Universal state inversion and concurrence in arbitrary dimensions

Pranaw Rungta,[1] V. Bužek,[2,*] Carlton M. Caves,[1] M. Hillery,[3] and G. J. Milburn[4]
[1]*Center for Advanced Studies, Department of Physics and Astronomy, University of New Mexico, Albuquerque, New Mexico 87131-1156*
[2]*The Erwin Schrödinger Institute for Mathematical Physics, Boltzmanngasse 9, A-1090 Wien, Austria*
[3]*Department of Physics and Astronomy, Hunter College of CUNY, 695 Park Avenue, New York, New York 10021*
[4]*Centre for Quantum Computer Technology, The University of Queensland, Queensland 4072, Australia*
(Received 13 February 2001; published 18 September 2001)

Wootters [Phys. Rev. Lett. **80**, 2245 (1998)] has given an explicit formula for the entanglement of formation of two qubits in terms of what he calls the *concurrence* of the joint density operator. Wootters's concurrence is defined with the help of the superoperator that flips the spin of a qubit. We generalize the spin-flip superoperator to a ''universal inverter,'' which acts on quantum systems of arbitrary dimension, and we introduce the corresponding generalized concurrence for joint pure states of $D_1\times D_2$ bipartite quantum systems. We call this generalized concurrence the *I concurrence* to emphasize its relation to the universal inverter. The universal inverter, which is a positive, but not completely positive superoperator, is closely related to the completely positive universal-NOT superoperator, the quantum analogue of a classical NOT gate. We present a physical realization of the universal-NOT superoperator.

DOI: 10.1103/PhysRevA.64.042315 PACS number(s): 03.67.Lx, 03.65.Ud

I. INTRODUCTION

Entanglement plays a central role in quantum information theory [1,2]. Perhaps the most important measure of entanglement for bipartite systems is the entanglement of formation [3,4]. For a bipartite pure state $|\Psi^{AB}\rangle$, the entanglement of formation is given by the entropy of the marginal density operators ρ_A and ρ_B of systems A and B. For a bipartite mixed state ρ_{AB}, the entanglement of formation is given by the minimum average marginal entropy of ensemble decompositions of ρ_{AB}.

Hill and Wootters [5] introduced another measure of entanglement, called the *concurrence*, for pairs of qubits. The concurrence is defined with the help of a superoperator $\mathcal{S}_2$, whose action on a qubit density operator $\rho=1/2(I+\vec{P}\cdot\vec{\sigma})$ is to flip the spin of the qubit

$$\mathcal{S}_2(\rho)=\sigma_y\rho^*\sigma_y=\frac{1}{2}(I-\vec{P}\cdot\vec{\sigma}). \tag{1}$$

Here, ρ^* is the complex conjugate (or transpose) of ρ relative to the eigenbasis of σ_z. The concurrence of a pure state $|\Psi_{AB}\rangle$ of two qubits is defined to be [5]

$$\begin{aligned} C_2(\Psi_{AB}) &\equiv \sqrt{\langle\Psi_{AB}|\mathcal{S}_2\otimes\mathcal{S}_2(|\Psi_{AB}\rangle\langle\Psi_{AB}|)|\Psi_{AB}\rangle} \\ &= |\langle\Psi_{AB}|\sigma_y\otimes\sigma_y|\Psi^*_{AB}\rangle|. \end{aligned} \tag{2}$$

Wootters [6] showed that the entanglement of formation of an arbitrary two-qubit mixed state ρ_{AB} can be written in terms of the minimum average pure-state concurrence, where the minimum is taken over all ensemble decompositions of ρ_{AB}, and he derived an explicit expression for this minimum average pure-state concurrence. Wootters called this minimum the concurrence of the mixed state. Uhlmann [7] introduced a generalization of Wootters's concurrence to higher dimensions, which we discuss further in Sec. II B.

In this paper, we generalize the notion of concurrence to pairs of quantum systems of arbitrary dimension, in a way different from Uhlmann's. We show in Sec. II that if the concurrence is to be generated by a product superoperator, as in the expression (2), then the only suitable superoperator to go into the tensor product is what we call the ''universal inverter.'' For a D-dimensional quantum system, which we call a ''qudit,'' we denote the universal inverter by $\mathcal{S}_D$. The action of the universal inverter on a qudit state ρ is given by

$$\mathcal{S}_D(\rho)=\nu_D(I-\rho), \tag{3}$$

where ν_D is a positive constant. Acting on a pure qudit state $|\psi\rangle$, the universal inverter maps $|\psi\rangle$ to a multiple of the maximally mixed state in the subspace orthogonal to $|\psi\rangle$. The universal inverter has been used previously in studies of the separability of mixed states by Horodecki and Horodecki [8].

The corresponding generalized concurrence for a joint pure state $|\Psi_{AB}\rangle$ of a $D_1\times D_2$ system, in analogy to Eq. (2) for qubits, is given by

$$\begin{aligned} C(\Psi_{AB}) &\equiv \sqrt{\langle\Psi_{AB}|\mathcal{S}_{D_1}\otimes\mathcal{S}_{D_2}(|\Psi_{AB}\rangle\langle\Psi_{AB}|)|\Psi_{AB}\rangle} \\ &= \sqrt{2\,\nu_{D_1}\nu_{D_2}[1-\mathrm{tr}(\rho_A^2)]}. \end{aligned} \tag{4}$$

Thus, for pure states, this generalized concurrence is simply related to the purity of the marginal density operators. A sensible choice for the constant ν_D, consistent with the concurrence for qubits, is $\nu_D=1$. We call the generalized concurrence (4) the *I concurrence* to emphasize its relation to the universal inverter and also to distinguish it from a generalized concurrence introduced by Uhlmann [7].

*Permanent address: Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 842 28 Bratislava, Slovakia, and Faculty of Informatics, Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic.

The universal inverter is a natural generalization to higher dimensions of the qubit spin flip. Only for $D=2$, the spin flip, does the universal inverter map pure states to pure states. The universal inverter cannot be realized as a quantum dynamics, because though it is a positive superoperator, it is not completely positive. In Sec. II D we explore a one-parameter family of trace-preserving superoperators that are closely related to the universal inverter, and we show that the completely positive member of this family that is closest to the universal inverter is the universal-NOT superoperator [9,10]. The universal-NOT superoperator is thus a physically realizable quantum analogue of the classical NOT gate. The action of the universal-NOT superoperator, denoted $\mathcal{G}_{\rm NOT}$, on a qudit state is given by

$$\mathcal{G}_{\rm NOT}(\rho)=\frac{1}{D^2-1}(DI-\rho)\equiv\rho^{\rm NOT}. \tag{5}$$

In Sec. III, we give two physical realizations of the universal-NOT superoperator, one in terms of the quantum information distributor introduced by Braunstein, Bužek, and Hillery [11] and the other in terms of a measurement of the isotropic POVM followed by state inversion.

The paper concludes in Sec. IV with a brief discussion that includes the natural extension of I concurrence to mixed states.

II. UNIVERSAL INVERTER

In this section, we first review in Sec. II A, Wootters's spin-flip operation for a qubit and how it leads to an entanglement measure called the concurrence for an arbitrary pure state of two qubits [6]. The main result of this paper is to generalize the spin flip to a superoperator that we call the *universal inverter*. The universal inverter is defined in all Hilbert-space dimensions, and it leads to a generalized concurrence for joint pure states of two quantum systems of arbitrary dimension. In Sec. II B, we formulate the requirements for the universal inverter and explore some of its properties. In Sec. II C, we show that these requirements pick out a unique universal inverter up to a constant multiple, and in Sec. II D, we consider trace-preserving superoperators that are closely related to the universal inverter.

The formalism we use for superoperators has been used extensively in open-systems theory [12]. The particular notation we use can be found in Ref. [13] and is summarized briefly in Appendix A, along with a description of several superoperators that play key roles in our discussion. In contrast to Ref. [13], we use $\odot$, instead of $\otimes$, to denote the slot into which one inserts the operator on which a superoperator acts, reserving $\otimes$ to denote tensor products between quantum systems. This superoperator formalism has been used to analyze entanglement in Ref. [14].

We refer to the two subsystems of a bipartite system as systems A and B. Where necessary for clarity, we use subscripts A, B, and AB to distinguish quantities belonging to the subsystems and to the joint system. To reduce notational clutter, however, we omit these subscripts on pure states, denoting pure states of a single system by a lower-case Greek letter, e.g., $|\psi\rangle$, and joint pure states of a bipartite system by an upper-case Greek letter, e.g., $|\Psi\rangle$.

A. Spin flip and qubit concurrence

A spin flip for a single qubit is effected by the antiunitary operator $\sigma_y\mathcal{C}=-\mathcal{C}\sigma_y$, where $\mathcal{C}$ denotes complex conjugation in the eigenbasis of σ_z. Acting on a state vector $|\psi\rangle$ or an operator A, the antiunitary complex conjugation operator gives $\mathcal{C}|\psi\rangle=|\psi^*\rangle$ or $\mathcal{C}A=A^*\mathcal{C}$, where $|\psi^*\rangle$ and A^* denote complex conjugation of the state or operator in the eigenbasis of σ_z. An antiunitary operator that satisfies $\Theta^2=\pm 1$, i.e., $\Theta^\dagger=\pm\Theta$, is called a *conjugation*; conjugations are ordinarily introduced in quantum mechanics to represent time reversal. Complex conjugation in some orthornormal basis is a conjugation because $\mathcal{C}^2=1$, and spin flip is a conjugation because $(\sigma_y\mathcal{C})^\dagger=\mathcal{C}^\dagger\sigma_y^\dagger=\mathcal{C}\sigma_y=-\sigma_y\mathcal{C}$. For a description of other properties and uses of antilinear operators, see Ref. [15].

Promoted to an operator on operators, the spin flip becomes an *antilinear* superoperator $\sigma_y\mathcal{C}\odot\mathcal{C}\sigma_y$, which acts on operators according to $\sigma_y\mathcal{C}A\mathcal{C}\sigma_y=\sigma_yA^*\sigma_y$. Since we are only interested in the operation of the spin flip on Hermitian operators, where complex conjugation is equivalent to transposition, we can replace this antilinear superoperator with the corresponding linear superoperator

$$\mathcal{S}_2=\sigma_y\odot\sigma_y\circ\mathcal{T}_2, \tag{6}$$

where $\mathcal{T}_2$ denotes transposition in the eigenbasis of σ_z (see Appendix A). The subscript 2 distinguishes the spin flip and transposition in two dimensions from the similar quantities for arbitrary dimensions that we introduce later in this section.

