrix}Q_2^\dagger & P_2\\ R_2 & 0\end{pmatrix},\qquad\text{(B2)}$$

where $P_1,Q_1,R_1,P_2,Q_2,R_2\in\mathbb{M}_2$ satisfies $\|P_1R_1\|_{\mathrm{tr}}^2\geqslant\|P_1Q_1^\dagger\|_{\mathrm{tr}}^2-\|P_1Q_1\|_{\mathrm{tr}}^2$, $\|P_2R_2\|_{\mathrm{tr}}^2=\|P_2Q_2^\dagger\|_{\mathrm{tr}}^2-\|P_2Q_2\|_{\mathrm{tr}}^2$ and $P_1,R_1,P_2,R_2\geqslant 0$.

Under our assumption, σ_{AB} has full rank; thus

$$\sigma_{AB}^{-1}=\begin{pmatrix}0 & R_2^{-1}\\ P_2^{-1} & -P_2^{-1}Q_2^\dagger R_2^{-1}\end{pmatrix}\begin{pmatrix}0 & P_2^{-1}\\ R_2^{-1} & -R_2^{-1}Q_2P_2^{-1}\end{pmatrix}.$$

Hence $\mathrm{tr}[(\sqrt{\det\sigma_{AB}}\sigma_{AB}^{-1}-\sigma_{AB}+\sigma_B)\rho_{AB}]$ can be written as

$$\mathrm{tr}\left[A\left(Q_1Q_1^\dagger+R_1^2\right)\right]-\mathrm{tr}(BQ_1P_1)-\mathrm{tr}(P_1Q_1^\dagger B^\dagger)+\mathrm{tr}\left(CP_1^2\right),\qquad\text{(B3)}$$

where

$$
\begin{aligned}
A &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \det(P_2R_2)R_2^{-2} + P_2^2,\\
B &= \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \det(P_2R_2)P_2^{-1}Q_2^\dagger R_2^{-2} + P_2Q_2^\dagger,\\
C &= \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = Q_2Q_2^\dagger + R_2^2\\
&\quad + \det(P_2R_2)\big(P_2^{-2} + P_2^{-1}Q_2^\dagger R_2^{-2}Q_2P_2^{-1}\big).
\end{aligned} \tag{B4}
$$

We will denote our objective function (B3) as $\tau(P_1,Q_1,R_1,P_2,Q_2,R_2)$. We will prove $\tau(P_1,Q_1,R_1,P_2,Q_2,R_2) \geqslant 0$ under the assumption that $\|P_1R_1\|_{\rm tr}^2 \geqslant \|P_1Q_1^\dagger\|_{\rm tr}^2 - \|P_1Q_1\|_{\rm tr}^2$, $\|P_2R_2\|_{\rm tr}^2 = \|P_2Q_2^\dagger\|_{\rm tr}^2 - \|P_2Q_2\|_{\rm tr}^2$, and $P_1,R_1,P_2,R_2 \geqslant 0$.

To prove the desired conditional inequality, let us first fix P_1,Q_1,P_2,Q_2,R_2 and minimize $\tau(P_1,Q_1,R_1,P_2,Q_2,R_2)$ subject to $\|P_1R_1\|_{\rm tr}^2 \geqslant \|P_1Q_1^\dagger\|_{\rm tr}^2 - \|P_1Q_1\|_{\rm tr}^2$. In this step, we only need to consider the terms involving R_1; that is, we will minimize $\mathrm{tr}(AR_1^2)$ subject to $\|P_1R_1\|_{\rm tr}^2 \geqslant \|P_1Q_1^\dagger\|_{\rm tr}^2 - \|P_1Q_1\|_{\rm tr}^2$.

If $\|P_1Q_1^\dagger\|_{\rm tr} \leqslant \|P_1Q_1\|_{\rm tr}$, there is no constraint on R_1. Trivially, we have $\mathrm{tr}(AR_1^2) \geqslant 0$.

Now let us investigate the nontrivial situation where $\|P_1Q_1^\dagger\|_{\rm tr} > \|P_1Q_1\|_{\rm tr}$.

Let $\mathbb{U}_2$ denote the set of 2×2 unitary matrices. According to the Cauchy-Schwarz inequality, we have

$$
\begin{aligned}
&\mathrm{tr}\left(AR_1^2\right)\mathrm{tr}\left(A^{-1}P_1^2\right)\\
&\quad= \max_{U,V\in\mathbb{U}_2}[\mathrm{tr}(U^\dagger R_1AR_1U)\,\mathrm{tr}(V^\dagger P_1A^{-1}P_1V)]\\
&\quad\geqslant \max_{U,V\in\mathbb{U}_2}|\mathrm{tr}(V^\dagger P_1R_1U)|^2\\
&\quad= \|P_1R_1\|_{\rm tr}^2 \geqslant \mathrm{tr}\left[P_1^2(Q_1^\dagger Q_1 - Q_1Q_1^\dagger)\right].
\end{aligned}
$$

