Sending entanglement through noisy quantum channels

Benjamin Schumacher*
Theoretical Astrophysics, T-6 M.S. B288, Los Alamos National Laboratory, Los Alamos, New Mexico 87545
(Received 26 April 1996)

This paper addresses some general questions of quantum information theory arising from the transmission of quantum entanglement through (possibly noisy) quantum channels. A pure entangled state is prepared of a pair of systems R and Q, after which Q is subjected to a dynamical evolution given by the superoperator $\mathcal{E}^Q$. Two interesting quantities can be defined for this process: the entanglement fidelity F_e and the entropy exchange S_e. It turns out that neither of these quantities depends in any way on the system R, but only on the initial state and dynamical evolution of Q. F_e and S_e are related to various other fidelities and entropies and are connected by an inequality reminiscent of the Fano inequality of classical information theory. Some insight can be gained from these techniques into the security of quantum cryptographic protocols and the nature of quantum error-correcting codes. [S1050-2947(96)03909-1]

PACS number(s): 03.65.Bz, 05.30.−d, 89.70.+c

I. INTRODUCTION

In recent years, considerable progress has been made toward developing a general quantum theory of information [1], analogous to classical information theory founded by Shannon [2]. Distinctively quantum-mechanical notions of coding [3] and channel fidelity [4] have been developed and the role of entangled states in storing and transferring quantum information has been explored [5]. Recently, the study of noisy quantum channels has yielded important results about quantum error-correcting codes [6] and the purification of noisy entangled states [7].

The aim of this paper is to further clarify our understanding of noisy quantum channels by defining and exploiting notions of fidelity and entropy associated with the quantum transmission process. These quantities are based on an analysis of the transmission of entangled states through the noisy channel, although (as we shall see) the use of entanglement is not essential to their definition. A number of applications of these ideas will be outlined.

Here is the general situation that we will consider. Suppose R and Q are two quantum systems and Q is described by a Hilbert space $\mathcal{H}_Q$ of finite dimension d. Initially the joint system RQ is prepared in a pure entangled state $|\Psi^{RQ}\rangle$. The system R is dynamically isolated and has a zero internal Hamiltonian, while the system Q undergoes some evolution that possibly involves interaction with the environment E. The evolution of Q might, for example, represent a coding, transmission, and decoding process via some quantum channel for the quantum information in Q. The final state of RQ is possibly mixed and is described by the density operator $\rho^{RQ'}$.

The *fidelity* of this process is $F_e=\langle\Psi^{RQ}|\rho^{RQ'}|\Psi^{RQ}\rangle$, which is the probability that the final state $\rho^{RQ'}$ would pass a test checking whether it agreed with the initial state $|\Psi^{RQ}\rangle$. (This imagined test would be a measurement of a joint observable on RQ.) F_e measures how successfully the quantum channel preserves the entanglement of Q with the ''reference system'' R.

We will demonstrate three important results. First, the fidelity F_e can be defined entirely in terms of the initial state and evolution of the system Q. Furthermore, $F_e \leq F$, where F is the average fidelity when the channel carries one of an ensemble of pure states of Q described by $\rho^Q = \mathrm{Tr}_R|\Psi^{RQ}\rangle\langle\Psi^{RQ}|$. Thus channels that can convey entanglement faithfully will also convey ensembles of pure states faithfully.

Second, there exists a quantity S_e called *entropy exchange*, also defined in terms of the internal properties of the system Q. This quantity can be viewed as the amount of information that is exchanged with the environment during the interaction of Q and E and it characterizes the amount of ''quantum noise'' in the evolution of Q.

Finally, we will find an inequality (resembling the Fano inequality of classical information theory) that bounds F_e in terms of the dimension d and the entropy exchange S_e in Q. In other words, the faithfulness of Q's dynamical evolution in preserving entanglement is limited by the amount of information that is exchanged with the environment.

The Appendix uses some ideas from the paper to give a derivation of two representation theorems for trace-preserving, completely positive maps, which are the most general descriptions for quantum dynamical evolutions [8].

Throughout this paper, the systems relevant to a particular vector, operator, or superoperator will be indicated by a superscript. Thus $|\psi^Q\rangle$ is a state vector for the system Q, while A^{RQ} is an operator acting on $\mathcal{H}_{RQ}=\mathcal{H}_R\otimes\mathcal{H}_Q$. (If no superscript is given, the quantum system is supposed to be generic.) A prime denotes that a particular state or density operator arises as a result of some dynamical evolution. A tilde is usually present when a particular state vector or operator is not normalized, so that $\langle\psi|\psi\rangle=1$, but $\langle\tilde{\psi}|\tilde{\psi}\rangle\neq 1$ in general.

II. CHANNEL DYNAMICS

A. Completely positive maps

Imagine that the system Q is prepared in an initial state ρ^Q and then subjected to some dynamical process, after

*Permanent address: Department of Physics, Kenyon College, Gambier, OH 43022.

which the state is $\rho^{Q'}$. The dynamical process is described by a map $\mathcal{E}^Q$, so that the evolution is

$$\rho^Q \rightarrow \rho^{Q'} = \mathcal{E}^Q(\rho^Q). \tag{1}$$

In the most general case, the map $\mathcal{E}^Q$ must be a trace-preserving, completely positive linear map [8]. In other words, we have the following.

(i) $\mathcal{E}^Q$ must be linear in the density operators. That is, if $\rho^Q = p_1\rho_1^Q + p_2\rho_2^Q$, then

$$\begin{aligned}\mathcal{E}^Q(\rho^{Q'}) &= p_1\rho_1^{Q'} + p_2\rho_2^{Q'} \\ &= p_1(\mathcal{E}^Q(\rho_1^Q)) + p_2(\mathcal{E}^Q(\rho_2^Q)).\end{aligned}$$

A probabilistic mixture of inputs to $\mathcal{E}^Q$ leads to a probabilistic mixture of outputs. This means that $\mathcal{E}^Q$ must be a *superoperator*, that is, a linear operator acting on the space of linear operators (e.g., density operators) on $\mathcal{H}_Q$.

(ii) $\mathcal{E}^Q$ must be trace-preserving, so that $\mathrm{Tr}\rho^{Q'} = \mathrm{Tr}\rho^Q = 1$.

(iii) $\mathcal{E}^Q$ must be positive. This means that if ρ^Q is positive[1] then $\rho^{Q'} = \mathcal{E}^Q(\rho^Q)$ must be positive.

These three conditions mean that the superoperator $\mathcal{E}^Q$ takes normalized density operators to normalized density operators in a reasonable way. The requirement of *complete* positivity is somewhat more subtle.