The action of the spin-flip superoperator on an arbitrary qubit density operator, $\rho=(I+\vec{P}\cdot\vec{\sigma})/2$, is to invert the Bloch vector $\vec{P}$ through the origin, as in Eq. (1). Since inversion commutes with rotations, representing unitary operators, we have immediately that $\mathcal{S}_2$ commutes with all unitary operators U, i.e., $\mathcal{S}_2\circ U\odot U^\dagger=U\odot U^\dagger\circ\mathcal{S}_2$.

For a quantum state ρ of a two-qubit system, the spin-flipped density operator, distinguished by a tilde, is

$$\tilde{\rho}=\mathcal{S}_2\otimes\mathcal{S}_2(\rho)=\sigma_y\otimes\sigma_y\rho^*\sigma_y\otimes\sigma_y. \tag{7}$$

Hill and Wootters [5] defined the concurrence of a two-qubit pure state, $\rho=|\Psi\rangle\langle\Psi|$, to be

$$\begin{aligned}C_2(\Psi)&\equiv\sqrt{\mathrm{tr}(\rho\tilde{\rho})}=\sqrt{\langle\Psi|\mathcal{S}_2\otimes\mathcal{S}_2(|\Psi\rangle\langle\Psi|)|\Psi\rangle}\\&=|\langle\Psi|\sigma_y\otimes\sigma_y|\Psi^*\rangle|.\end{aligned} \tag{8}$$

The joint pure state can be written in terms of a Schmidt decomposition,

$$|\Psi\rangle=a_1|e_1\rangle\otimes|f_1\rangle+a_2|e_2\rangle\otimes|f_2\rangle, \tag{9}$$

where $|e_j\rangle$ and $|f_j\rangle$ are the orthonormal eigenvectors of the marginal density operators for the two qubits and a_1 and a_2 are the (positive) square roots of the corresponding eigenval-

ues. Since $\mathcal{S}_2$ commutes with all unitary operators, the concurrence $C_2(\Psi)$ is unchanged by local unitary transformations. This means that $C_2(\Psi)$ is a function only of a_1 and a_2; it is easy to verify that $C_2(\Psi)=2a_1a_2$. As noted by Wootters, the concurrence can serve as a measurement of entanglement: it is invariant under local unitary transformations, as any good measure of entanglement should be, and it varies smoothly from 0 for pure product states to 1 for maximally entangled pure states.

Wootters [6] went on to show that the concurrence can also be used to measure the entanglement of mixed states of two qubits. He showed that the entanglement of formation of an arbitrary two-qubit mixed state ρ can be written in terms of the minimum average pure-state concurrence of ensemble decompositions of ρ, and he derived an explicit expression for this minimum in terms of the eigenvalues of $\rho\tilde{\rho}$. Wootters called the minimum the concurrence of the mixed state.

Uhlmann [7] based his generalization of concurrence on the fact that the spin flip is a conjugation, defining concurrence in arbitrary dimensions in terms of a conjugation Θ. Following Uhlmann, we call his concurrence the Θ *concurrence*, and we discuss it further in the next subsection.

B. Universal inverter and I concurrence

Our goal in this paper is to generalize the spin-flip superoperator $\mathcal{S}_2$ for a qubit to a superoperator $\mathcal{S}_D$ that acts on qudit states and generates a generalized concurrence for $D_1\times D_2$ bipartite quantum systems. The spin-flip superoperator has several important properties that we might wish its generalization to retain:

(1) $\mathcal{S}_2$ maps Hermitian operators to Hermitian operators.

(2) $\mathcal{S}_2$ commutes with all unitary operators.

(3) $\langle\Psi|\mathcal{S}_2\otimes\mathcal{S}_2(|\Psi\rangle\langle\Psi|)|\Psi\rangle$ is nonnegative for all joint pure states $|\Psi\rangle$ and goes to zero if and only if $|\Psi\rangle$ is a product state.

(4) $\mathcal{S}_2$ is a positive superoperator; i.e., it maps positive operators to positive operators.

(5) $\mathcal{S}_2$ is trace preserving.

(6) $\mathcal{S}_2$ maps any pure state $|\psi\rangle\langle\psi|$ to the orthogonal pure state $|\psi^\perp\rangle\langle\psi^\perp|$.

(7) $\mathcal{S}_2$ is derived from a conjugation Θ, i.e., an antiunitary operator satisfying $\Theta^2=\pm 1$.

Property (1) guarantees that $\mathcal{S}_2\otimes\mathcal{S}_2$ maps Hermitian operators to Hermitian operators (see Appendix B) and thus that the quantity $\langle\Psi|\mathcal{S}_2\otimes\mathcal{S}_2(|\Psi\rangle\langle\Psi|)|\Psi\rangle$ of property (3) is real. Property (2) ensures that $C_2(\Psi)$ is unchanged by local unitary transformations, as an entanglement measure should be. Property (3) makes $C_2(\Psi)$ well defined, by ensuring that the quantity inside the square root is non-negative, and it sets the zero so that pure product states, but no other pure states, have vanishing concurrence.

In generalizing the spin flip to higher dimensions, we want the generalized concurrence of a pure state $\rho=|\Psi\rangle\langle\Psi|$ of a $D_1\times D_2$ bipartite system to be defined as for qubits, i.e.,

$$C(\Psi)\equiv\sqrt{\langle\Psi|\mathcal{S}_{D_1}\otimes\mathcal{S}_{D_2}(|\Psi\rangle\langle\Psi|)|\Psi\rangle}. \tag{10}$$

It is clear that the analogues of properties (1)–(3) are desirable properties of $\mathcal{S}_D$, for the same reasons as for qubits, and it turns out that they are sufficient to pick out a unique superoperator $\mathcal{S}_D$ up to a constant multiple.

The upshot of this discussion is that we require $\mathcal{S}_D$ to have the following properties:

(1′) $\mathcal{S}_D$ maps Hermitian operators to Hermitian operators.

(2′) $\mathcal{S}_D$ commutes with all unitary operators.

(3′) $\langle\Psi|\mathcal{S}_{D_1}\otimes\mathcal{S}_{D_2}(|\Psi\rangle\langle\Psi|)|\Psi\rangle$ is non-negative for all joint pure states $|\Psi\rangle$ and goes to zero if and only if $|\Psi\rangle$ is a product state.

The only superoperator that has these three properties is

$$\mathcal{S}_D=\nu_D(\mathbf{I}-\mathcal{I}), \tag{11}$$

where $\mathbf{I}$ is the unit superoperator relative to the left-right action, $\mathcal{I}$ is the unit superoperator relative to the ordinary action, and ν_D is an arbitrary real constant. For the considerations in Sec. II D, we allow ν_D to have a dependence on D. For purposes of defining a generalized concurrence, however, ν_D should be independent of D; otherwise the generalized concurrence of a joint pure state could be changed simply by adding extra, unused dimensions to one or both systems.

We show that $\mathcal{S}_D$ is the *only* superoperator allowed by properties (1′)–(3′) in Sec. II C. For the remainder of this subsection, we show that $\mathcal{S}_D$ does satisfy properties (1′)–(3′), and we spell out some of its other properties and properties of the corresponding concurrence. Notice, first, that $\mathcal{S}_D$ takes an operator A to

$$\mathcal{S}_D(A)=\nu_D[\mathbf{I}(A)-\mathcal{I}(A)]=\nu_D[\mathrm{tr}(A)I-A], \tag{12}$$

from which it is clear that $\mathcal{S}_D$ satisfies properties (1′) and (2′). If A is a density operator ρ, we get

$$\mathcal{S}_D(\rho)=\nu_D(I-\rho). \tag{13}$$

Since $I-\rho$ is a positive operator for any ρ, we have immediately that $\mathcal{S}_D$ is a positive superoperator provided that ν_D is positive. The generalized concurrence is indifferent to a change in the sign of ν_D, so we are free to choose ν_D to be positive, which we do henceforth, thus making $\mathcal{S}_D$ positive. If $\nu_D=1/(D-1)$, $\mathcal{S}_D$ is trace preserving; this trace-preserving normalization is useful for the considerations of Sec. II D, but we see below that $\nu_D=1$ is a more reasonable normalization to use for the generalized concurrence $C(\Psi)$. Finally, $\mathcal{S}_D$ maps a pure state $\rho=|\psi\rangle\langle\psi|$ to a positive multiple of the projector orthogonal to ρ:

$$\mathcal{S}_D(|\psi\rangle\langle\psi|)=\nu_D(I-|\psi\rangle\langle\psi|). \tag{14}$$

It is this property that prompts us to call $\mathcal{S}_D$ the *universal inverter*. We call the corresponding generalized concurrence (10) the *I concurrence* to emphasize its connection with inversion. Other properties of $\mathcal{S}_D$, which follow directly from the corresponding properties of $\mathbf{I}$ and $\mathcal{I}$ (see Appendix A), are that $\mathcal{S}_D$ is Hermitian relative to the ordinary action, i.e., $\mathcal{S}_D^\times=\mathcal{S}_D$, and that it changes sign under sharping, i.e., $\mathcal{S}_D^\#$

$=-\mathcal{S}_D$. The universal inverter has been used previously by Horodecki and Horodecki [8] to provide a criterion for the separability of mixed states.

We now see that properties (4)–(6) of the qubit spin flip survive, in amended form, in its generalization:

(4′) $\mathcal{S}_D$ is a positive superoperator.

(5′) $\mathcal{S}_D$ is a positive multiple of a trace-preserving superoperator, i.e., $\mathcal{S}_D^{\times}(I)=\nu_D(D-1)I$.

(6′) $\mathcal{S}_D$ maps any pure state $|\psi\rangle\langle\psi|$ to a positive multiple of the projector onto the subspace orthogonal to $|\psi\rangle$.

It is worth pointing out that if we added to properties (1′)–(3′) the additional requirement that $\mathcal{S}_D$ map each pure state to a multiple of some orthogonal state, then the superoperator of Eq. (11) would trivially be the only possibility for the universal inverter.