This implies

$$
\mathrm{tr}\left(AR_1^2\right) \geqslant \frac{\mathrm{tr}\left[P_1^2(Q_1^\dagger Q_1 - Q_1Q_1^\dagger)\right]}{\mathrm{tr}\left(A^{-1}P_1^2\right)},
$$

and the equality holds only if there exist $U,V\in\mathbb{U}_2$ such that $A^{\frac12}R_1U$ and $A^{-\frac12}P_1V$ are linearly dependent, $V^\dagger P_1R_1U$ is diagonal, and $\|P_1R_1\|_{\rm tr}^2 = \|P_1Q_1^\dagger\|_{\rm tr}^2 - \|P_1Q_1\|_{\rm tr}^2$.

Thus by combining the two situations together, we have

$$
\mathrm{tr}\left(AR_1^2\right) \geqslant \max\left\{0, \frac{\mathrm{tr}\left[P_1^2(Q_1^\dagger Q_1 - Q_1Q_1^\dagger)\right]}{\mathrm{tr}\left(A^{-1}P_1^2\right)}\right\} \tag{B5}
$$

$$
\geqslant \frac{\mathrm{tr}\left[P_1^2(Q_1^\dagger Q_1 - Q_1Q_1^\dagger)\right]}{\mathrm{tr}\left(A^{-1}P_1^2\right)}. \tag{B6}
$$

As a consequence, it suffices to prove

$$
\begin{aligned}
&\mathrm{tr}\left[\big(Q_1^\dagger A^{\frac12} - P_1BA^{-\frac12}\big)\big(A^{\frac12}Q_1 - A^{-\frac12}B^\dagger P_1\big)\right]\\
&\quad + \mathrm{tr}\left[(C - BA^{-1}B^\dagger)P_1^2\right] + \frac{\mathrm{tr}\left[P_1^2(Q_1^\dagger Q_1 - Q_1Q_1^\dagger)\right]}{\mathrm{tr}\left(A^{-1}P_1^2\right)} \geqslant 0
\end{aligned} \tag{B7}
$$

for any $P_1,Q_1\in\mathbb{M}_2$ and $P_1 \geqslant 0$.

Without loss of generality, we can always assume P_1 is diagonal. Let $P_1 = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ and $Q_1 = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}$. Note that q_{11} and q_{22} only appear in the first term, i.e., $\mathrm{tr}[(Q_1^\dagger A^{\frac12} - P_1BA^{-\frac12})(A^{\frac12}Q_1 - A^{-\frac12}B^\dagger P_1)]$. We thus choose suitable q_{11} and q_{22} to minimize $\mathrm{tr}[(Q_1^\dagger A^{\frac12} - P_1BA^{-\frac12})(A^{\frac12}Q_1 - A^{-\frac12}B^\dagger P_1)]$.

Here we divide Q_1 into the diagonal part $\widehat{Q}_1 = \begin{pmatrix} q_{11} & 0 \\ 0 & q_{22} \end{pmatrix}$ and the antidiagonal part $\widetilde{Q}_1 = \begin{pmatrix} 0 & q_{12} \\ q_{21} & 0 \end{pmatrix}$; then

$$
\begin{aligned}
&\|A^{\frac12}Q_1 - A^{-\frac12}B^\dagger P_1\|_F\\
&\quad= \|q_{11}A^{\frac12}|0\rangle\langle 0| + q_{22}A^{\frac12}|1\rangle\langle 1| + A^{\frac12}\widetilde{Q}_1 - A^{-\frac12}B^\dagger P_1\|_F,
\end{aligned}
$$

which can be considered to be the distance from a point $(-A^{\frac12}\widetilde{Q}_1 + A^{-\frac12}B^\dagger P_1)$ to another point on the plane spanned by $A^{\frac12}|0\rangle\langle 0|$ and $A^{\frac12}|1\rangle\langle 1|$.

Certainly, the minimum can be achieved if and only if $q_{11}A^{\frac12}|0\rangle\langle 0| + q_{22}A^{\frac12}|1\rangle\langle 1|$ is the projection of $(-A^{\frac12}\widetilde{Q}_1 + A^{-\frac12}B^\dagger P_1)$ onto the plane, i.e., $q_{11}A^{\frac12}|0\rangle\langle 0| + q_{22}A^{\frac12}|1\rangle\langle 1| + A^{\frac12}\widetilde{Q}_1 - A^{-\frac12}B^\dagger P_1 \perp \mathrm{span}\{A^{\frac12}|0\rangle\langle 0|, A^{\frac12}|1\rangle\langle 1|\}$.