(iv) $\mathcal{E}^Q$ must be completely positive. That is, suppose we extend the evolution superoperator $\mathcal{E}^Q$ in a trivial way to an evolution superoperator for a compound system RQ, yielding $\mathcal{I}^R \otimes \mathcal{E}^Q$, where $\mathcal{I}^R$ is the identity superoperator on R states. Physically, this means adjoining a system R that has trivial dynamics (no state of R is changed) and which does not interact with Q. $\mathcal{E}^Q$ is completely positive if, for all such trivial extensions, the resulting superoperator $\mathcal{I}^R \otimes \mathcal{E}^Q$ is positive.

A completely positive map is not only a reasonable map from density operators to density operators for Q, but it is *extensible* in a trivial way to a reasonable map from density operators to density operators on any larger system RQ. Since we cannot exclude *a priori* that our system Q is in fact initially entangled with some distant isolated system R, any acceptable $\mathcal{E}^Q$ had better satisfy this condition.

B. Representations of $\mathcal{E}^Q$

Completely positive, trace-preserving linear maps obviously include all unitary evolutions of the state $\rho^{Q'} = U^Q\rho^Q U^{Q\dagger}$. They also include unitary evolutions involving interactions with an external system. Suppose we consider an environment system E that is initially in the pure state $|0^E\rangle$. Then we could have

$$\mathcal{E}^Q(\rho^Q) = \mathrm{Tr}_E U^{QE}(\rho^Q \otimes |0^E\rangle\langle 0^E|)U^{QE\dagger}, \tag{2}$$

where U^{QE} is some arbitrary unitary evolution on the joint system QE. This map is also trace preserving and completely positive.

If we can write a superoperator $\mathcal{E}^Q$ as a unitary evolution on an extended system QE followed by a partial trace over E, we say that we have a ''unitary representation'' of the superoperator. Such a representation is not unique since many different unitary operators U^{QE} will lead to the same $\mathcal{E}^Q$.

Another useful sort of representation for completely positive maps employs only operators on $\mathcal{H}_Q$. Let A_μ^Q be a collection of such operators indexed by μ. Then the map $\mathcal{E}^Q$ given by

$$\mathcal{E}^Q(\rho^Q) = \sum_\mu A_\mu^Q \rho^Q A_\mu^{Q\dagger} \tag{3}$$

is a completely positive map. If, in addition, the A_μ operators satisfy

$$\sum_\mu A_\mu^{Q\dagger} A_\mu^Q = 1^Q, \tag{4}$$

then the map is also trace preserving. Such a representation for $\mathcal{E}^Q$ in terms of operators A_μ^Q will be called an ''operator-sum representation'' for $\mathcal{E}^Q$. A single $\mathcal{E}^Q$ will admit many different operator-sum representations.

Some insight into the connection between these representations for $\mathcal{E}^Q$ can be gained by explicitly writing down the partial trace Tr_E from Eq. (2). Suppose that $\rho^Q = |\phi^Q\rangle\langle\phi^Q|$ and let $|\mu^E\rangle$ be a complete orthonormal set of states of E. Then

$$\mathcal{E}^Q(\rho^Q) = \sum_\mu \langle\mu^E|U^{QE}(|\phi^Q\rangle\langle\phi^Q| \otimes |0^E\rangle\langle 0^E|)U^{QE\dagger}|\mu^E\rangle. \tag{5}$$

If we define the operator A_μ^Q by

$$A_\mu^Q|\phi^Q\rangle = \langle\mu^E|U^{QE}(|\phi^Q\rangle \otimes |0^E\rangle), \tag{6}$$

then we recover an expression identical to Eq. (3). Since every input state ρ^Q is a convex combination of pure states, we recover Eq. (3) for arbitrary ρ^Q by linearity.

A pair of important representation theorems [9] state the following.

(i) Every trace-preserving, completely positive linear map $\mathcal{E}^Q$ has a unitary representation, as in Eq. (2).

(ii) Every trace-preserving, completely positive linear map $\mathcal{E}^Q$ has an operator-sum representation, as in Eq. (3).

(By our argument above, the second statement follows from the first.) These statements, particularly the first, motivate us to assert that the trace-preserving, completely positive linear maps is exactly the class of allowed evolutions of a quantum system. Any reasonable evolution should be such a map and every such map could be accomplished by unitary dynamics (i.e., Hamiltonian evolution) on a larger system. A relatively simple proof of both of these representation theorems is found in the Appendix.

[1]We will use the term ''positive'' to refer generically to operators that are *positive semidefinite*, i.e., those that are Hermitian and have no negative eigenvalues.

From now on we will assume that a particular $\mathcal{E}^Q$ has been specified, giving the evolution of states of the system Q. We will use unitary representations and operator-sum representations as convenient.

III. MIXED STATES AND PURIFICATIONS

A. Entangled states

Given a pure state $|\Psi^{RQ}\rangle$ of a joint system RQ, we can form the reduced state ρ^Q for one of the subsystems Q by means of a partial trace operation

$$\rho^Q = \mathrm{Tr}_R |\Psi^{RQ}\rangle\langle\Psi^{RQ}| = \sum_k \langle k^R|\Psi^{RQ}\rangle\langle\Psi^{RQ}|k^R\rangle, \tag{7}$$

where $|k^R\rangle$ is an orthonormal basis for $\mathcal{H}_R$. We can define the reduced state ρ^Q given a mixed joint state ρ^{RQ} in the same fashion.

We have made use of a *partial inner product* between states of R and states of a larger system RQ. This is easy to understand. The vector

$$|\xi^Q\rangle = \langle\phi^R|\Psi^{RQ}\rangle \tag{8}$$

is defined to be the unique vector in $\mathcal{H}_Q$ such that

$$\langle\alpha^Q|\xi^Q\rangle = \langle\phi^R\alpha^Q|\Psi^{RQ}\rangle \tag{9}$$

for all vectors $|\alpha^Q\rangle$ in $\mathcal{H}_Q$ (where $|\phi^R\alpha^Q\rangle = |\phi^R\rangle\otimes|\alpha^Q\rangle$). We could also write this as

$$\langle\phi^R|\Psi^{RQ}\rangle = \sum_k \langle\phi^R\xi_k^Q|\Psi^{RQ}\rangle|\xi_k^Q\rangle \tag{10}$$

for some orthonormal basis set $|\xi_k^Q\rangle$ for $\mathcal{H}_Q$.