We still have to deal with property 3′. For that purpose, we need the tensor-product superoperator

$$\mathcal{S}_{D_1}\otimes\mathcal{S}_{D_2}=\nu_{D_1}\nu_{D_2}(\mathbf{I}\otimes\mathbf{I}-\mathcal{I}\otimes\mathbf{I}-\mathbf{I}\otimes\mathcal{I}+\mathcal{I}\otimes\mathcal{I}). \quad (15)$$

Applied to an arbitrary joint density operator ρ_{AB}, this tensor-product superoperator gives

$$\mathcal{S}_{D_1}\otimes\mathcal{S}_{D_2}(\rho_{AB})=\nu_{D_1}\nu_{D_2}(I\otimes I-\rho_A\otimes I-I\otimes\rho_B+\rho_{AB}). \quad (16)$$

Projecting back onto ρ_{AB} gives

$$\mathrm{tr}(\rho_{AB}\mathcal{S}_{D_1}\otimes\mathcal{S}_{D_2}(\rho_{AB})) = \nu_{D_1}\nu_{D_2}[1-\mathrm{tr}(\rho_A^2)-\mathrm{tr}(\rho_B^2)+\mathrm{tr}(\rho_{AB}^2)]\geqslant 0. \quad (17)$$

The inequality here, which shows that the quantity in property (3′) is non-negative, is proved in Appendix C, where it is also shown that the inequality is saturated if and only if $\rho_{AB}=\rho_A\otimes\rho_B$ is a product state, with ρ_A or ρ_B a pure state. For a joint pure state ρ_{AB}, this establishes property (3′).

It is useful to specialize Eq. (17) to a joint pure state $|\Psi\rangle$, in which case it becomes the square of the pure-state I concurrence:

$$C^2(\Psi)=\langle\Psi|\mathcal{S}_{D_1}\otimes\mathcal{S}_{D_2}(|\Psi\rangle\langle\Psi|)|\Psi\rangle = 2\nu_{D_1}\nu_{D_2}[1-\mathrm{tr}(\rho_A^2)]. \quad (18)$$

Thus, the I concurrence measures the entanglement of a pure state in terms of the purity, $\mathrm{tr}(\rho_A^2)=\mathrm{tr}(\rho_B^2)$, of the marginal density operators. A joint pure state has a Schmidt decomposition,

$$|\Psi\rangle=\sum_j a_j|e_j\rangle\otimes|f_j\rangle, \quad a_j>0, \quad (19)$$

in terms of which the squared I concurrence becomes

$$C^2(\Psi)=2\nu_{D_1}\nu_{D_2}\left(1-\sum_j a_j^4\right)=4\nu_{D_1}\nu_{D_2}\sum_{j<k}a_j^2a_k^2. \quad (20)$$

For defining a concurrence, one should choose the scaling factor ν_D to be independent of D—otherwise, as noted above, the pure state I concurrence could be changed simply by adding extra, unused dimensions to one of the subsystems—and to be consistent with the qubit concurrence, one should choose $\nu_D=1$. With this choice, the pure-state I concurrence runs from zero for product states to $\sqrt{2(M-1)/M}$, where $M=\min(D_1,D_2)$, for a maximally entangled state.

Of the seven properties of the spin flip listed above, the first six survive, some in amended form, in the universal inverter. The seventh, that $\mathcal{S}_2$ is derived from a conjugation, is not a property of $\mathcal{S}_D$, because except in two dimensions, a conjugation cannot commute with all unitaries, and thus, cannot serve as the basis for a measure of entanglement. Uhlmann's work on conjugations [7] is valuable in that it generalizes to all conjugations the expression that Wootters gives for the minimum average pure-state concurrence of a bipartite density operator ρ in terms of the eigenvalues of $\rho\tilde{\rho}$. Our results show, however, that Uhlmann's Θ concurrence [7], founded as it is on the use of conjugations, cannot serve as the basis for a general measure of entanglement.

There is another interesting form of the universal inverter, which makes a direct connection to the form (7) of the spin flip. Choosing an orthonormal basis $|e_j\rangle$, let $\mathcal{T}$ be the superoperator that transposes matrix representations in this basis, and let $\mathcal{P}_A$ be the superoperator projector, relative to the left-right action, which projects onto the subspace of operators that are antisymmetric in this basis. We show in Appendix A that

$$\mathcal{S}_D/\nu_D=2\,\mathcal{P}_A\circ\mathcal{T}. \quad (21)$$

This form of the universal inverter has been given previously by Horodecki and Horodecki [8]. For qubits, if we use the eigenstates of σ_z as the chosen basis, then the antisymmetric operator subspace is spanned by the normalized operator $\sigma_y/\sqrt{2}$, so the projector onto this subspace is $\mathcal{P}_A=|\sigma_y)(\sigma_y|/2=\sigma_y\odot\sigma_y/2$. Thus, in the two dimensions the universal inverter becomes $\mathcal{S}_2=\nu_2\sigma_y\odot\sigma_y\circ\mathcal{T}_2$, which agrees with the spin flip if $\nu_2=1$.

C. Derivation of universal inverter

We now show that the only superoperator that satisfies properties (1′)–(3′) of the preceding subsection is the universal inverter (11). As we proceed through the proof, we use $\mathcal{G}_D$ to denote the operator under consideration.

As we show in Appendix B, property (1′) implies that $\mathcal{G}_D$ is left-right Hermitian, i.e., $\mathcal{G}_D=\mathcal{G}_D^{\dagger}$, and thus, has an eigendecomposition

$$\mathcal{G}_D=\sum_\alpha \mu_\alpha|\tau_\alpha)(\tau_\alpha|=\sum_\alpha \mu_\alpha\tau_\alpha\odot\tau_\alpha^{\dagger}, \quad (22)$$

where the μ_α are real (left-right) eigenvalues and the operators τ_α are the corresponding orthonormal eigenoperators.

Property (2′) implies that

$$\mathcal{G}_D = U^\dagger \odot U \circ \mathcal{G}_D \circ U \odot U^\dagger = \sum_\alpha \mu_\alpha U^\dagger \tau_\alpha U \odot U^\dagger \tau_\alpha^\dagger U, \tag{23}$$

which means that $U^\dagger \tau_\alpha U$ is an eigenoperator of $\mathcal{G}_D$, with eigenvalue μ_α, for any unitary operator U. This result can be restated as saying that the degenerate eigensubspaces of $\mathcal{G}_D$ are invariant under all unitary transformations. We show in Appendix D that the only operator subspaces that are invariant under all unitary transformations are the one-dimensional subspace spanned by the unit operator and the (D^2-1)-dimensional subspace of trace-free operators. As a consequence, $\mathcal{G}_D$ must have the form

$$\mathcal{G}_D = \mu_D \mathcal{I}/D + \nu_D \mathcal{F}. \tag{24}$$

Here, $\mathcal{I} = I \odot I$ is the unit superoperator relative to the ordinary action, $\mathcal{F}$ is the superoperator that projects onto the subspace of trace-free operators when acting to the right (see Appendix A), μ_D is the eigenvalue of $\mathcal{G}_D$ corresponding to the normalized eigenoperator $I/\sqrt{D}$, and ν_D is the eigenvalue corresponding to all of the tracefree operators. Notice that $\mathcal{G}_D$ is Hermitian relative to the ordinary action, i.e., $\mathcal{G}_D = \mathcal{G}_D^\times$.

If we add $I/\sqrt{D}$ to a complete, orthonormal set of trace-free operators, we obtain a complete, orthonormal set of operators, so the unit superoperator in the left-right sense is given by

$$\mathbf{I} = \mathcal{I}/D + \mathcal{F}, \tag{25}$$

from which we get

$$\mathcal{G}_D = \eta_D \mathcal{I} + \nu_D \mathbf{I}, \tag{26}$$

where

$$\eta_D = (\mu_D - \nu_D)/D. \tag{27}$$

Now we impose property $(3')$. In doing so, it is sufficient to consider the requirements of property $(3')$ in the case where the two subsystems have the same dimension D. In this case, the tensor-product superoperator takes the form

$$\mathcal{G}_D \otimes \mathcal{G}_D = \eta_D^2 \mathcal{I}\otimes\mathcal{I} + \eta_D \nu_D (\mathcal{I}\otimes\mathbf{I} + \mathbf{I}\otimes\mathcal{I}) + \nu_D^2 \mathbf{I}\otimes\mathbf{I}. \tag{28}$$

Applying this superoperator to a joint density operator ρ_{AB} gives

$$\mathcal{G}_D \otimes \mathcal{G}_D(\rho_{AB}) = \eta_D^2 \rho_{AB} + \eta_D \nu_D (\rho_A \otimes I + I \otimes \rho_B) + \nu_D^2 I \otimes I, \tag{29}$$

and projecting this back onto ρ_{AB} yields

$$\begin{aligned} &\mathrm{tr}(\rho_{AB} \mathcal{G}_D \otimes \mathcal{G}_D(\rho_{AB})) \\ &\quad = \eta_D^2 \mathrm{tr}(\rho_{AB}^2) + \eta_D \nu_D [\mathrm{tr}(\rho_A^2) + \mathrm{tr}(\rho_B^2)] + \nu_D^2. \end{aligned} \tag{30}$$

Specializing to a joint pure state $|\Psi\rangle$, we get

$$\begin{aligned} \langle\Psi|\mathcal{G}_D \otimes \mathcal{G}_D(|\Psi\rangle\langle\Psi|)|\Psi\rangle &= \eta_D^2 + \nu_D^2 + 2\eta_D \nu_D \,\mathrm{tr}(\rho_A^2) \\ &= (\eta_D \mp \nu_D)^2 \pm 2\eta_D \nu_D \\ &\quad \times [1 \pm \mathrm{tr}(\rho_A^2)]. \end{aligned} \tag{31}$$

If $\eta_D \nu_D \geqslant 0$, the top sign in Eq. (31) shows that the quantity in property $(3')$ is strictly positive, unless $\eta_D = \nu_D = 0$, a case of no interest. If $\eta_D \nu_D < 0$, the bottom sign in Eq. (31) shows that the quantity is nonnegative and goes to zero if and only if $\eta_D = -\nu_D$ and ρ_A is pure, i.e., the joint pure state is a product state. Thus, it turns out that the quantity in property $(3')$ is non-negative for all superoperators of the form (26), but the only way to set the zero properly is to choose $\eta_D = -\nu_D$, thus giving the universal inverter of Eq. (11). The left-right eigenvalues of the universal inverter are ν_D and $\mu_D = D\eta_D + \nu_D = -(D-1)\nu_D$.