Thus by solving the linear system derived by the orthogonal conditions, we have

$$
\begin{aligned}
&\min_{q_{11},q_{22}} \|q_{11}A^{\frac12}|0\rangle\langle 0| + q_{22}A^{\frac12}|1\rangle\langle 1| + A^{\frac12}\widetilde{Q}_1 - A^{-\frac12}B^\dagger P_1\|_F^2\\
&\quad= \|A^{\frac12}\widetilde{Q}_1 - A^{-\frac12}B^\dagger P_1\|_F^2 - \left\|\left(-\frac{\langle 0|A\widetilde{Q}_1 - B^\dagger P_1|0\rangle}{\langle 0|A|0\rangle}\right)A^{\frac12}|0\rangle\langle 0| + \left(-\frac{\langle 1|A\widetilde{Q}_1 - B^\dagger P_1|1\rangle}{\langle 1|A|1\rangle}\right)A^{\frac12}|1\rangle\langle 1|\right\|_F^2.
\end{aligned} \tag{B8}
$$

By substituting corresponding terms in the left-hand side of Eq. (B7), we have

$$
\begin{aligned}
&\tau(P_1,Q_1,R_1,P_2,Q_2,R_2)\\
&\quad\geqslant \mathrm{tr}\left[(Q_1^\dagger A^{\frac12} - P_1BA^{-\frac12})(A^{\frac12}Q_1 - A^{-\frac12}B^\dagger P_1)\right] + \mathrm{tr}\left[(C - BA^{-1}B^\dagger)P_1^2\right] + \frac{\mathrm{tr}\left[P_1^2(Q_1^\dagger Q_1 - Q_1Q_1^\dagger)\right]}{\mathrm{tr}\left(A^{-1}P_1^2\right)}\\
&\quad\geqslant \|A^{\frac12}\widetilde{Q}_1 - A^{-\frac12}B^\dagger P_1\|_F^2 - \left\|\left(-\frac{\langle 0|A\widetilde{Q}_1 - B^\dagger P_1|0\rangle}{\langle 0|A|0\rangle}\right)A^{\frac12}|0\rangle\langle 0| + \left(-\frac{\langle 1|A\widetilde{Q}_1 - B^\dagger P_1|1\rangle}{\langle 1|A|1\rangle}\right)A^{\frac12}|1\rangle\langle 1|\right\|_F^2
\end{aligned}
$$

$$
\begin{aligned}
&+\operatorname{tr}\left[(C-BA^{-1}B^{\dagger})P_1^2\right]+\frac{\operatorname{tr}\left[P_1^2(Q_1^{\dagger}Q_1-Q_1Q_1^{\dagger})\right]}{\operatorname{tr}\left(A^{-1}P_1^2\right)}\\
=\;&\operatorname{tr}(A\widetilde{Q}_1\widetilde{Q}_1^{\dagger})-\operatorname{tr}(B^{\dagger}P_1\widetilde{Q}_1^{\dagger})-\operatorname{tr}(B\widetilde{Q}_1P_1)-\frac{|\langle 0|A\widetilde{Q}_1-B^{\dagger}P_1|0\rangle|^2}{\langle 0|A|0\rangle}-\frac{|\langle 1|A\widetilde{Q}_1-B^{\dagger}P_1|1\rangle|^2}{\langle 1|A|1\rangle}\\
&+\operatorname{tr}\left(CP_1^2\right)+\frac{\operatorname{tr}\left[P_1^2(Q_1^{\dagger}Q_1-Q_1Q_1^{\dagger})\right]}{\operatorname{tr}\left(A^{-1}P_1^2\right)}\\
=\;&c_{11}x^2+c_{22}y^2+a_{11}|q_{12}|^2+a_{22}|q_{21}|^2-b_{21}q_{12}y-b_{12}q_{21}x-b_{21}^*q_{12}^*y-b_{12}^*q_{21}^*x\\
&+\frac{\det(A)(x^2-y^2)(|q_{21}|^2-|q_{12}|^2)}{a_{11}y^2+a_{22}x^2}-\frac{|q_{21}a_{12}-xb_{11}^*|^2}{a_{11}}-\frac{|q_{12}a_{21}-yb_{22}^*|^2}{a_{22}}\\
=\;&\frac{\det(A)(a_{11}+a_{22})}{a_{11}y^2+a_{22}x^2}\\
&\times\left(\frac{1}{a_{11}}\left|xq_{21}+\frac{(a_{11}y^2+a_{22}x^2)(a_{12}b_{11}-b_{12}a_{11})^*}{\det(A)(a_{11}+a_{22})}\right|^2+\frac{1}{a_{22}}\left|yq_{12}+\frac{(a_{11}y^2+a_{22}x^2)(a_{21}b_{22}-a_{22}b_{21})^*}{\det(A)(a_{11}+a_{22})}\right|^2\right)\\
&+\left(c_{11}-\frac{|b_{11}|^2}{a_{11}}-\frac{\frac{a_{22}}{a_{11}}|a_{12}b_{11}-a_{11}b_{12}|^2+|a_{21}b_{22}-a_{22}b_{21}|^2}{\det(A)(a_{11}+a_{22})}\right)x^2\\
&+\left(c_{22}-\frac{|b_{22}|^2}{a_{22}}-\frac{|a_{12}b_{11}-a_{11}b_{12}|^2+\frac{a_{11}}{a_{22}}|a_{21}b_{22}-a_{22}b_{21}|^2}{\det(A)(a_{11}+a_{22})}\right)y^2.
\end{aligned}
\tag{B9}
$$

To complete our proof, we will show the last two terms all vanish when the full-rank state satisfies $\sigma_{AB}\in\partial\mathcal{C}$, which will immediately lead to our desired conditional inequality.