There are, of course, many different pure entangled states $|\Psi^{RQ}\rangle$ that give rise to a given reduced state ρ^Q. These are generically called *purifications* of ρ^Q. Suppose $|\Psi_1^{RQ}\rangle$ and $|\Psi_2^{RQ}\rangle$ are two such purifications. Then we can write each of them using the Schmidt decomposition

$$|\Psi_1^{RQ}\rangle = \sum_k \sqrt{\lambda_k}|\xi_{1k}^R\rangle\otimes|\lambda_k^Q\rangle, \tag{11}$$

$$|\Psi_2^{RQ}\rangle = \sum_k \sqrt{\lambda_k}|\xi_{2k}^R\rangle\otimes|\lambda_k^Q\rangle, \tag{12}$$

where the λ_k and $|\lambda_k^Q\rangle$ are eigenvalues and eigenstates of ρ^Q and the $|\xi_{1k}^R\rangle$ and $|\xi_{2k}^R\rangle$ are two orthonormal sets of states in $\mathcal{H}_R$. Since the two purifications differ only in the choice of orthonormal set in $\mathcal{H}_R$, they are connected by a unitary operator of the form $U^R\otimes 1^Q$. Any purification of ρ^Q can be converted to any other by a unitary rotation acting on the auxilliary ''reference'' system R.

The Schmidt decomposition also makes clear the fact that, given a pure entangled state

$$|\Psi^{RQ}\rangle = \sum_k \sqrt{\lambda_k}|\xi^R\rangle\otimes|\lambda_k^Q\rangle, \tag{13}$$

the reduced states $\rho^Q = \mathrm{Tr}_R|\Psi^{RQ}\rangle\langle\Psi^{RQ}|$ and $\rho^R = \mathrm{Tr}_Q|\Psi^{RQ}\rangle\langle\Psi^{RQ}|$ will have exactly the same set of nonzero eigenvalues, namely, the λ_k.

B. Mixed-state fidelity

The notion of purification is used to define the *fidelity* between two density operators ρ_1 and ρ_2. This is

$$F(\rho_1,\rho_2) = \max|\langle 1|2\rangle|^2, \tag{14}$$

where the maximum is taken over all purifications $|1\rangle$ and $|2\rangle$ of ρ_1 and ρ_2 [4]. The fidelity has several important properties: $0\leq F(\rho_1,\rho_2)\leq 1$, with $F(\rho_1,\rho_2)=1$ if and only if $\rho_1=\rho_2$; $F(\rho_1,\rho_2)=F(\rho_2,\rho_1)$; and if $\rho_1=|\psi_1\rangle\langle\psi_1|$ is a pure state, then

$$F(\rho_1,\rho_2) = \mathrm{Tr}\rho_1\rho_2 = \langle\psi_1|\rho_2|\psi_1\rangle. \tag{15}$$

This is just the probability that the state ρ_2 would pass a measurement testing whether or not it is the state $|\psi_1\rangle$. The fidelity is a general way of defining the ''closeness'' of a pair of states.

If we have two states ρ_1^{RQ} and ρ_2^{RQ}, we can form

$$\rho_1^Q = \mathrm{Tr}_R\rho_1^{RQ}, \tag{16}$$

$$\rho_2^Q = \mathrm{Tr}_R\rho_2^{RQ}. \tag{17}$$

Then $F(\rho_1^{RQ},\rho_2^{RQ})\leq F(\rho_1^Q,\rho_2^Q)$. This can be seen directly from the definition by noting that every purification of ρ_1^{RQ} is also a purification of ρ_1^Q, and so on.

C. Ensembles of pure states

A mixed state ρ^Q may arise from a statistical ensemble $\mathcal{S}$ of pure states $|\psi_i^Q\rangle$ of Q. In this case we can write

$$\rho^Q = \sum_i p_i|\psi_i^Q\rangle\langle\psi_i^Q|, \tag{18}$$

where p_i is the probability of the state $|\psi_i^Q\rangle$ in the ensemble $\mathcal{S}$.

If $\rho^Q = \mathrm{Tr}_R|\Psi^{RQ}\rangle\langle\Psi^{RQ}|$ for a pure entangled state $|\Psi^{RQ}\rangle$ of RQ, we can ''realize'' an ensemble of pure states for ρ^Q by performing a complete measurement on the system R. (This and other characterizations of the ensembles described by ρ^Q are given in [10].) Let $|\epsilon_i^R\rangle$ be the basis for this complete measurement. Each outcome of the R measurement will be associated with a relative state [11] of the system Q. If p_i is the probability of the ith outcome of the R measurement and $|\psi_i^Q\rangle$ is the relative state of Q associated with this outcome, then

$$\sqrt{p_i}|\psi_i^Q\rangle = \langle\epsilon_i^R|\Psi^{RQ}\rangle. \tag{19}$$

(Note that, in dealing with ensembles of pure states, it is sometimes useful to consider the non-normalized vectors $|\tilde{\psi}_i^Q\rangle = \sqrt{p_i}|\psi_i^Q\rangle$. In other words, we can normalize the component states in $\mathcal{S}$ by their probabilities. The resulting vectors are in themselves a complete description of the ensemble $\mathcal{S}$. See [10] for fuller details.) It follows that

$$\sum_i p_i|\psi_i^Q\rangle\langle\psi_i^Q| = \sum_i \langle\epsilon_i^R|\Psi^{RQ}\rangle\langle\Psi^{RQ}|\epsilon_i^R\rangle = \mathrm{Tr}_R|\Psi^{RQ}\rangle\langle\Psi^{RQ}| = \rho^Q, \tag{20}$$

so that the ensemble $\mathcal{S}$ of relative states is a pure state ensemble for ρ^Q. In fact, any pure state ensemble for ρ^Q can be realized in just this way. That is, we can fix a particular purification $|\Psi^{RQ}\rangle$ for ρ^Q and give a prescription for realizing any pure state ensemble for ρ^Q as a relative state ensemble for some complete measurement on R.

Let $\mathcal{S}_1$ be a pure state ensemble for ρ^Q given by probabilities p_i and states $|\psi_i^Q\rangle$ and suppose that $\mathcal{H}_R$ has arbitrarily high dimension, at least as large as the number of distinct pure states in the ensembles we consider. Then we can construct a purification $|\Psi_1^{RQ}\rangle$ by

$$|\Psi_1^{RQ}\rangle = \sum_i \sqrt{p_i}|\alpha_i^R\rangle\otimes|\psi_i^Q\rangle, \tag{21}$$

where the $|\alpha_i^R\rangle$ are a basis for $\mathcal{H}_R$. (Only some of these basis vectors may appear in this superposition.) Clearly, $\rho^Q = \mathrm{Tr}_R|\Psi_1^{RQ}\rangle\langle\Psi_1^{RQ}|$. Similarly, if we have another ensemble $\mathcal{S}_2$ for ρ^Q given by probabilities q_i and states $|\phi_i^Q\rangle$, we can construct a purification

$$|\Psi_2^{RQ}\rangle = \sum_i \sqrt{q_i}|\beta_i^R\rangle\otimes|\phi_i^Q\rangle \tag{22}$$

for some other R basis $|\beta_i^R\rangle$. Since both of these are purifications of the same ρ^Q, there is a unitary operator U^R such that $|\Psi_2^{RQ}\rangle = (U^R\otimes 1^Q)|\Psi_1^{RQ}\rangle$.