D. Trace-preserving superoperators

All superoperators of the form (26) are proportional to a trace-preserving superoperator, since

$$\mathcal{G}_D^\times(I) = \mathcal{G}_D(I) = (\eta_D + D\nu_D) I. \tag{32}$$

Requiring $\mathcal{G}_D$ to be trace preserving gives the condition

$$\eta_D = 1 - D\nu_D \tag{33}$$

$[\mu_D = D - \nu_D(D^2-1)]$, which allows us to eliminate one parameter and to write the trace-preserving version of $\mathcal{G}_D$ as

$$\mathcal{G}_{DT} = (1 - D\nu_D)\mathcal{I} + \nu_D \mathbf{I}. \tag{34}$$

Acting on an arbitrary input state ρ, this superoperator gives

$$\mathcal{G}_{DT}(\rho) = (1 - D\nu_D)\rho + \nu_D I. \tag{35}$$

It is instructive to investigate this one-parameter family of trace-preserving operators.

We first ask which of the trace-preserving operators (34) are completely positive. The condition that a superoperator be completely positive is that its left-right eigenvalues be non-negative (see Appendix A). Thus, the condition for the complete positivity of $\mathcal{G}_{DT}$ is that $\mu_D \geqslant 0$ and $\nu_D \geqslant 0$, which is equivalent to

$$0 \leqslant \nu_D \leqslant \frac{D}{D^2-1}. \tag{36}$$

When $\nu_D = 0$, $\mathcal{G}_{DT} = \mathcal{I}$ is the unit superoperator, and when $\nu_D = D/(D^2-1)$,

$$\mathcal{G}_{DT} = \frac{D}{D^2-1}\mathcal{F} = \frac{1}{D^2-1}(D\mathbf{I} - \mathcal{I}) \equiv \mathcal{G}_{\mathrm{NOT}} \tag{37}$$

is the universal-NOT superoperator [9,10]. Notice that the universal-NOT superoperator is a multiple of $\mathcal{F}$, the superoperator whose right action projects onto the subspace of trace-free operators. Since the dynamics of a quantum system must be completely positive, the universal-NOT superoperator is the closest physical approximation to the universal inverter

in the one-parameter family (35); it is the quantum analogue of the classical NOT gate. We present a realization of the universal-NOT superoperator in Sec. III.

Another interesting completely positive superoperator occurs for $\nu_D=1/(D+1)$:

$$\mathcal{G}_{DT}=\frac{1}{D+1}(\mathbf{I}+\mathcal{I})=\frac{1}{D}\mathcal{I}+\frac{1}{D+1}\mathcal{F}\equiv\mathcal{G}_{\mathrm{AV}}. \tag{38}$$

This superoperator was used to generate operator expansions in Ref. [14], where it was shown that it is the unique trace-preserving superoperator that satisfies $\mathcal{G}=\mathcal{G}^{\dagger}=\mathcal{G}^{\times}=\mathcal{G}^{\#}$ and commutes with all unitaries. In contrast, the universal inverter is the unique superoperator that satisfies $\mathcal{G}=\mathcal{G}^{\dagger}=\mathcal{G}^{\times}=-\mathcal{G}^{\#}$ and commutes with all unitaries.

As shown in Ref. [14], the superoperator $\mathcal{G}_{\mathrm{AV}}$ is the trace-preserving version of the superoperator that describes projection onto a random pure state,

$$\mathcal{G}_{\mathrm{AV}}=D\int\frac{d\mathcal{V}}{\mathcal{V}}|\psi\rangle\langle\psi|\odot|\psi\rangle\langle\psi|, \tag{39}$$

where $d\mathcal{V}$ is the unitarily invariant integration measure on projective Hilbert space and $\mathcal{V}$ is the corresponding total volume. Projection onto a random pure state is the measurement that results in the optimal estimation of the state of the qudit [16]. This estimated state is given by the density operator

$$\mathcal{G}_{\mathrm{AV}}(\rho)=\frac{1}{D+1}(I+\rho). \tag{40}$$

The superoperator $\mathcal{G}_{\mathrm{AV}}$ returns in Sec. III as an ingredient in one of the physical realizations of the universal-NOT superoperator.

We now consider which of the trace-preserving operators (34) are positive. Letting p_j be the eigenvalues of the input density operator ρ, one sees that the eigenvalues of $\mathcal{G}_{DT}(\rho)$ [Eq. 35)] are $(1-D\nu_D)p_j+\nu_D$. The condition that $\mathcal{G}_{DT}$ be positive is that these eigenvalues be non-negative for all input eigenvalues p_j, which is equivalent to

$$0\leqslant\nu_D\leqslant\frac{1}{D-1}. \tag{41}$$

When $\nu_D=1/(D-1)$, $\mathcal{G}_{DT}$ becomes the trace-preserving version of the universal inverter,

$$\mathcal{S}_{DT}=\frac{1}{D-1}(\mathbf{I}-\mathcal{I}). \tag{42}$$

The positive superoperators are convex combinations of $\mathcal{I}$ and $\mathcal{S}_{DT}$:

$$\mathcal{G}_{DT}=[1-\nu_D(D-1)]\mathcal{I}+\nu_D(D-1)\mathcal{S}_{DT}. \tag{43}$$

Notice that the universal-NOT superoperator can be written as

$$\mathcal{G}_{\mathrm{NOT}}=\frac{1}{2}(\mathcal{S}_{DT}+\mathcal{G}_{\mathrm{AV}}). \tag{44}$$

III. PHYSICAL REALIZATIONS OF THE UNIVERSAL-NOT SUPEROPERATOR

In this section we give two physical realizations of the universal-NOT superoperator $\mathcal{G}_{\mathrm{NOT}}$ of Eq. (37), the first in terms of the quantum information distributor introduced by Braunstein, Bužek, and Hillery [11] and the second in terms of a measurement of the isotropic POVM followed by state inversion.

For the first, consider a qudit in a pure state $\rho=|\psi\rangle\langle\psi|$. As shown in Sec. II, the ideal inversion of this state is given by

$$\mathcal{S}_{DT}(\rho)=\frac{1}{D-1}(I-\rho)\equiv\rho^{\perp}, \tag{45}$$

where $\mathcal{S}_{DT}$ is the trace-preserving version of the universal inverter [see Eq. (42)]. The inverted state $\rho^{\perp}$ is the maximally mixed state in the $(D-1)$-dimensional subspace orthogonal to the input state $\rho=|\psi\rangle\langle\psi|$. Notice that by construction, $\mathrm{tr}(\rho\rho^{\perp})=0$ for pure input states.

As shown in Sec. II D, the trace-preserving universal inverter $\mathcal{S}_{\mathrm{DT}}$ is a positive, but not completely positive superoperator and as such cannot be realized physically. In the one-parameter family of trace-preserving inverters considered in Sec. II D, the universal-NOT superoperator $\mathcal{G}_{\mathrm{NOT}}$ of Eq. (37) is the closest completely positive superoperator to the universal inverter. We denote the physically possible inversion of the state ρ obtained using the universal-NOT superoperator as

$$\rho^{\mathrm{NOT}}\equiv\mathcal{G}_{\mathrm{NOT}}(\rho)=\frac{1}{D^2-1}(DI-\rho). \tag{46}$$

In order to realize the universal-NOT superoperator, we couple the qudit to be inverted, denoted by A, to the quantum information distributor (QID) introduced in Ref. [11]. The QID is composed of two ancilla qudits, B and C, each of which has the same dimension D as qudit A. To describe the universal inverter, we introduce several operators and states for qudits.

First we need the conjugate ''position'' and ''momentum'' operators, x and p. The eigenvectors of x are denoted by $|x_k\rangle$,

$$x|x_k\rangle=x_k|x_k\rangle, \tag{47}$$

with the eigenvalues given by $x_k=k\sqrt{2\pi/D}$; analogously, the eigenstates of p are denoted by $|p_k\rangle$,

$$p|p_k\rangle=p_k|p_k\rangle, \tag{48}$$

with the eigenvalues given by $p_k=k\sqrt{2\pi/D}$. We use units such that the two operators are dimensionless. The two sets of eigenvectors, $\{|x_k\rangle\}$ and $\{|p_k\rangle\}$, form bases in the qudit Hilbert space and are related by a discrete Fourier transform,

$$|x_k\rangle=\frac{1}{\sqrt{D}}\sum_{l=0}^{D-1}e^{-2\pi ikl/D}|p_l\rangle, \tag{49}$$

$$|p_l\rangle = \frac{1}{\sqrt{D}} \sum_{k=0}^{D-1} e^{2\pi i k l/D} |x_k\rangle. \tag{50}$$

The translation (shift) operators, defined by

$$R_x(n) = e^{-ix_n p}, \quad R_p(m) = e^{ip_m x}, \tag{51}$$

cyclically permute the basis vectors according to

$$R_x(n)|x_k\rangle = |x_{(k+n) \bmod D}\rangle, \tag{52}$$

$$R_p(m)|p_l\rangle = |p_{(l+m) \bmod D}\rangle, \tag{53}$$

where the sums of indices are taken modulo D.