Note that $\begin{pmatrix} A & -B^{\dagger}\\ -B & C\end{pmatrix}$ represents the matrix form of $H_{AB}=\sqrt{\det\sigma_{AB}}\sigma_{AB}^{-1}-\sigma_{AB}+\sigma_B$. Thus the last two terms vanish if and only if

$$
\begin{aligned}
\det\langle 0_B|H_{AB}|0_B\rangle &= \det\langle 1_B|H_{AB}|1_B\rangle\\
&=\frac{a_{22}|\det\langle 0_B|H_{AB}|0_A\rangle|^2+a_{11}|\det\langle 1_B|H_{AB}|0_A\rangle|^2}{\det\langle 0_A|H_{AB}|0_A\rangle(a_{11}+a_{22})}.
\end{aligned}
$$

Let $H_{AB}^{(i_1,\dots,i_k)}$ be the submatrix formed by taking the $(i_1,\dots,i_k)$th rows and columns of H_{AB}. Then $\det\langle 0_B|H_{AB}|0_B\rangle=\det\langle 1_B|H_{AB}|1_B\rangle$ means $\det H_{AB}^{(1,3)}=\det H_{AB}^{(2,4)}$. Once we have proved the first equality, the second equality can be rewritten as

$$
\begin{aligned}
&a_{22}\det\langle 0_A|H_{AB}|0_A\rangle\det\langle 0_B|H_{AB}|0_B\rangle\\
&\quad+a_{11}\det\langle 0_A|H_{AB}|0_A\rangle\det\langle 1_B|H_{AB}|1_B\rangle\\
&\quad=a_{22}|\det\langle 0_B|H_{AB}|0_A\rangle|^2+a_{11}|\det\langle 1_B|H_{AB}|0_A\rangle|^2,
\end{aligned}
$$

which can be further reformulated as $\det H_{AB}^{(1,2,3)}=-\det H_{AB}^{(1,2,4)}$.

Thus, to accomplish our goal, it suffices to prove

$$\det H_{AB}^{(1,3)}=\det H_{AB}^{(2,4)}, \tag{B10}$$

$$\det H_{AB}^{(1,2,3)}=-\det H_{AB}^{(1,2,4)}. \tag{B11}$$

For Eq. (B10), i.e.,

$$\langle 0|A|0\rangle\langle 0|C|0\rangle-|\langle 0|B|0\rangle|^2=\langle 1|A|1\rangle\langle 1|C|1\rangle-|\langle 1|B|1\rangle|^2,$$

it is equivalent to

$$\langle 0|AC|0\rangle+\langle 1|CA|1\rangle=\langle 1|B^{\dagger}B|1\rangle+\langle 0|BB^{\dagger}|0\rangle.$$

To prove this, it suffices to show $AC-BB^{\dagger}$ is the adjugate matrix of $CA-B^{\dagger}B$, i.e., $AC-BB^{\dagger}+CA-B^{\dagger}B=\operatorname{tr}(AC-BB^{\dagger})\mathbb{I}$.

In fact, to prove the above claim, our assumption $\|P_2R_2\|_{\mathrm{tr}}^2=\|P_2Q_2^{\dagger}\|_{\mathrm{tr}}^2-\|P_2Q_2\|_{\mathrm{tr}}^2$ is not necessary. The identity holds for all 2×2 Hermitian matrices P_2, R_2 and any 2×2 matrix Q_2. This fact can be easily verified by using symbolic computing software like *Mathematica* [44].

Now let us look at Eq. (B11). Let

$$
\begin{aligned}
\widetilde{H}&=\begin{pmatrix} A & 0\\ 0 & C-BA^{-1}B^{\dagger}\end{pmatrix}\\
&=\begin{pmatrix}\mathbb{I} & 0\\ BA^{-1} & \mathbb{I}\end{pmatrix}H\begin{pmatrix}\mathbb{I} & A^{-1}B^{\dagger}\\ 0 & \mathbb{I}\end{pmatrix}.
\end{aligned}
$$

The determinant is invariant under elementary row and column operations; we have $\det H_{AB}^{(1,2,3)}=\det\widetilde{H}^{(1,2,3)}=\det(A)\widetilde{H}_{3,3}$ and $\det H_{AB}^{(1,2,4)}=\det\widetilde{H}^{(1,2,4)}=\det(A)\widetilde{H}_{4,4}$. Therefore Eq. (B11) is equivalent to $\widetilde{H}_{3,3}=-\widetilde{H}_{4,4}$, i.e.,

$$\operatorname{tr}(C-BA^{-1}B^{\dagger})=0.$$

$\operatorname{tr}(C-BA^{-1}B^{\dagger})$ is invariant under local unitary operations; thus it suffices to prove $\operatorname{tr}(C-BA^{-1}B^{\dagger})=0$ for diagonal P_2.