We can clearly realize the ensemble $\mathcal{S}_2$ by making a measurement of the $|\beta_i^R\rangle$ basis on the state $|\Psi_2^{RQ}\rangle$ of R; but this is equivalent to making a measurement of the basis $|\gamma_i^R\rangle = U^{R\dagger}|\beta_i^R\rangle$ on the state $|\Psi_1^{RQ}\rangle$:

$$\begin{aligned}\langle\gamma_i^R|\Psi_1^{RQ}\rangle &= (\langle\beta_i^R|U^R)|\Psi_1^{RQ}\rangle \\ &= \langle\beta_i^R|[(U^R\otimes 1^Q)|\Psi_1^{RQ}\rangle] \\ &= \langle\beta_i^R|\Psi_2^{RQ}\rangle \\ &= \sqrt{q_i}|\phi_i^Q\rangle.\end{aligned} \tag{23}$$

Thus the ensemble $\mathcal{S}_2$ can be realized by making an R measurement on the purification $|\Psi_1^{RQ}\rangle$. It follows that we could pick a particular purification $|\Psi^{RQ}\rangle$ and obtain *any* pure state ensemble for ρ^Q by a suitable choice of measurement basis for the system R.

We have assumed that $\dim\mathcal{H}_R$ is arbitrarily large so that we can have an arbitrarily large number of basis vectors (since the pure state ensembles may have an arbitrarily large number of components). But this is not really necessary. If we allow positive operator measurements (POMs) [12] on R, then the dimension of $\mathcal{H}_R$ need be no greater than the dimension of $\mathcal{H}_Q$, which is the minimum size necessary to purify all mixed states ρ^Q. The only relevant part of the basis $|\alpha_i^R\rangle$ is the set of subnormalized vectors $|\tilde{\alpha}_i^R\rangle = \Pi|\alpha_i^R\rangle$, where Π is the projection onto the subspace of $\mathcal{H}_R$ that supports $\rho^R = \mathrm{Tr}_Q|\Psi^{RQ}\rangle\langle\Psi^{RQ}|$. Since $\dim\mathcal{H}_Q = d$, this subspace need have only up to d dimensions. The $|\tilde{\alpha}_i^R\rangle\langle\tilde{\alpha}_i^R|$ are elements of a POM on this subspace. We can use this POM on the d-dimensional subspace of $\mathcal{H}_R$ to find a POM for a purification that uses another reference system R_*, with $\dim\mathcal{H}_{R_*} = d$.

D. Entropy

Since entropy will be of central importance for our results, we will review some of the relevant properties of classical and quantum entropy. Suppose the non-negative numbers $p_1, p_2, \ldots$ sum to unity and thus form a probability distribution. The Shannon entropy $H(\vec{p})$ of this probability distribution (represented by the vector $\vec{p}$) is just

$$H(\vec{p}) = -\sum_k p_k \log p_k. \tag{24}$$

We specify the base of our logarithms to be 2 and take $0\log 0 = 0$. If $\vec{p}$ forms the probability for some random variable X, so that $p(x_k) = p_k$ for various values x_k of X, then we will often write this entropy as $H(X)$.

The Shannon entropy $H(X)$ is the fundamental quantity in classical information theory and it represents the average number of binary digits (or *bits*) required to represent the value of X [2]. It can be thought of as a measure of the uncertainty in the value of X expressed by the probability distribution. We can use it to define various information-theoretic quantities, such as the conditional entropy

$$H(X|Y) = \sum_k p(y_k)H(X|y_k) = -\sum_{j,k} p(x_j, y_k)\log p(x_j|y_k) \tag{25}$$

for a joint distribution $p(x_j, y_k)$ over values of two variables X and Y. A very important quantity is the *mutual information* $I(X:Y)$ between two random variables X and Y:

$$I(X:Y) = H(X) - H(X|Y), \tag{26}$$

which is the average amount that the uncertainty about X decreases when the value of Y is known. If X represents the input of a communications channel and Y represents the output, then $I(X:Y)$ represents the amount of information conveyed by the channel. It turns out that $I(X:Y) = I(Y:X)$.

The quantum-mechanical definition of entropy was first given by von Neumann [13]. Suppose ρ^Q is a density operator representing a mixed state of Q. Then the entropy is

$$S(\rho^Q) = -\mathrm{Tr}\rho^Q\log\rho^Q. \tag{27}$$

If $\lambda_1, \lambda_2, \ldots$ are the eigenvalues of ρ^Q, then $S(\rho^Q) = H(\vec{\lambda})$. The von Neumann entropy also has a signficance for coding similar to the Shannon entropy: it is the average number of two-level quantum systems (or *qubits*) needed to faithfully represent one of the pure states of an ensemble described by ρ^Q [3].

Suppose that systems R and Q are in a pure entangled state $|\Psi^{RQ}\rangle$. Then $S(\rho^{RQ}) = 0$. However, unlike the classical Shannon entropy, it is possible for the von Neumann entropy of the subsystems R and Q to be nonzero even when the

entropy of the joint system RQ is zero. We saw above that the density operators ρ^Q and ρ^R have the same nonzero eigenvalues. Thus $S(\rho^R)=S(\rho^Q)$. That is, if a pair of quantum systems are in a pure entangled state, the reduced mixed states will have the same von Neumann entropy.

The von Neumann entropy has a number of important properties (usefully reviewed in [14]). Suppose A and B are quantum systems with joint state ρ^{AB} and reduced states ρ^A and ρ^B. Then

$$S(\rho^{AB}) \leqslant S(\rho^A)+S(\rho^B), \tag{28}$$

$$S(\rho^{AB}) \geqslant S(\rho^A)-S(\rho^B). \tag{29}$$

Equation (28) is the *subadditivity* property of the von Neumann entropy and Eq. (29) is sometimes called the ''triangle inequality'' for the entropy functional.