An orthonormal basis of D^2 two-qudit maximally entangled states $|\Xi_{mn}\rangle$ is given by

$$|\Xi_{mn}\rangle = \frac{1}{\sqrt{D}} \sum_{k=0}^{D-1} e^{2\pi i m k/D} |x_k\rangle \otimes |x_{(k+n) \bmod D}\rangle, \tag{54}$$

where $m,n = 0, \ldots, D-1$. Using Eq. (49), we can rewrite the states $|\Xi_{mn}\rangle$ in the joint momentum basis

$$|\Xi_{mn}\rangle = \frac{1}{\sqrt{D}} \sum_{l=0}^{D-1} e^{-2\pi i n l/D} |p_{(m-l) \bmod D}\rangle \otimes |p_l\rangle. \tag{55}$$

The state $|\Xi_{00}\rangle$ can be written as

$$|\Xi_{00}\rangle = \frac{1}{\sqrt{D}} \sum_{k=0}^{D-1} |x_k\rangle \otimes |x_k\rangle = \frac{1}{\sqrt{D}} \sum_{l=0}^{D-1} |p_{-l \bmod D}\rangle \otimes |p_l\rangle. \tag{56}$$

It is interesting to note that the whole set of D^2 maximally entangled states $|\Xi_{mn}\rangle$ can be generated from $|\Xi_{00}\rangle$ by the action of *local* unitary operations (shifts):

$$|\Xi_{mn}\rangle = R_p(m) \otimes R_x(n) |\Xi_{00}\rangle. \tag{57}$$

Now we are ready to describe the QID. The ancilla qudits, B and C, are initially prepared in the state

$$|\Phi\rangle_{BC} = \xi_1 |\Xi_{00}\rangle_{BC} + \xi_2 |x_0\rangle_B \otimes |p_0\rangle_C. \tag{58}$$

The phase freedom in $|\Phi\rangle_{BC}$ can be used to make ξ_1 real and non-negative, but then ξ_2 is in general complex. We do not use the freedom to make ξ_1 non-negative, thereby retaining for use below the ability to multiply both ξ_1 and ξ_2 by -1.

Normalization of $|\Phi_{BC}\rangle$ imposes the constraint

$$1 = \xi_1^2 + |\xi_2|^2 + \frac{\xi_1(\xi_2 + \xi_2^*)}{D} = \xi_1^2 + a^2 + b^2 + \frac{2a\xi_1}{D}, \tag{59}$$

where $\xi_2 = a + ib$. Solving for ξ_1, we get

$$\xi_1 = -\frac{a}{D} + \sqrt{1 - b^2 - a^2 \frac{D^2-1}{D^2}}. \tag{60}$$

We discard the other solution of the quadratic equation, because it can be converted to this solution by multiplying both ξ_1 and ξ_2 by -1. Since ξ_1 is real, we must have

$$\frac{D^2-1}{D^2} a^2 + b^2 \leqslant 1, \tag{61}$$

which means that ξ_2 lies on or within an ellipse that has principal radius $D/\sqrt{D^2-1} \geqslant 1$ along the real axis and principal radius 1 along the imaginary axis. Therefore, we conclude that

$$0 \leqslant |\xi_2|^2 \leqslant \frac{D^2}{D^2-1}. \tag{62}$$

It is easy to see that the minimum value of ξ_1 occurs when $\xi_2 = D/\sqrt{D^2-1}$, this minimum value being $\xi_1 = -1/\sqrt{D^2-1}$. It is also easy to see that the maximum value of ξ_1 occurs when ξ_2 is real; the maximum occurs at $\xi_2 = -1/\sqrt{D^2-1}$ and is given by $\xi_1 = D/\sqrt{D^2-1}$. The upshot is that ξ_1 is bounded by

$$-\frac{1}{\sqrt{D^2-1}} \leqslant \xi_1 \leqslant \frac{D}{\sqrt{D^2-1}}. \tag{63}$$

The negative values of ξ_1 are unimportant, because they can be converted to positive values by multiplying both ξ_1 and ξ_2 by -1. What is important is that $|\xi_1|^2$ has the same range of possible values as $|\xi_2|^2$.

We now allow qudit A to interact with the two ancilla qudits, the resulting dynamics described by the unitary operator

$$U_{ABC} = \exp[-i(x_C - x_B)p_A] \exp[-ix_A(p_B + p_C)], \tag{64}$$

(for more details, see Ref. [11]). For an initial pure state $|\psi\rangle$ of qudit A, the joint state after the interaction is

$$U_{ABC} |\psi\rangle_A \otimes |\Phi\rangle_{BC} = \xi_1 |\psi\rangle_A \otimes |\Xi_{00}\rangle_{BC} + \xi_2 |\psi\rangle_B \otimes |\Xi_{00}\rangle_{AC}. \tag{65}$$

The output states of the individual qudits after tracing out the other two qudits are

$$\rho_A^{(\mathrm{out})} = \left(\xi_1^2 + \frac{\xi_1(\xi_2 + \xi_2^*)}{D} \right) \rho + \frac{|\xi_2|^2}{D} I, \tag{66}$$

$$\rho_B^{(\mathrm{out})} = \left(|\xi_2|^2 + \frac{\xi_1(\xi_2 + \xi_2^*)}{D} \right) \rho + \frac{\xi_1^2}{D} I, \tag{67}$$

$$\rho_C^{(\mathrm{out})} = \frac{\xi_1(\xi_2 + \xi_2^*)}{D} \rho^T + \frac{\xi_1^2 + |\xi_2|^2}{D} I, \tag{68}$$

where ρ is an arbitrary initial state of qudit A and ρ^T is its transpose. Taking into account the constraint (59), we can rewrite the output states of qudits A and B as

$$\rho_A^{(\mathrm{out})} = (1 - |\xi_2|^2)\rho + |\xi_2|^2 I/D, \tag{69}$$

$$\rho_B^{(\mathrm{out})}=(1-\xi_1^2)\rho+\xi_1^2 I/D. \tag{70}$$

As far as qudit A is concerned, the QID acts like the superoperator $\mathcal{G}_{DT}$ of Eqs. (34) and (35) with $D\nu_D=|\xi_2|^2$. As far as qudit B is concerned, the QID first swaps the states of A and B and then acts like $\mathcal{G}_{DT}$ with $D\nu_D=\xi_1^2$.

Rewriting the output state of qudit A in terms of the ideal inverted state $\rho^{\perp}=(I-\rho)/(D-1)$, we get

$$\rho_A^{(\mathrm{out})}=(|\xi_2|^2-1)(D-1)\rho^{\perp}+[D-|\xi_2|^2(D-1)]I/D. \tag{71}$$

To make $\rho_A^{(\mathrm{out})}$ as close as possible to $\rho^{\perp}$, we need to maximize $|\xi_2|^2$; i.e., we need to choose

$$D\nu_D=|\xi_2|^2=\frac{D^2}{D^2-1}, \tag{72}$$

thus making the action of the QID on qudit A the same as the action of the universal-NOT superoperator given in Eq. (46). Notice that the QID gives the superoperator $\mathcal{G}_{\mathrm{AV}}$ of Eq. (38) when $D\nu_D=|\xi_2|^2=D/(D+1)$.

When $|\xi_2|^2$ has its maximum value, $\xi_1^2=1/(D^2-1)$, so the output state (70) of qudit B becomes

$$\rho_B^{(\mathrm{out})}=\left(1-\frac{1}{D^2-1}\right)\rho+\frac{1}{(D^2-1)}\frac{I}{D}. \tag{73}$$

Notice that in the limit of large D, we have $|\xi_2|\to 1$ and $\xi_1\to 0$. The output state of qudit B reduces to the input state of qudit A, and the output states of A and C reduce to the maximally mixed state I/D. All this is a consequence of the fact that the initial state of qudits B and C limits to $|\Phi\rangle_{BC}\to|x_0\rangle_B\otimes|p_0\rangle_C$, and the QID swaps the states of A and B

$$U_{ABC}|\psi\rangle_A\otimes|\Xi_{00}\rangle_{BC}=|\psi\rangle_B\otimes|\Xi_{00}\rangle_{AC}. \tag{74}$$

Our second realization of the universal-NOT superoperator starts with a measurement of the isotropic POVM

$$dE(|\psi\rangle)=D\frac{d\mathcal{V}}{\mathcal{V}}|\psi\rangle\langle\psi|, \tag{75}$$

where

$$\int dE(|\psi\rangle)=D\int\frac{d\mathcal{V}}{\mathcal{V}}|\psi\rangle\langle\psi|=I. \tag{76}$$

We assume that the measurement projects the system onto the measured state, so the operation that describes a measurement whose result is the state $|\psi\rangle$ is

$$d\mathcal{A}(|\psi\rangle)=D\frac{d\mathcal{V}}{\mathcal{V}}|\psi\rangle\langle\psi|\odot|\psi\rangle\langle\psi|. \tag{77}$$

Knowing that the system is in the state $|\psi\rangle$, we can invert the state. The operation that describes the measurement followed by inversion is $\mathcal{S}_{DT}\circ d\mathcal{A}(|\psi\rangle)$, where $\mathcal{S}_{DT}$ is the trace-preserving version of the universal inverter. If we now throw away the result of the measurement of the isotropic POVM, the resulting trace-preserving operation is

$$\int \mathcal{S}_{DT}\circ d\mathcal{A}(|\psi\rangle)=\mathcal{S}_{DT}\circ\mathcal{G}_{\mathrm{AV}}, \tag{78}$$

where $\mathcal{G}_{\mathrm{AV}}$ is the superoperator that describes projection onto a random pure state [see Eq. (39)].

Using the forms (42) and (38), we can write the overall operation as

$$\mathcal{S}_{DT}\circ\mathcal{G}_{\mathrm{AV}}=\frac{1}{D^2-1}(\mathbf{I}-\mathcal{I})\circ(\mathbf{I}+\mathcal{I})=\frac{1}{D^2-1}(D\mathbf{I}-\mathcal{I})=\mathcal{G}_{\mathrm{NOT}}, \tag{79}$$

where we use the fact that $\mathbf{I}\circ\mathbf{I}=D\mathbf{I}$. This demonstrates that the universal-NOT superoperator results from a measurement of the isotropic POVM followed by state inversion.

IV. CONCLUSION

The concurrence introduced by Hill and Wootters [5] and by Wootters [6] provides a good measure of the entanglement of any state of two qubits, pure or mixed. The Hill-Wootters concurrence is generated with the help of the superoperator that flips the spin of a qubit. In this paper, we have identified the crucial properties of the spin-flip superoperator, which allow it to generate a good entanglement measure for pure states of two qubits. By generalizing these properties to systems of arbitrary dimension, we have singled out a unique superoperator, which we call the universal inverter. In the same way that the spin flip generates a concurrence for pairs of qubits, the universal inverter generates a concurrence, which we call the I concurrence, for joint pure states of pairs of quantum systems of arbitrary dimension. This pure-state I concurrence measures entanglement in terms of the purity of the marginal density operators of the joint pure state.