Again, let $P_2=\begin{pmatrix} x' & 0\\ 0 & y'\end{pmatrix}$ and divide $Q_2=\begin{pmatrix} q'_{11} & q'_{12}\\ q'_{21} & q'_{22}\end{pmatrix}$ into the diagonal part $\widehat{Q}_2$ and antidiagonal part $\widetilde{Q}_2$. Simple calculation will show that $\widehat{Q}_2$ all cancel out in $\operatorname{tr}(C-BA^{-1}B^{\dagger})$, so we can assume $q'_{11}=q'_{22}=0$ without loss of generality. Then everything is straightforward.

By substituting $P_2 = \begin{pmatrix} x' & 0 \\ 0 & y' \end{pmatrix}$, $Q_2 = \begin{pmatrix} 0 & q'_{12} \\ q'_{21} & 0 \end{pmatrix}$, and $R_2 = \begin{pmatrix} r_{11} & r_{12} \\ r^*_{12} & r_{22} \end{pmatrix}$ in Eq. (B4), we will have

$$\begin{aligned}
&\mathrm{tr}(C - BA^{-1}B^\dagger)\\
&= \frac{(r_{11}x' + r_{22}y')(r_{11}y' + r_{22}x') - |r_{12}|^2(x'-y')^2}{x'y'[(r_{11}x' + r_{22}y')^2 + |r_{12}|^2(x'-y')^2]}\\
&\quad \times \{ (r_{11}x' + r_{22}y')^2 + |r_{12}|^2(x'-y')^2\\
&\quad - [(x')^2 - (y')^2](|q'_{21}|^2 - |q'_{12}|^2)\}.
\end{aligned}$$

Under our assumption, a full-rank state $\sigma_{AB} \in \partial\mathcal{C}$ implies $\|P_2R_2\|^2_{\mathrm{tr}} = \|P_2Q_2^\dagger\|^2_{\mathrm{tr}} - \|P_2Q_2\|^2_{\mathrm{tr}}$, or, equivalently, $(r_{11}x' + r_{22}y')^2 + |r_{12}|^2(x'-y')^2 = [(x')^2 - (y')^2](|q'_{21}|^2 - |q'_{12}|^2)$. $\mathrm{tr}(C - BA^{-1}B^\dagger) = 0$ follows immediately. ■

APPENDIX C: FACES OF $\mathcal{C}$

From Theorem 2, $\mathcal{C}$ is a convex body. The faces of $\mathcal{C}$ are its intersections with the supporting hyperplanes.

Let us start with a full-rank boundary point $\sigma_{AB} \in \partial\mathcal{C}$. Let $H_{AB}(\sigma_{AB}) = \sqrt{\det\sigma_{AB}}\sigma_{AB}^{-1} - \sigma_{AB} + \sigma_B$; then the supporting hyperplane

$$\mathcal{L}(\sigma_{AB}) := \{X : \mathrm{tr}[H_{AB}(\sigma_{AB})X] = 0\}$$

also defines a face $\mathcal{F}(\sigma_{AB}) = \mathcal{L}(\sigma_{AB}) \bigcap \mathcal{C}$.

Recall that in Appendix B, we applied a step-by-step optimization procedure to prove $\mathrm{tr}[H_{AB}(\sigma_{AB})\rho_{AB}] \geqslant 0$ for any $\rho_{AB} \in \mathcal{C}$. Thus $\mathcal{L}(\sigma_{AB}) \bigcap \mathcal{C}$ contains all those states satisfying the equality in every optimization step. In this appendix, we will solve the equation system and then provide a complete parametrization of $\mathcal{F}(\sigma_{AB})$. As a by-product, we will prove Theorem 3 at the end of this appendix.

According to Appendix A, σ_{AB} can be represented as follows by using the 2×2 matrices P_2, Q_2, R_2 satisfying $\|P_2R_2\|^2_{\mathrm{tr}} = \|P_2Q_2^\dagger\|^2_{\mathrm{tr}} - \|P_2Q_2\|^2_{\mathrm{tr}}$ and $P_2, R_2 \geqslant 0$:

$$\sigma_{AB} = \begin{pmatrix} Q_2 & R_2 \\ P_2 & 0 \end{pmatrix}\begin{pmatrix} Q_2^\dagger & P_2 \\ R_2 & 0 \end{pmatrix} \in \partial\mathcal{C}.$$

We can represent any state $\rho_{AB} \in \mathcal{F}(\sigma_{AB})$ in the same way:

$$\rho_{AB} = \begin{pmatrix} Q_1 & R_1 \\ P_1 & 0 \end{pmatrix}\begin{pmatrix} Q_1^\dagger & P_1 \\ R_1 & 0 \end{pmatrix}.$$