Another useful property of the von Neumann entropy relates it to the Shannon entropy of the probability distribution for the measurement outcomes of a complete observable. Let ρ be a mixed state with eigenvalues λ_k, so that

$$\rho=\sum_k \lambda_k|\lambda_k\rangle\langle\lambda_k|. \tag{30}$$

Now imagine that a measurement is performed of some complete ordinary observable, that is, the state is resolved using an orthonormal basis $|a_j\rangle$. The probability p_j that the jth outcome is obtained is thus

$$p_j=\langle a_j|\rho|a_j\rangle=\sum_k \lambda_k\langle a_j|\lambda_k\rangle\langle\lambda_k|a_j\rangle$$

$$=\sum_k M_{jk}\lambda_k. \tag{31}$$

The matrix $V_{jk}=\langle a_j|\lambda_k\rangle$ is unitary, so the matrix $M_{jk}=|V_{jk}|^2$ is doubly stochastic. That is, the rows and columns of V_{jk} are orthonormal vectors, so that the rows and columns of M_{jk} all sum to one:

$$\sum_i M_{ij}=1 \text{ for all j}, \quad \sum_j M_{ij}=1 \text{ for all i}.$$

It is a standard theorem of information theory that the Shannon entropy $H(\vec{q})=-\Sigma_i q_i \log q_i$ cannot decrease if the probabilities q_i are changed via a doubly stochastic matrix [15]. Therefore,

$$H(\vec{p}) \geqslant H(\vec{\lambda})=S(\rho). \tag{32}$$

The von Neumann entropy is thus a lower bound on the Shannon entropy for the outcome of a complete measurement on the system.

IV. ENTANGLEMENT FIDELITY

A. Definition

Suppose that an entangled state $|\Psi^{RQ}\rangle$ is prepared for the joint system RQ and that Q is subjected to a dynamical evolution described by $\mathcal{E}^Q$ (so that the overall evolution is given by $\mathcal{I}^R\otimes\mathcal{E}^Q$). The final state is

$$\rho^{RQ'}=\mathcal{I}^R\otimes\mathcal{E}^Q(|\Psi^{RQ}\rangle\langle\Psi^{RQ}|). \tag{33}$$

The fidelity of this process is

$$F_e=\mathrm{Tr}|\Psi^{RQ}\rangle\langle\Psi^{RQ}|\rho^{RQ'}=\langle\Psi^{RQ}|\rho^{RQ'}|\Psi^{RQ}\rangle. \tag{34}$$

We call F_e the *entanglement fidelity* of the process.

Written in these terms, F_e depends on the initial and final states of the system RQ. We will next show that F_e depends only on the map $\mathcal{E}^Q$ and the initial reduced state ρ^Q obtained by a partial trace

$$\rho^Q=\mathrm{Tr}_R|\Psi^{RQ}\rangle\langle\Psi^{RQ}|. \tag{35}$$

That is, the entanglement fidelity F_e, which is associated with an entangled state including Q, is (rather surprisingly) a property *intrinsic* to the system Q itself.

The superoperator $\mathcal{I}^R\otimes\mathcal{E}^Q$ can be expressed

$$\mathcal{I}^R\otimes\mathcal{E}^Q(\rho^{RQ})=\sum_\mu (1^R\otimes A_\mu^Q)\rho^{RQ}(1^R\otimes A_\mu^Q)^\dagger. \tag{36}$$

Suppose that the initial states $|\Psi_1^{RQ}\rangle$ and $|\Psi_2^{RQ}\rangle$, both purifications of ρ^Q, lead to final states $\rho_1^{RQ'}$ and $\rho_2^{RQ'}$, respectively, under the action of the superoperator $\mathcal{I}^R\otimes\mathcal{E}^Q$ and let U^R be the unitary operator for R such that

$$|\Psi_2^{RQ}\rangle=(U^R\otimes 1^Q)|\Psi_1^{RQ}\rangle. \tag{37}$$

Clearly, $U^R\otimes 1^Q$ commutes with $1^R\otimes A_\mu^Q$ for all μ. Therefore,

$$\begin{aligned}\rho_2^{RQ'}&=\sum_\mu (1^R\otimes A_\mu^Q)|\Psi_2^{RQ}\rangle\langle\Psi_2^{RQ}|(1^R\otimes A_\mu^Q)^\dagger\\ &=\sum_\mu (1^R\otimes A_\mu^Q)(U^R\otimes 1^Q)|\Psi_1^{RQ}\rangle\\ &\quad\times\langle\Psi_1^{RQ}|(U^R\otimes 1^Q)^\dagger(1^R\otimes A_\mu^Q)\\ &=(U^R\otimes 1^Q)\left(\sum_\mu (1^R\otimes A_\mu^Q)|\Psi_1^{RQ}\rangle\langle\Psi_1^{RQ}|(1^R\otimes A_\mu^Q)^\dagger\right)\\ &\quad\times(U^R\otimes 1^Q)^\dagger\rho_2^{RQ'}\\ &=(U^R\otimes 1^Q)\rho_1^{RQ'}(U^R\otimes 1^Q)^\dagger.\end{aligned} \tag{38}$$

[Note that Eq. (38) implies that $\rho_1^{RQ'}$ and $\rho_2^{RQ'}$ must have the same eigenvalues. This will be important later in the definition of entropy exchange.] From Eq. (38) it follows that

$$\begin{aligned}F_{e2}&=\langle\Psi_2^{RQ}|\rho_2^{RQ'}|\Psi_2^{RQ}\rangle\\ &=\langle\Psi_1^{RQ}|(U^R\otimes 1^Q)^\dagger(U^R\otimes 1^Q)\rho_1^{RQ'}(U^R\otimes 1^Q)^\dagger\\ &\quad\times(U^R\otimes 1^Q)|\Psi_1^{RQ}\rangle\\ &=\langle\Psi_1^{RQ}|\rho_1^{RQ'}|\Psi_1^{RQ}\rangle\\ &=F_{e1}.\end{aligned} \tag{39}$$

Hence the fidelity F_e does not depend on *which* purification for ρ^Q is chosen. It only depends on ρ^Q and the superoperator $\mathcal{E}^Q$.