It is natural to define the I concurrence of mixed states of $D_1\times D_2$ quantum systems as the minimum average I concurrence of ensemble decompositions of the joint density operator. Property (3′) of the I concurrence—that the I concurrence of a pure state $|\Psi\rangle$ is zero if and only if $|\Psi\rangle$ is a product state—implies immediately that the mixed-state concurrence just defined is zero if and only if the mixed state is separable. We are investigating further properties of this mixed-state I concurrence and how it is related to other measures of mixed-state entanglement.

The universal inverter turns out to be the ideal inverter of pure states, since it takes a pure state to the maximally mixed state in the subspace orthogonal to the pure state. Because the universal inverter is a positive, but not completely positive superoperator, it cannot be realized as the dynamics of a quantum system coupled to an ancilla. We have shown that among a one-parameter family of inverting superoperators, the completely positive superoperator that comes closest to achieving an ideal state inversion is a superoperator called the universal-NOT superoperator, and we have presented a physical realization of the universal-NOT.

ACKNOWLEDGMENTS

This work was supported in part by the Office of Naval Research (Grant No. N00014-00-1-0578), the EQUIP project of the European Union Fifth Framework research program, Information Society Technologies (Contract No. IST-1999-11053), and the National Science Foundation (Grant No. PHY-9970507).

APPENDIX A: SUPEROPERATOR FORMALISM AND SPECIAL SUPEROPERATORS

The formalism we use for superoperators has been used extensively in open-systems theory [12]. In this appendix, we summarize our notation, which follows that of Ref. [13], and we introduce and describe key properties of several superoperators that are important for our analysis.

The space of linear operators acting on a Hilbert space $\mathcal{H}$ is a D^2-dimensional complex vector space. We introduce operator "kets" $|A)=A$ and "bras" $(A|=A^\dagger$, distinguished from vector kets and bras by the use of smooth brackets. The natural operator inner product can be written as $(A|B)=\mathrm{tr}(A^\dagger B)$. An orthonormal basis $|e_j\rangle$ induces an orthonormal operator basis

$$|e_j\rangle\langle e_k|=\tau_{jk}\equiv\tau_\alpha, \tag{A1}$$

where the Greek index is an abbreviation for two Roman indices. Not all orthonormal operator bases are of this outer-product form. In the following, τ_α can be a general orthonormal operator basis, or it can be specialized to an outer-product basis.

The space of superoperators on $\mathcal{H}$, i.e., linear maps on operators, is a D^4-dimensional complex vector space. A superoperator $\mathcal{A}$ is specified by its "matrix elements"

$$\mathcal{A}_{lj,mk}\equiv\langle e_l|\mathcal{A}(|e_j\rangle\langle e_k|)|e_m\rangle, \tag{A2}$$

for the superoperator can be written in terms of its matrix elements as

$$\mathcal{A}=\sum_{lj,mk}\mathcal{A}_{lj,mk}|e_l\rangle\langle e_j|\odot|e_k\rangle\langle e_m|=\sum_{\alpha,\beta}\mathcal{A}_{\alpha\beta}\tau_\alpha\odot\tau_\beta^\dagger$$

$$=\sum_{\alpha,\beta}\mathcal{A}_{\alpha\beta}|\tau_\alpha)(\tau_\beta|. \tag{A3}$$

The *ordinary action* of $\mathcal{A}$ on an operator A, used above to generate the matrix elements, is obtained by dropping an operator A into the center of the representation of $\mathcal{A}$, in place of the $\odot$ sign, i.e.,

$$\mathcal{A}(A)=\sum_{\alpha,\beta}\mathcal{A}_{\alpha\beta}\tau_\alpha A\tau_\beta^\dagger. \tag{A4}$$

There is clearly another way that $\mathcal{A}$ can act on A, the *left-right action*,

$$\mathcal{A}|A)\equiv\sum_{\alpha,\beta}\mathcal{A}_{\alpha\beta}|\tau_\alpha)(\tau_\beta|A), \tag{A5}$$

in terms of which the matrix elements are

$$\mathcal{A}_{\alpha\beta}=(\tau_\alpha|\mathcal{A}|\tau_\beta)$$
$$=(|e_l\rangle\langle e_j||\mathcal{A}||e_m\rangle\langle e_k|)$$
$$=\langle e_l|\mathcal{A}(|e_j\rangle\langle e_k|)|e_m\rangle$$
$$=\mathcal{A}_{lj,mk}. \tag{A6}$$

This expression provides the fundamental connection between the two actions of a superoperator.

With respect to the left-right action, a superoperator works just like an operator. Multiplication of superoperators $\mathcal{B}$ and $\mathcal{A}$ is given by

$$\mathcal{B}\mathcal{A}=\sum_{\alpha,\beta,\gamma}\mathcal{B}_{\alpha\gamma}\mathcal{A}_{\gamma\beta}|\tau_\alpha)(\tau_\beta|, \tag{A7}$$

and the "left-right" adjoint, defined by

$$(A|\mathcal{A}^\dagger|B)=(B|\mathcal{A}|A)^*, \tag{A8}$$

is given by

$$\mathcal{A}^\dagger=\sum_{\alpha,\beta}\mathcal{A}^*_{\alpha\beta}\tau_\beta\odot\tau_\alpha^\dagger=\sum_{\alpha,\beta}\mathcal{A}^*_{\beta\alpha}|\tau_\alpha)(\tau_\beta|. \tag{A9}$$

With respect to the ordinary action, superoperator multiplication, denoted as a composition $\mathcal{B}\circ\mathcal{A}$, is given by

$$\mathcal{B}\circ\mathcal{A}=\sum_{\alpha,\beta,\gamma,\delta}\mathcal{B}_{\gamma\delta}\mathcal{A}_{\alpha\beta}\tau_\gamma\tau_\alpha\odot\tau_\beta^\dagger\tau_\delta^\dagger. \tag{A10}$$

The adjoint with respect to the ordinary action, denoted by $\mathcal{A}^\times$, is defined by

$$\mathrm{tr}([\mathcal{A}^\times(B)]^\dagger A)=\mathrm{tr}(B^\dagger\mathcal{A}(A)). \tag{A11}$$

In terms of a representation in an operator basis, this "cross" adjoint becomes

$$\mathcal{A}^\times=\sum_{\alpha,\beta}\mathcal{A}^*_{\alpha\beta}\tau_\alpha^\dagger\odot\tau_\beta. \tag{A12}$$

Notice that

$$(\mathcal{B}\circ\mathcal{A})^\dagger=\mathcal{B}^\dagger\circ\mathcal{A}^\dagger \quad\text{and}\quad (\mathcal{B}\mathcal{A})^\times=\mathcal{B}^\times\mathcal{A}^\times. \tag{A13}$$

We can formalize the connection between the two kinds of action by defining an operation, called "sharp," which exchanges the two

$$\mathcal{A}^\#|A)\equiv\mathcal{A}(A). \tag{A14}$$

Simple consequences of the definition are that

$$(\mathcal{A}^\#)^\dagger=(\mathcal{A}^\times)^\#, \tag{A15}$$

$$(\mathcal{B}\circ\mathcal{A})^\#=\mathcal{B}^\#\mathcal{A}^\#. \tag{A16}$$

The matrix elements of $\mathcal{A}^\#$ are given by

$$\begin{aligned}\mathcal{A}^{\#}_{lj,mk} &= (|e_l\rangle\langle e_j||\mathcal{A}^{\#}||e_m\rangle\langle e_k|) \\ &= \mathrm{tr}(|e_j\rangle\langle e_l|\mathcal{A}(|e_m\rangle\langle e_k|)) \\ &= \langle e_l|\mathcal{A}(|e_m\rangle\langle e_k|)|e_j\rangle \\ &= \mathcal{A}_{lm,jk}, \end{aligned} \tag{A17}$$

which implies that

$$\mathcal{A}^{\#} = \sum_{lj,mk} \mathcal{A}_{lj,mk}|e_l\rangle\langle e_m| \odot |e_k\rangle\langle e_j|. \tag{A18}$$

A superoperator is left-right Hermitian, i.e., $\mathcal{A}^{\dagger}=\mathcal{A}$, if and only if it has an eigendecomposition

$$\mathcal{A} = \sum_{\alpha} \mu_{\alpha}|\tau_{\alpha})(\tau_{\alpha}| = \sum_{\alpha} \mu_{\alpha}\tau_{\alpha} \odot \tau_{\alpha}^{\dagger}, \tag{A19}$$

where the μ_{α} are real (left-right) eigenvalues and the operators τ_{α} are orthonormal eigenoperators.

A superoperator is *trace preserving* if, under the ordinary action, it leaves the trace unchanged, i.e., if $\mathrm{tr}(A) = \mathrm{tr}[\mathcal{A}(A)] = \mathrm{tr}([\mathcal{A}^{\times}(I)]^{\dagger}A)$ for all operators A. Thus, $\mathcal{A}$ is trace preserving if and only if $\mathcal{A}^{\times}(I)=I$.

A superoperator is said to be *positive* if it maps positive operators to positive operators under the ordinary action. A superoperator is *completely positive* if it and all its extensions $\mathcal{I}\otimes\mathcal{A}$ to tensor-product spaces, where $\mathcal{I}$ is the unit superoperator on the appended space, are positive. It can be shown that $\mathcal{A}$ is completely positive if and only if it is positive relative to the left-right action, i.e., $(A|\mathcal{A}|A) \geqslant 0$ for all operators A (for a proof in the present notation, see Ref. [13]). This is equivalent to saying that $\mathcal{A}$ is left-right Hermitian with non-negative left-right eigenvalues.

In this paper we make use of several special superoperators, whose properties we summarize here. The identity superoperator with respect to the ordinary action is

$$\mathcal{I} = I \odot I = \sum_{j,k} |e_j\rangle\langle e_j| \odot |e_k\rangle\langle e_k|. \tag{A20}$$

This superoperator is Hermitian in both senses, i.e., $\mathcal{I}=\mathcal{I}^{\dagger}=\mathcal{I}^{\times}$. It is the identity superoperator relative to the ordinary action because $\mathcal{I}(A)=A$ for all operators A, but its left-right action gives $\mathcal{I}|A) = \mathrm{tr}(A)I$.