Thus our aim is to characterize the set of three-tuples $\{(P_1, Q_1, R_1) : \begin{pmatrix} Q_1 & R_1 \\ P_1 & 0 \end{pmatrix}\begin{pmatrix} Q_1^\dagger & P_1 \\ R_1 & 0 \end{pmatrix} \in \mathcal{F}(\sigma_{AB})\}$ for any given $\sigma_{AB} = \begin{pmatrix} Q_2 & R_2 \\ P_2 & 0 \end{pmatrix}\begin{pmatrix} Q_2^\dagger & P_2 \\ R_2 & 0 \end{pmatrix} \in \partial\mathcal{C}$, or, equivalently, the three-tuples (P_1, Q_1, R_1) to make $\tau(P_1, Q_1, R_1, P_2, Q_2, R_2)$, which is defined in Eq. (B3), vanish.

We first consider the three-tuples (P_1, Q_1, R_1) in which P_1 is a diagonal matrix $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$, which is also what we assumed in our proof in Appendix B. $A = (a_{ij})_{1\leqslant i,j\leqslant 2}$ and $B = (b_{ij})_{1\leqslant i,j\leqslant 2}$ are matrices depending on only P_2, Q_2, R_2, as given in Eq. (B4). As we provide a step-by-step optimization procedure to show $\tau(P_1, Q_1, R_1, P_2, Q_2, R_2) \geqslant 0$ in Appendix B, Q_1 and R_1 must be chosen to make the equalities hold in every optimization step.

(1) The equality in Eq. (B6) holds if and only if there exist $U, V \in \mathbb{U}_2$ such that $A^{\frac12}R_1U$ and $A^{-\frac12}P_1V$ are linearly dependent, $V^\dagger P_1R_1U$ is diagonal, and $\|P_1R_1\|^2_{\mathrm{tr}} = \|P_1Q_1^\dagger\|^2_{\mathrm{tr}} - \|P_1Q_1\|^2_{\mathrm{tr}}$.

(2) The minimum of the left-hand side in Eq. (B8) can be achieved if and only if $q_{11}A^{\frac12}|0\rangle\langle 0| + q_{22}A^{\frac12}|1\rangle\langle 1|$ is the projection of $(-A^{\frac12}\widetilde{Q}_1 + A^{-\frac12}B^\dagger P_1)$ onto the plane, i.e., $q_{11}A^{\frac12}|0\rangle\langle 0| + q_{22}A^{\frac12}|1\rangle\langle 1| + A^{\frac12}\widetilde{Q}_1 - A^{-\frac12}B^\dagger P_1 \perp \mathrm{span}\{A^{\frac12}|0\rangle\langle 0|, A^{\frac12}|1\rangle\langle 1|\}$.

(3) The right-hand side of Eq. (B9) equals zero if and only if $xq_{21} + \frac{(a_{11}y^2 + a_{22}x^2)(a_{12}b_{11} - b_{12}a_{11})^*}{\det(A)(a_{11}+a_{22})}$ and $yq_{12} + \frac{(a_{11}y^2 + a_{22}x^2)(a_{21}b_{22} - a_{22}b_{21})^*}{\det(A)(a_{11}+a_{22})}$ all vanish.

Q_1 and R_1 can thus be derived by using elementary linear algebra. Explicit expressions will be given later in the more general Lemma 3.

If P_1 is not diagonal, then from the eigenvalue decomposition, we can write $P_1 = U\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}U^\dagger$, where U is a 2×2 unitary matrix and x, y are positive numbers. Note that $\rho_{AB} \in \mathcal{F}(\sigma_{AB})$ if and only if $(U^\dagger \otimes U^\dagger)\rho_{AB}(U \otimes U) \in \mathcal{F}((U^\dagger \otimes U^\dagger)\sigma_{AB}(U \otimes U))$ and $(U^\dagger \otimes U^\dagger)\rho_{AB}(U \otimes U)$ can be represented by the three-tuple $(U^\dagger P_1U, U^\dagger Q_1U, U^\dagger R_1U)$; hence our result for diagonal case will apply directly.

To summarize, given a full-rank $\sigma_{AB} = \begin{pmatrix} Q_2 & R_2 \\ P_2 & 0 \end{pmatrix}\begin{pmatrix} Q_2^\dagger & P_2 \\ R_2 & 0 \end{pmatrix} \in \partial\mathcal{C}$, we can parametrize all full-rank states in $\mathcal{F}(\sigma_{AB})$ by using a 2×2 unitary matrix U and positive numbers x, y as the following lemma.