B. Intrinsic expression for F_e

It is instructive to derive an expression for F_e in terms of things that are intrinsic to the system Q, i.e., an expression that does not refer to R. Suppose we have an operator-sum representation for $\mathcal{E}^Q$, as in Eq. (3). Consider a particular pure entangled state for RQ

$$|\Psi^{RQ}\rangle = \sum_k \sqrt{p_k}|k^R\rangle \otimes |\phi_k^Q\rangle, \tag{40}$$

where the $|k^R\rangle$ are orthonormal states in $\mathcal{H}_R$. (We do not need to require the $|\phi_k^Q\rangle$ to be orthonormal.) This state evolves under $\mathcal{I}^R \otimes \mathcal{E}^Q$ into $\rho^{RQ'}$. The initial state of Q is

$$\rho^Q = \mathrm{Tr}_R |\Psi^{RQ}\rangle\langle\Psi^{RQ}| = \sum_k p_k |\phi_k^Q\rangle\langle\phi_k^Q|. \tag{41}$$

Now, for any operator X^Q acting on $\mathcal{H}_Q$,

$$\begin{aligned}\langle\Psi^{RQ}|(1^R \otimes X^Q)|\Psi^{RQ}\rangle &= \sum_{jk} \sqrt{p_j p_k}\langle j^R|1^R|k^R\rangle\langle\phi_j^Q|X^Q|\phi_k^Q\rangle \\ &= \sum_{jk} \sqrt{p_j p_k}\delta_{jk}\langle\phi_j^Q|X^Q|\phi_k^Q\rangle \\ &= \sum_k p_k\langle\phi_k^Q|X^Q|\phi_k^Q\rangle = \mathrm{Tr}\rho^Q X^Q.\end{aligned} \tag{42}$$

We can now work out the fidelity very easily:

$$\begin{aligned}F_e &= \langle\Psi^{RQ}|\rho^{RQ'}|\Psi^{RQ}\rangle \\ &= \sum_\mu \langle\Psi^{RQ}|(1^R \otimes A_\mu^Q)|\Psi^{RQ}\rangle\langle\Psi^{RQ}|(1^R \otimes A_\mu^Q)^\dagger|\Psi^{RQ}\rangle,\end{aligned}$$

$$F_e = \sum_\mu (\mathrm{Tr}\rho^Q A_\mu^Q)(\mathrm{Tr}\rho^Q A_\mu^{Q\dagger}). \tag{43}$$

Although this is written with respect to a particular operator-sum representation of $\mathcal{E}^Q$ (which is not unique), the value of F_e will clearly be independent of this representation. Equation (43) expresses F_e entirely in terms of the initial state ρ^Q of the system Q and the evolution superoperator $\mathcal{E}^Q$.

C. Relations to other fidelities

It is worth noting what F_e is not. It is not the simple fidelity of the input and output states of Q. This fidelity can be written $F(\rho^Q, \rho^{Q'})$, where $\rho^{Q'} = \mathcal{E}^Q(\rho^Q)$. We can show that $F_e \neq F(\rho^Q, \rho^{Q'})$ in general by considering an operation defined by

$$A_\mu^Q = |\mu^Q\rangle\langle\mu^Q| \tag{44}$$

for some orthonormal basis $|\mu^Q\rangle$. The effect of the operation is to completely destroy any coherences between different elements of the basis. That is, the superposition $\Sigma_\mu c_\mu |\mu^Q\rangle$ would be transformed into the mixed state

$$\rho^{Q'} = \sum_\mu |c_\mu|^2 |\mu^Q\rangle\langle\mu^Q|. \tag{45}$$

Now suppose $\rho^Q = \Sigma_\mu \lambda_\mu |\mu^Q\rangle\langle\mu^Q|$. Then $\rho^{Q'} = \rho^Q$ and thus $F(\rho^Q, \rho^{Q'}) = 1$. However, let $|\Psi^{RQ}\rangle$ be a purification of ρ^Q, for example,

$$|\Psi^{RQ}\rangle = \sum_\mu \sqrt{\lambda_\mu}|\phi_\mu^R\rangle \otimes |\mu^Q\rangle. \tag{46}$$

The action of the superoperator $\mathcal{I}^R \otimes \mathcal{E}^Q$ on this state yields

$$\rho^{RQ'} = \sum_\mu \lambda_\mu |\phi_\mu^R\rangle\langle\phi_\mu^R| \otimes |\mu^Q\rangle\langle\mu^Q|. \tag{47}$$

If more than one of the λ_μ's is nonzero, then $F_e = F(\rho^{RQ}, \rho^{RQ'}) \neq 1$. Thus $F_e \neq F(\rho^Q, \rho^{Q'})$.

However, there is a general relation between F_e and $F(\rho^Q, \rho^{Q'})$,

$$F_e = F(\rho^{RQ}, \rho^{RQ'}) \leq F(\rho^Q, \rho^{Q'}). \tag{48}$$

The entanglement fidelity F_e is thus a lower bound to the input-output fidelity $F(\rho^Q, \rho^{Q'})$ for states of Q.

F_e and $F(\rho^Q, \rho^{Q'})$ do sometimes agree. Suppose that the initial state ρ^Q is in fact a pure state of Q, so that there is no entanglement between R and Q. Then, letting $\rho^Q = |\psi^Q\rangle\langle\psi^Q|$,

$$\begin{aligned}F(\rho^Q, \rho^{Q'}) &= \langle\psi^Q|\rho^{Q'}|\psi^Q\rangle \\ &= \sum_\mu \langle\psi^Q|A_\mu^Q|\psi^Q\rangle\langle\psi^Q|A_\mu^{Q\dagger}|\psi^Q\rangle \\ &= \sum_\mu (\mathrm{Tr}\rho^Q A_\mu^Q)(\mathrm{Tr}\rho^Q A_\mu^{Q\dagger}) \\ &= F_e.\end{aligned} \tag{49}$$

The entanglement fidelity equals the ''input-output'' fidelity when the input state is a pure state.

Now suppose that ρ^Q is a mixed state of Q arising from an ensemble $\mathcal{S}$ in which the pure state $|\psi_i^Q\rangle$ occurs with probability p_i. The average input-output fidelity for this ensemble is

$$\begin{aligned}\overline{F} &= \sum_i p_i F(|\psi_i^Q\rangle\langle\psi_i^Q|, \rho_i^{Q'}) \\ &= \sum_i p_i \langle\psi_i^Q|\rho_i^{Q'}|\psi_i^Q\rangle,\end{aligned} \tag{50}$$

where $\rho_i^{Q'} = \mathcal{E}^Q(|\psi_i^Q\rangle\langle\psi_i^Q|)$.

It turns out that $F \geq F_e$. Some such connection is reasonable physically, since we can realize a pure state ensemble

$\mathcal{S}$ by means of an R measurement on a purification of ρ^Q, and this measurement may be performed either before or after the dynamical evolution given by $\mathcal{S}^Q$. A full proof follows.