The identity superoperator with respect to the left-right action is

$$\mathbf{I} = \sum_{\alpha} |\tau_{\alpha})(\tau_{\alpha}| = \sum_{j,k} |e_j\rangle\langle e_k| \odot |e_k\rangle\langle e_j|. \tag{A21}$$

This superoperator is also Hermitian in both senses, i.e., $\mathbf{I}=\mathbf{I}^{\dagger}=\mathbf{I}^{\times}$. It is the identity superoperator relative to the left-right action because $\mathbf{I}|A)=A$ for all operators A, but its ordinary action gives $\mathbf{I}(A)=\mathrm{tr}(A)I$. Since sharping exchanges the two kinds of action, it is clear that $\mathcal{I}^{\#}=\mathbf{I}$.

To define the remaining superoperators, it is useful to introduce a set of D^2-1 trace-free Hermitian operators [17], which are the generators of SU(D). We label these operators by a Greek index α, which runs from 1 to D^2-1. The operators are defined by

$$\alpha = 1, \ldots, D-1:$$

$$\lambda_{\alpha} = \Gamma_j \equiv \frac{1}{\sqrt{j(j-1)}} \left(\sum_{k=1}^{j-1} \tau_{kk} - (j-1)\tau_{jj} \right), \quad 2 \leqslant j \leqslant D, \tag{A22}$$

$$\alpha = D, \ldots, (D+2)(D-1)/2:$$

$$\lambda_{\alpha} = \Gamma_{jk}^{(+)} \equiv \frac{1}{\sqrt{2}}(\tau_{jk} + \tau_{kj}), \quad 1 \leqslant j < k \leqslant D, \tag{A23}$$

$$\alpha = D(D+1)/2, \ldots, D^2-1:$$

$$\lambda_{\alpha} = \Gamma_{jk}^{(-)} \equiv \frac{-i}{\sqrt{2}}(\tau_{jk} - \tau_{kj}), \quad 1 \leqslant j < k \leqslant D. \tag{A24}$$

In Eq. (A22), α stands for a single Roman index j, whereas in Eqs. (A23) and (A24), it stands for the pair of Roman indices, jk. These operators are Hermitian generalizations of the two-dimensional Pauli operators: the operators (A22) are diagonal in the chosen basis, like σ_z; for each pair of dimensions, the operators (A23) are like the Pauli operator σ_x; and for each pair of dimensions, the operators (A24) are like σ_y.

Like the Pauli operators, the operators λ_{α} are orthonormal, i.e.,

$$(\lambda_{\alpha}|\lambda_{\beta}) = \mathrm{tr}(\lambda_{\alpha}\lambda_{\beta}) = \delta_{\alpha\beta}. \tag{A25}$$

Thus, they constitute an operator basis for the subspace of trace-free operators. Indeed, we can define a superoperator projector,

$$\mathcal{F} \equiv \sum_{\alpha} |\lambda_{\alpha})(\lambda_{\alpha}| = \sum_{\alpha} \lambda_{\alpha} \odot \lambda_{\alpha}, \tag{A26}$$

which relative to the left-right action, projects onto the subspace of trace-free operators. Notice that $\mathcal{F}=\mathcal{F}^{\dagger}=\mathcal{F}^{\times}$.

If we add to the set of operators λ_{α} the normalized unit operator $I/\sqrt{D}$, we obtain an orthonormal operator basis. Thus, the unit superoperator $\mathbf{I}$ can be written as

$$\mathbf{I} = \frac{|I)(I|}{D} + \sum_{\alpha} |\lambda_{\alpha})(\lambda_{\alpha}| = \mathcal{I}/D + \mathcal{F}. \tag{A27}$$

Writing $\mathcal{F}=\mathbf{I}-\mathcal{I}/D$, we find that

$$\mathcal{F}^{\#} = \mathcal{I} - \frac{\mathbf{I}}{D} = \frac{D^2-1}{D^2}\mathcal{I} - \frac{\mathcal{F}}{D}. \tag{A28}$$

In the chosen basis, the operators (A22) and (A23) are real and symmetric. Together with $I/\sqrt{D}$, they constitute a set of $D(D+1)/2$ orthonormal operators, which span the subspace of operators that are symmetric in the chosen basis. In contrast, the $D(D-1)/2$ operators in Eq. (A24) are pure

imaginary and antisymmetric and span the subspace of operators that are antisymmetric in the chosen basis. We can define superoperator projectors,

$$\mathcal{P}_S \equiv \frac{|I)(I|}{D} + \sum_{\lambda_\alpha \text{ real}} |\lambda_\alpha)(\lambda_\alpha|, \tag{A29}$$

$$\mathcal{P}_A \equiv \sum_{\lambda_\alpha \text{ imaginary}} |\lambda_\alpha)(\lambda_\alpha|, \tag{A30}$$

which relative to the left-right action, project onto the symmetric and antisymmetric operator subspaces. Notice that $\mathcal{P}_S = \mathcal{P}_S^\dagger = \mathcal{P}_S^\times$ and $\mathcal{P}_A = \mathcal{P}_A^\dagger = \mathcal{P}_A^\times$. It is clear that

$$\mathbf{I} = \mathcal{P}_S + \mathcal{P}_A. \tag{A31}$$

The last superoperator we need is the superoperator that transposes operators in the chosen basis. The ordinary action of the transposition superoperator is given by

$$\mathcal{T}(A) = \sum_{j,k} |e_j\rangle\langle e_k|A|e_j\rangle\langle e_k|, \tag{A32}$$

so the superoperator has the form

$$\mathcal{T} = \sum_{j,k} |e_j\rangle\langle e_k| \odot |e_j\rangle\langle e_k|. \tag{A33}$$

The transposition superoperator is Hermitian in both senses and is unchanged by sharping, i.e., $\mathcal{T} = \mathcal{T}^\dagger = \mathcal{T}^\times = \mathcal{T}^\#$. In addition to satisfying $\mathcal{T} \circ \mathcal{T} = \mathcal{I}$, the transposition superoperator has the property that

$$\mathbf{I} \circ \mathcal{T} = \mathbf{I}, \tag{A34}$$

which in view of Eq. (A16), is equivalent to $\mathcal{I}\mathcal{T} = \mathcal{I}$.

It is easy to see that $\mathcal{P}_S - \mathcal{P}_A$, acting to the right, transposes an operator, i.e.,

$$\mathcal{P}_S|A) - \mathcal{P}_A|A) = \mathcal{T}(A) = \mathcal{T}^\#|A), \tag{A35}$$

which gives us, since $\mathcal{T}$ is invariant under sharping,

$$\mathcal{T} = \mathcal{T}^\# = \mathcal{P}_S - \mathcal{P}_A. \tag{A36}$$

Combined with Eq. (A31), this gives us

$$\mathcal{P}_S = \frac{1}{2}(\mathbf{I} + \mathcal{T}), \tag{A37}$$

$$\mathcal{P}_A = \frac{1}{2}(\mathbf{I} - \mathcal{T}). \tag{A38}$$

Combining these forms with Eq. (A34) yields

$$2\mathcal{P}_S \circ \mathcal{T} = \mathbf{I} + \mathcal{I} = (D+1)\mathcal{G}_{\mathrm{AV}}, \tag{A39}$$

$$2\mathcal{P}_A \circ \mathcal{T} = \mathbf{I} - \mathcal{I} = \mathcal{S}_D / \nu_D. \tag{A40}$$

The form (A40) has been given previously [8].

APPENDIX B: SUPEROPERATOR THEOREM

In this appendix, we show that a superoperator is Hermitian relative to the left-right action if and only if it maps all Hermitian operators to Hermitian operators.

Let $\mathcal{A}$ be a superoperator, and let $|e_j\rangle$ be an orthonormal basis, which induces an orthonormal operator basis $|e_j\rangle\langle e_k|$. Notice that

$$\begin{aligned}\langle e_l|\mathcal{A}^\dagger(|e_j\rangle\langle e_k|)|e_m\rangle &= (|e_l\rangle\langle e_j||\mathcal{A}^\dagger||e_m\rangle\langle e_k|) \\ &= (|e_m\rangle\langle e_k||\mathcal{A}||e_l\rangle\langle e_j|)^* \\ &= \langle e_m|\mathcal{A}(|e_k\rangle\langle e_j|)|e_l\rangle^* \\ &= \langle e_l|[\mathcal{A}(|e_k\rangle\langle e_j|)]^\dagger|e_m\rangle. \end{aligned} \tag{B1}$$

Here, the first and third equalities follow from relating the ordinary action of a superoperator to its left-right action [Eq. (A6)], the second equality follows from the definition of the left-right adjoint of $\mathcal{A}$ [Eq. (A8)], and the fourth equality follows from the definition of the operator adjoint. Equation (B1) gives the relation between the operator adjoint and the left-right superoperator adjoint:

$$\mathcal{A}^\dagger(|e_j\rangle\langle e_k|) = [\mathcal{A}(|e_k\rangle\langle e_j|)]^\dagger. \tag{B2}$$

Thus, we have that $\mathcal{A} = \mathcal{A}^\dagger$, i.e., $\mathcal{A}$ is left-right Hermitian, if and only if

$$\mathcal{A}(|e_j\rangle\langle e_k|) = [\mathcal{A}(|e_k\rangle\langle e_j|)]^\dagger \tag{B3}$$

for all j and k. This result allows us to prove the desired theorem easily.

Theorem. A superoperator $\mathcal{A}$ is left-right Hermitian if and only if it maps all Hermitian operators to Hermitian operators.