Lemma 3. All full-rank states in $\mathcal{F}(\sigma_{AB})$ can be represented as some

$$\widetilde{\rho}_{AB}(x,y,U) = \begin{pmatrix} Q_1 & R_1 \\ P_1 & 0 \end{pmatrix}\begin{pmatrix} Q_1^\dagger & P_1 \\ R_1 & 0 \end{pmatrix},$$

where

$$P_1 = U\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}U^\dagger,$$

$$Q_1 = \frac{1}{\det(A)\,\mathrm{tr}(A)}U\begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}^{-1}U^\dagger,$$

and

$$R_1 = \frac{\sqrt{(x^2-y^2)\left(\left|\frac{a_{12}b_{11}-b_{12}a_{11}}{x}\right|^2 - \left|\frac{a_{21}b_{22}-a_{22}b_{21}}{y}\right|^2\right)}}{\det(A)\,\mathrm{tr}(A)}U\sqrt{\begin{pmatrix} a_{22}^2x^2 + |a_{12}|^2y^2 & -a_{12}(a_{11}y^2 + a_{22}x^2) \\ -a_{21}(a_{11}y^2 + a_{22}x^2) & |a_{21}|^2x^2 + a_{11}^2y^2 \end{pmatrix}}U^\dagger,$$

where

$$A(U) = (a_{ij})_{1\leqslant i,j\leqslant 2} = U^\dagger\big[\det(P_2R_2)R_2^{-2} + P_2^2\big]U, \quad B(U) = (b_{ij})_{1\leqslant i,j\leqslant 2} = U^\dagger\big[\det(P_2R_2)P_2^{-1}Q_2^\dagger R_2^{-2} + P_2Q_2^\dagger\big]U,$$

and

$$\begin{aligned}
q_{11} &= \left[\left(a_{11}a_{22}+a_{22}^2-a_{12}a_{21}\right)b_{11}^*-a_{12}a_{22}b_{12}^*\right]x^2+a_{12}(a_{21}b_{11}^*-a_{11}b_{12}^*)y^2,\\
q_{12} &= -(a_{11}y^2+a_{22}x^2)(a_{21}b_{22}-a_{22}b_{21})^*,\\
q_{21} &= -(a_{11}y^2+a_{22}x^2)(a_{12}b_{11}-b_{12}a_{11})^*,\\
q_{22} &= a_{21}(a_{12}b_{22}^*-a_{22}b_{21}^*)x^2+\left[\left(a_{11}a_{22}+a_{11}^2-a_{12}a_{21}\right)b_{22}^*-a_{21}a_{11}b_{21}^*\right]y^2.
\end{aligned}$$

We reuse the symbols a_{ij} and b_{ij} to keep our formulas simple, but one should keep in mind that they depend on the unitary matrix U. Indeed, we should instead use the more precise form $a_{ij}(U)$ and $b_{ij}(U)$ in Lemma 3 if we do not care about the length of the expressions.

To make sure that $\widetilde{\rho}_{AB}(x,y,U)$ lies in $\mathcal{C}$, x and y must satisfy

$$(x-y)(|a_{21}b_{22}-a_{22}b_{21}|x-|a_{12}b_{11}-b_{12}a_{11}|y)\leqslant 0.$$

All full-rank states in $\mathcal{F}(\sigma_{AB})$ can be parameterized in this way. However, for the case $x=y$ or $\frac{x}{y}=|\frac{a_{12}b_{11}-b_{12}a_{11}}{a_{21}b_{22}-a_{22}b_{21}}|$, $\widetilde{\rho}_{AB}(x,y,U)$ has rank 2 since the corresponding R_1 is a zero matrix for both cases.

$\mathcal{F}(\sigma_{AB})$ also contains other non-full-rank states which correspond to $x=0$ or $y=0$. $y=0$ occurs only if $|a_{21}b_{22}-a_{22}b_{21}|=0$. In this case, we have

$$\widetilde{\rho}_{AB}(x,0,U)=(U\otimes U)\begin{pmatrix}\frac{|b_{11}|^2x^2}{a_{12}a_{21}} & -\frac{|b_{11}|^2x^2}{a_{22}a_{21}} & 0 & 0\\ -\frac{|b_{11}|^2x^2}{a_{12}a_{22}} & \frac{|b_{11}|^2x^2}{a_{12}a_{21}}+\frac{|b_{11}|^2x^2}{a_{22}^2} & \frac{b_{11}^*x^2}{a_{12}} & 0\\ 0 & \frac{b_{11}x^2}{a_{21}} & x^2 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}(U^\dagger\otimes U^\dagger),$$

which is a rank-2 state. We have similar results for the case with $x=0$.

We will now prove Theorem 3 as an application of our parametrization scheme. A simple calculation will show us that all entries of $\widetilde{\rho}_{AB}(x,y,U)$ are linear combinations of x^2 and y^2. Let us assume $|\frac{a_{12}b_{11}-b_{12}a_{11}}{a_{21}b_{22}-a_{22}b_{21}}|>1$ without loss of generality; then for any $y\leqslant x\leqslant|\frac{a_{12}b_{11}-b_{12}a_{11}}{a_{21}b_{22}-a_{22}b_{21}}|y$, $\rho_{AB}(x,y,U)$ is a convex combination of $\widetilde{\rho}_{AB}(y,y,U)$ and $\widetilde{\rho}_{AB}(|\frac{a_{12}b_{11}-b_{12}a_{11}}{a_{21}b_{22}-a_{22}b_{21}}|y,y,U)$, both of which are rank-2 states.