Let $|\alpha_i^R\rangle$ be an orthonormal set in $\mathcal{H}_R$ (assumed to have as many dimensions as there are elements in the ensemble $\mathcal{S}$) and let

$$|\Psi^{RQ}\rangle = \sum_i \sqrt{p_i}\,|\alpha_i^R\rangle \otimes |\psi_i^Q\rangle. \tag{51}$$

$|\Psi^{RQ}\rangle$ is clearly a purification of ρ^Q and the $|\alpha_i^R\rangle$ basis is the basis in $\mathcal{H}_R$ that, when measured, generates the ensemble $\mathcal{S}$ as an ensemble of relative states in Q. That is, $\sqrt{p_i}\,|\psi_i^Q\rangle = \langle \alpha_i^R|\Psi^{RQ}\rangle$, which we could also write as

$$(|\alpha_i^R\rangle\langle\alpha_i^R| \otimes 1^Q)|\Psi^{RQ}\rangle = \sqrt{p_i}\,|\alpha_i^R\rangle \otimes |\psi_i^Q\rangle. \tag{52}$$

Now consider the operator Γ^{RQ} given by

$$\begin{aligned}\Gamma^{RQ} &= \sum_j |\alpha_j^R\rangle\langle\alpha_j^R| \otimes |\psi_j^Q\rangle\langle\psi_j^Q| \\ &= \sum_j (1^R \otimes |\psi_j^Q\rangle\langle\psi_j^Q|)(|\alpha_j^R\rangle\langle\alpha_j^R| \otimes 1^Q).\end{aligned} \tag{53}$$

Since Γ^{RQ} is the sum of an orthogonal set of projections, it is itself a projection operator onto some subspace of $\mathcal{H}_R \otimes \mathcal{H}_Q$. $|\Psi^{RQ}\rangle$ itself is in this subspace:

$$\begin{aligned}\Gamma^{RQ}|\Psi^{RQ}\rangle &= \sum_j (1^R \otimes |\psi_j^Q\rangle\langle\psi_j^Q|)(|\alpha_j^R\rangle\langle\alpha_j^R| \otimes 1^Q)|\Psi^{RQ}\rangle \\ &= \sum_j (1^R \otimes |\psi_j^Q\rangle\langle\psi_j^Q|)\sqrt{p_j}\,|\alpha_j^R\rangle \otimes |\psi_j^Q\rangle \\ &= \sum_j \sqrt{p_j}\,|\alpha_j^R\rangle \otimes |\psi_j^Q\rangle \\ &= |\Psi^{RQ}\rangle.\end{aligned} \tag{54}$$

Therefore, we have the operator inequality $\Gamma^{RQ} \geqslant |\Psi^{RQ}\rangle\langle\Psi^{RQ}|$. This means that, for any vector $|\chi^{RQ}\rangle$,

$$\langle\chi^{RQ}|\Gamma^{RQ}|\chi^{RQ}\rangle \geqslant \langle\chi^{RQ}|(|\Psi^{RQ}\rangle\langle\Psi^{RQ}|)|\chi^{RQ}\rangle, \tag{55}$$

which in turn implies that, for all positive operators X^{RQ},

$$\mathrm{Tr}\Gamma^{RQ}X^{RQ} \geqslant \mathrm{Tr}|\Psi^{RQ}\rangle\langle\Psi^{RQ}|X^{RQ} = \langle\Psi^{RQ}|X^{RQ}|\Psi^{RQ}\rangle. \tag{56}$$

Let A_μ^Q be the operators in an operator-sum representation of the evolution superoperator $\mathcal{E}^Q$. Then

$$\begin{aligned}&\Gamma^{RQ}(1^R \otimes A_\mu^Q)|\Psi^{RQ}\rangle \\ &= \sum_j (1^R \otimes |\psi_j^Q\rangle\langle\psi_j^Q|)(|\alpha_j^R\rangle\langle\alpha_j^R| \otimes 1^Q)(1^R \otimes A_\mu^Q)|\Psi^{RQ}\rangle \\ &= \sum_j (1^R \otimes |\psi_j^Q\rangle\langle\psi_j^Q|)(1^R \otimes A_\mu^Q)(|\alpha_j^R\rangle\langle\alpha_j^R| \otimes 1^Q)|\Psi^{RQ}\rangle \\ &= \sum_j (1^R \otimes |\psi_j^Q\rangle\langle\psi_j^Q|)(1^R \otimes A_\mu^Q)\sqrt{p_j}\,|\alpha_j^R\rangle \otimes |\psi_j^Q\rangle \\ &= \sum_j (1^R \otimes |\psi_j^Q\rangle\langle\psi_j^Q|)\sqrt{p_j}\,|\alpha_j^R\rangle \otimes A_\mu^Q|\psi_j^Q\rangle \\ &= \sum_j \sqrt{p_j}\langle\psi_j^Q|A_\mu^Q|\psi_j^Q\rangle|\alpha_j^R\rangle \otimes |\psi_j^Q\rangle.\end{aligned} \tag{57}$$

If $\rho^{RQ'} = \mathcal{I}^R \otimes \mathcal{E}^Q(|\Psi^{RQ}\rangle\langle\Psi^{RQ}|)$, then

$$\begin{aligned}F_e &= \mathrm{Tr}|\Psi^{RQ}\rangle\langle\Psi^{RQ}|\rho^{RQ'} \\ &\leqslant \mathrm{Tr}\Gamma^{RQ}\rho^{RQ'} \\ &= \mathrm{Tr}\Gamma^{RQ}\rho^{RQ'}\Gamma^{RQ} \\ &= \sum_\mu \mathrm{Tr}\Gamma^{RQ}(1^R \otimes A_\mu^Q)|\Psi^{RQ}\rangle\langle\Psi^{RQ}|(1^R \otimes A_\mu^Q)^\dagger\Gamma^{RQ} \\ &= \sum_{j,k}\sum_\mu \sqrt{p_j p_k}\langle\psi_j^Q|A_\mu^Q|\psi_j^Q\rangle\langle\psi_k^Q|A_\mu^{Q\dagger}|\psi_k^Q\rangle\langle\psi_k^Q|\psi_j^Q\rangle \\ &\quad \times\langle\alpha_k^R|\alpha_j^R\rangle \\ &= \sum_k\sum_\mu p_k\langle\psi_k^Q|A_\mu^Q|\psi_k^Q\rangle\langle\psi_k^Q|A_\mu^{Q\dagger}|\psi_k^Q\rangle \\ &= \sum_k p_k\langle\psi_k^Q|\left(\sum_\mu A_\mu^Q|\psi_k^Q\rangle\langle\psi_k^Q|A_\mu^{Q\dagger}\right)|\psi_k^Q\rangle \\ &= \sum_k p_k\langle\psi_k^Q|\rho_k^{Q'}|\psi_k^Q\rangle \\ &= \overline{F}.\end{aligned} \tag{58}$$

Thus $\overline{F} \geqslant F_e$, as we wished to show. The average input-output fidelity under the evolution superoperator $\mathcal{E}^Q$ for any ensemble of pure states with density operator ρ^Q is bounded below by the entanglement fidelity F_e.