Proof: First suppose $\mathcal{A}$ is left-right Hermitian, i.e., $\mathcal{A} = \mathcal{A}^\dagger$. This implies that $\mathcal{A}$ has a complete, orthonormal set of eigenoperators τ_α, with real eigenvalues μ_α. Using the eigendecomposition (A19), we have for any Hermitian operator H,

$$\mathcal{A}(H) = \sum_\alpha \mu_\alpha \tau_\alpha H \tau_\alpha^\dagger = \mathcal{A}(H)^\dagger. \tag{B4}$$

Now, suppose $\mathcal{A}$ maps all Hermitian operators to Hermitian operators. Letting $\tau_{jk} = |e_j\rangle\langle e_k|$, it follows that

$$\begin{aligned}\mathcal{A}(\tau_{jk}) &= \mathcal{A}\left(\frac{1}{2}(\tau_{jk}+\tau_{kj})+i\frac{-i}{2}(\tau_{jk}-\tau_{kj})\right)\\ &= \mathcal{A}\left(\frac{1}{2}(\tau_{jk}+\tau_{kj})\right)+i\mathcal{A}\left(\frac{-i}{2}(\tau_{jk}-\tau_{kj})\right)\\ &= \left[\mathcal{A}\left(\frac{1}{2}(\tau_{jk}+\tau_{kj})\right)\right]^{\dagger}+i\left[\mathcal{A}\left(\frac{-i}{2}(\tau_{jk}-\tau_{kj})\right)\right]^{\dagger}\\ &= \left[\mathcal{A}\left(\frac{1}{2}(\tau_{jk}+\tau_{kj})\right)-i\mathcal{A}\left(\frac{-i}{2}(\tau_{jk}-\tau_{kj})\right)\right]^{\dagger}\\ &= \left[\mathcal{A}\left(\frac{1}{2}(\tau_{jk}+\tau_{kj})-i\frac{-i}{2}(\tau_{jk}-\tau_{kj})\right)\right]^{\dagger}=[\mathcal{A}(\tau_{kj})]^{\dagger}.\end{aligned} \tag{B5}$$

Equation (B3) then implies that $\mathcal{A}=\mathcal{A}^{\dagger}$.

Since a superoperator is left-right Hermitian if and only if it has an eigendecomposition as in Eq. (A19), we can conclude, by grouping together positive and negative eigenvalues, that being left-right Hermitian is equivalent to being the difference between two completely positive superoperators. Using the theorem, we have that a superoperator takes all Hermitian operators to Hermitian operators if and only if it is the difference between two completely positive superoperators. This generalizes a result of Yu [18], who showed that a positive superoperator is the difference between two completely positive superoperators. From our perspective, we can say that since a positive superoperator takes positive operators to positive operators, it also takes Hermitian operators to Hermitian operators, and thus, is left-right Hermitian. A positive operator that is not completely positive has one or more negative left-right eigenvalues.

We can get one further result relevant to the considerations in this paper: if $\mathcal{A}$ and $\mathcal{B}$ are left-right Hermitian superoperators for two separate quantum systems, then $\mathcal{A}\otimes\mathcal{B}$ is also left-right Hermitian, and thus, maps all Hermitian operators of the joint system to Hermitian operators.

APPENDIX C: INEQUALITY FOR PURITY

Let

$$\rho_A=\sum_{j=1}^{D_1}\mu_j|e_j\rangle\langle e_j| \quad \text{and} \quad \rho_B=\sum_{k=1}^{D_2}\nu_k|f_k\rangle\langle f_k| \tag{C1}$$

be the eigendecompositions of ρ_A and ρ_B. In the joint basis $|e_j\rangle\otimes|f_k\rangle$, ρ_{AB} has the form

$$\rho_{AB}=\sum_{j,k,l,m}\rho_{jk,lm}|e_j\rangle\langle e_l|\otimes|f_k\rangle\langle f_m|. \tag{C2}$$

The diagonal forms of the marginal density operators show that

$$\sum_{k=1}^{D_2}\rho_{jk,lk}=\mu_j\delta_{jl} \quad \text{and} \quad \sum_{j=1}^{D_1}\rho_{jk,jm}=\nu_k\delta_{km}. \tag{C3}$$

Thus, the diagonal elements of $\rho_{jk,lm}$ are a probability distribution $p_{jk}=\rho_{jk,jk}$, whose marginals are the eigenvalues of the marginal density operators:

$$\sum_{k=1}^{D_2}p_{jk}=\mu_j \quad \text{and} \quad \sum_{j=1}^{D_1}p_{jk}=\nu_k. \tag{C4}$$

We now can write

$$\begin{aligned}1+\mathrm{tr}(\rho_{AB}^2) &= 1+\sum_{j,k,l,m}|\rho_{jk,lm}|^2\\ &\geqslant 1+\sum_{j,k}p_{jk}^2\\ &= \sum_{j,k,l,m}p_{jk}p_{lm}+\sum_{j,k}p_{jk}^2\\ &= \sum_{j,k,m}p_{jk}p_{jm}+\sum_{j\neq l,k,m}p_{jk}p_{lm}\\ &\quad +\sum_{j,k,l}p_{jk}p_{lk}-\sum_{j\neq l,k}p_{jk}p_{lk}\\ &= \sum_{j}\left(\sum_{k}p_{jk}\right)^2+\sum_{k}\left(\sum_{j}p_{jk}\right)^2\\ &\quad +\sum_{j\neq l,k\neq m}p_{jk}p_{lm}\\ &\geqslant \sum_{j}\mu_j^2+\sum_{k}\nu_k^2=\mathrm{tr}(\rho_A^2)+\mathrm{tr}(\rho_B^2).\end{aligned} \tag{C5}$$

The first inequality here is saturated if and only if ρ_{AB} is diagonal in the basis $|e_j\rangle\otimes|f_k\rangle$. The second inequality is saturated if and only if $p_{jk}p_{lm}=0$ whenever $j\neq l$ and $k\neq m$. This requirement is equivalent to saying that the nonzero entries in p_{jk} are restricted to one row or to one column. In view of the first requirement, this means that overall equality is achieved in Eq. (C5) if and only if $\rho_{AB}=\rho_A\otimes\rho_B$ is a product state, with ρ_A or ρ_B a pure state.

APPENDIX D: UNITARILY INVARIANT OPERATOR SUBSPACES

In this appendix, we show that the vector space of operators acting on a D-dimensional Hilbert space has only two proper operator subspaces that are invariant under all unitary transformations. These two subspaces are the one-dimensional subspace spanned by the unit operator I and the subspace consisting of all trace-free operators.

It is obvious that the subspace consisting of multiples of I and the subspace of trace-free operators are unitarily invariant. To show that these are the only unitarily invariant proper subspaces, we consider a unitarily invariant subspace that is not the subspace spanned by I, and we show that this subspace is either the subspace of trace-free operators or the entire operator space. Let A be a nonzero operator in the unitarily invariant subspace, which is not a multiple of I. There exists an orthonormal basis $|e_j\rangle$ such that $A_{11}\neq A_{22}$. Adopt this basis, in which A has the representation

$$A=\sum_{j,k=1}^{D} A_{jk}|e_j\rangle\langle e_k|. \tag{D1}$$

Consider the unitary operator U that changes the sign of $|e_1\rangle$, i.e., $U|e_1\rangle=-|e_1\rangle$ and $U|e_j\rangle=|e_j\rangle$ for $j=2,\ldots,D$. Also in the unitarily invariant subspace is the operator

$$B=\frac{1}{2}(A+UAU^{\dagger})=A_{11}|e_1\rangle\langle e_1|+\sum_{j,k=2}^{D} A_{jk}|e_j\rangle\langle e_k|. \tag{D2}$$

Do the same thing to the second basis vector; i.e., use the unitary operator V defined by $V|e_2\rangle=-|e_2\rangle$, and $V|e_j\rangle=|e_j\rangle$ for $j=1$ and $j=3,\ldots,D$. Also in the subspace is the operator

$$\begin{aligned} C&=\frac{1}{2}(B+VBV^{\dagger})\\ &=A_{11}|e_1\rangle\langle e_1|+A_{22}|e_2\rangle\langle e_2|+\sum_{j,k=3}^{D} A_{jk}|e_j\rangle\langle e_k|. \end{aligned} \tag{D3}$$

Now consider the unitary operator W that swaps $|e_1\rangle$ and $|e_2\rangle$, i.e., $W|e_1\rangle=|e_2\rangle$, $W|e_2\rangle=|e_1\rangle$, and $W|e_j\rangle=|e_j\rangle$ for $j=3,\ldots,D$. Also in the subspace is the (nonzero) trace-free operator

$$D=C-WCW^{\dagger}=(A_{11}-A_{22})(|e_1\rangle\langle e_1|-|e_2\rangle\langle e_2|). \tag{D4}$$

We conclude that the subspace contains the trace-free operator $|e_1\rangle\langle e_1|-|e_2\rangle\langle e_2|$, which is a Pauli σ_z operator for the first two dimensions. From this operator, we can generate by unitary transformations that interchange basis vectors, a σ_z-like operator for every pair of dimensions, and from these σ_z operators, we can generate by unitary transformations a σ_x and a σ_y operator for every pair of dimensions. Since these Pauli-like operators span the space of trace-free operators, we conclude that any unitarily invariant operator subspace that is not the space spanned by I contains all trace-free operators.

The unitarily invariant subspace could be the subspace of trace-free operators. Suppose that it is not and thus contains an operator E that is not trace free. Defining a trace-free operator $F=E-\mathrm{tr}(E)I/D$, we see that I can be written as linear combination of F and E, and thus, is in the subspace. Since the tracefree operators together with I span the entire space of operators, we conclude that in this case the unitarily invariant subspace is the entire operator space. This establishes our result.

[1] *Introduction to Quantum Computation and Information*, edited by H.-K. Lo, S. Popescu, and T. Spiller (World Scientific, Singapore, 1998).

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[3] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[5] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).

[6] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[7] A. Uhlmann, Phys. Rev. A **62**, 032307 (2000).

[8] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[9] V. Bužek, M. Hillery, and R. F. Werner, Phys. Rev. A **60**, R2626 (1999).

[10] V. Bužek, M. Hillery, and R. F. Werner, J. Mod. Opt. **47**, 211 (2000).

[11] S. L. Braunstein, V. Bužek, and M. Hillery, Phys. Rev. A **63**, 052313 (2001).

[12] R. Alicki and K. Lendi, *Quantum Dynamical Semigroups and Applications* (Springer, Berlin, 1987).

[13] C. M. Caves, J. Supercond. **12**, 707 (1999).

[14] P. Rungta, W. J. Munro, K. Nemoto, P. Deuar, G. J. Milburn, and C. M. Caves, in *In Directions in Quantum Optics: A Collection of Papers Dedicated to the Memory of Dan Walls*, edited by H. J. Carmichael, R. J. Glauber, and M. O. Scully (Springer-Verlag, Berlin, 2000), pp. 149–164.

[15] A. Messiah, *Quantum Mechanics*, Vol. II (North-Holland, Amsterdam, 1968), Chap. 15.

[16] R. Derka, V. Bužek, and A. Ekert, Phys. Rev. Lett. **80**, 1571 (1998).

[17] K. Lendi, J. Phys. A **20**, 15 (1987).

[18] S. Yu, e-print quant-ph/0001053.