In other words, after the normalization, $\widetilde{\rho}_{AB}(x,y,U)$ only depends on the unitary matrix U and the ratio of x and y. Let $\rho_{AB}(1,0,U)=\widetilde{\rho}_{AB}(1,1,U)$ and $\rho_{AB}(0,1,U)=\widetilde{\rho}_{AB}(|a_{12}b_{11}-b_{12}a_{11}|,|a_{21}b_{22}-a_{22}b_{21}|,U)$; then all states on the face $\mathcal{F}(\sigma_{AB})$ can be represented as $\rho_{AB}(\lambda,1-\lambda,U)=\lambda\rho_{AB}(1,0,U)+(1-\lambda)\rho_{AB}(0,1,U)$, where $0\leqslant\lambda\leqslant 1$ and $U\in\mathbb{U}_2$.

[1] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).
[2] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).
[3] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).
[4] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **71**, 032333 (2005).
[5] M. Navascués, M. Owari, and M. B. Plenio, Phys. Rev. A **80**, 052306 (2009).
[6] F. G. S. L. Brandão and M. Christandl, Phys. Rev. Lett. **109**, 160502 (2012).
[7] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[8] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[9] M. Horodecki, P. Horodecki, and R. Horodecki, in *Quantum Information* (Springer, Berlin, 2001), pp. 151–195.
[10] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[11] P. Horodecki and M. Lewenstein, Phys. Rev. Lett. **85**, 2657 (2000).
[12] B. M. Terhal, A. C. Doherty, and D. Schwab, Phys. Rev. Lett. **90**, 157903 (2003).
[13] M. L. Nowakowski and P. Horodecki, J. Phys. A **42**, 135306 (2009).
[14] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. A **57**, 2368 (1998).
[15] G. Ove Myhr, Ph.D. thesis, Friedrich-Alexander-Universität Erlangen-Nürnberg, 2011.
[16] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[17] C. Cachin and U. M. Maurer, J. Cryptol. **10**, 97 (1997).
[18] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[19] H. F. Chau, Phys. Rev. A **66**, 060302 (2002).
[20] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[21] G. O. Myhr, J. M. Renes, A. C. Doherty, and N. Lütkenhaus, Phys. Rev. A **79**, 042329 (2009).
[22] G. O. Myhr and N. Lütkenhaus, Phys. Rev. A **79**, 062307 (2009).
[23] A. A. Klyachko, J. Phys. Conf. Ser. **36**, 72 (2006).
[24] A. J. Coleman, Rev. Mod. Phys. **35**, 668 (1963).
[25] R. M. Erdahl, J. Math. Phys. **13**, 1608 (1972).
[26] M. Altunbulak and A. Klyachko, Commun. Math. Phys. **282**, 287 (2008).

[27] Y.-K. Liu, in *Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques*, edited by J. Diaz, K. Jansen, J. D. Rolim, and U. Zwick, Lecture Notes in Computer Science Vol. 4110 (Springer, Berlin, 2006), pp. 438–449.
[28] Y.-K. Liu, M. Christandl, and F. Verstraete, Phys. Rev. Lett. **98**, 110503 (2007).
[29] T.-C. Wei, M. Mosca, and A. Nayak, Phys. Rev. Lett. **104**, 040501 (2010).
[30] D. W. Smith, J. Chem. Phys. **43**, S258 (1965).
[31] E. A. Carlen, J. L. Lebowitz, and E. H. Lieb, J. Math. Phys. **54**, 062103 (2013).
[32] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, 2004).
[33] J. R. Magnus and H. Neudecker, *Matrix Differential Calculus with Applications in Statistics and Econometrics* (Wiley, New York, 1988).
[34] J. Chen, Z. Ji, M. B. Ruskai, B. Zeng, and D.-L. Zhou, J. Math. Phys. **53**, 072203 (2012).
[35] J. Chen, Z. Ji, B. Zeng, and D. L. Zhou, Phys. Rev. A **86**, 022339 (2012).
[36] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[37] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[38] T. S. Cubitt, M. B. Ruskai, and G. Smith, J. Math. Phys. **49**, 102104 (2008).
[39] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[40] C.-S. Niu and R. B. Griffiths, Phys. Rev. A **58**, 4377 (1998).
[41] K. S. Ranade, Phys. Rev. A **80**, 022301 (2009).
[42] K. S. Ranade, J. Phys. A **42**, 425302 (2009).
[43] P. D. Johnson and L. Viola, Phys. Rev. A **88**, 032323 (2013).
[44] The *Mathematica* notebook can be found at http://jianxin.iqubit.org/downloads/Verification.nb.