V. ENTROPY EXCHANGE

A. Definition

As shown in Eq. (38) above, if $|\Psi_1^{RQ}\rangle$ and $|\Psi_2^{RQ}\rangle$ are two purifications of ρ^Q and each is subjected to the same evolution superoperator $\mathcal{I}^R \otimes \mathcal{E}^Q$, the resulting states $\rho_1^{RQ'}$ and $\rho_2^{RQ'}$ will have exactly the same eigenvalues. Therefore,

$$S(\rho_1^{RQ'}) = S(\rho_2^{RQ'}), \tag{59}$$

where $S(\rho)$ is the von Neumann entropy of the density operator ρ. In other words, the entropy of the final joint state of

RQ is independent of which purification is chosen. Again, rather surprisingly, we have a quantity that depends only on the initial state ρ^Q and the evolution superoperator $\mathcal{E}^Q$; that is, we have a quantity that is *intrinsic* to Q. For a given ρ^Q and $\mathcal{E}^Q$, we therefore define the *entropy exchange* S_e to be

$$S_e = -\,\mathrm{Tr}\rho^{RQ'}\log\rho^{RQ'} \tag{60}$$

where $\rho^{RQ'}=\mathcal{I}^R\otimes\mathcal{E}^Q(|\Psi^{RQ}\rangle\langle\Psi^{RQ}|)$ and $|\Psi^{RQ}\rangle$ is some purification of ρ^Q.

Why call S_e the entropy ''exchange''? Suppose we have two systems A and B, initially in the state $\rho^{AB}=\rho^A\otimes\rho^B$, which interact according to a unitary evolution operator U^{AB}. The evolution of each system will be describable in terms of a superoperator. That is,

$$\mathcal{E}^A(\rho^A) = \mathrm{Tr}_B U^{AB}(\rho^A\otimes\rho^B)U^{AB\dagger}, \tag{61}$$

$$\mathcal{E}^B(\rho^B) = \mathrm{Tr}_A U^{AB}(\rho^A\otimes\rho^B)U^{AB\dagger}. \tag{62}$$

(In the definition of $\mathcal{E}^A$ we imagine that ρ^B is given, and vice versa.) We can thus calculate the entropy exchanges S_e^A and S_e^B This can be done by including reference systems R_A and R_B to purify the initial state:

$$|\Psi^{ABR_AR_B}\rangle = |\Psi^{AR_A}\rangle\otimes|\Phi^{BR_B}\rangle. \tag{63}$$

Now, since the overall evolution is unitary, the final state $|\Psi^{ABR_AR_B'}\rangle$ is also pure. This means that $\rho^{AR_A'}$ and $\rho^{BR_B'}$ have exactly the same nonzero eigenvalues and thus the same entropy. Thus $S_e^A=S_e^B$ In other words, the entropy exchange is a *common* quantity for two initially uncorrelated systems that interact unitarily.

We will now derive an explicit expression for S_e in terms of ρ^Q and $\mathcal{E}^Q$. Suppose we have an operator-sum representation for $\mathcal{E}^Q$ and we define

$$|\tilde{\Phi}_\mu^{RQ'}\rangle = (1^R\otimes A_\mu^Q)|\Psi^{RQ}\rangle. \tag{64}$$

(These are not normalized vectors in general.) Then

$$\rho^{RQ'} = \sum_\mu\ (1^R\otimes A_\mu^Q)|\Psi^{RQ}\rangle\langle\Psi^{RQ}|(1^R\otimes A_\mu^Q)^\dagger$$

$$= \sum_\mu\ |\tilde{\Phi}_\mu^{RQ'}\rangle\langle\tilde{\Phi}_\mu^{RQ'}|. \tag{65}$$

Thus the vectors $|\tilde{\Phi}_\mu^{RQ'}\rangle$ give us a pure state ensemble for $\rho^{RQ'}$. We can use these states to construct a purification for $\rho^{RQ'}$. Let us adjoin a system E whose Hilbert space $\mathcal{H}_E$ has at least as many dimensions as the number of A_μ^Q operators. Then the state

$$|\Upsilon^{RQE'}\rangle = \sum_\mu\ |\tilde{\Phi}_\mu^{RQ'}\rangle\otimes|\mu^E\rangle \tag{66}$$

(where the $|\mu^E\rangle$ are an orthonormal set of E states) will be a purification for $\rho^{RQ'}$.

Since the state $|\Upsilon^{RQE'}\rangle$ is a pure state, the reduced states

$$\rho^{RQ'} = \mathrm{Tr}_E|\Upsilon^{RQE'}\rangle\langle\Upsilon^{RQE'}|, \tag{67}$$

$$\rho^{E'} = \mathrm{Tr}_{RQ}|\Upsilon^{RQE'}\rangle\langle\Upsilon^{RQE'}| \tag{68}$$

will have the same entropy. Therefore, $S_e=S(\rho^{RQ'})=S(\rho^{E'})$. We can write down the density operator $\rho^{E'}$,

$$\rho^{E'} = \mathrm{Tr}_{RQ}|\Upsilon^{RQE'}\rangle\langle\Upsilon^{RQE'}|$$

$$= \sum_{\mu,\nu}\langle\tilde{\Phi}_\nu^{RQ'}|\tilde{\Phi}_\mu^{RQ'}\rangle|\mu^E\rangle\langle\nu^E|. \tag{69}$$

That is, $\rho^{E'}=\Sigma_{\mu\nu}W_{\mu\nu}|\mu^E\rangle\langle\nu^E|$, where

$$W_{\mu\nu} = \langle\tilde{\Phi}_\nu^{RQ'}|\tilde{\Phi}_\mu^{RQ'}\rangle$$

$$= \mathrm{Tr}|\tilde{\Phi}_\mu^{RQ'}\rangle\langle\tilde{\Phi}_\nu^{RQ'}|$$

$$= \mathrm{Tr}(1^R\otimes A_\mu^Q)|\Psi^{RQ'}\rangle\langle\Psi^{RQ'}|(1^R\otimes A_\nu^Q)^\dagger$$

$$= \mathrm{Tr}_Q A_\mu^Q(\ \mathrm{Tr}_R|\Psi^{RQ}\rangle\langle\Psi^{RQ}|)A_\nu^{Q\dagger}$$

$$= \mathrm{Tr}_Q A_\mu^Q\rho^Q A_\nu^{Q\dagger}. \tag{70}$$

In other words, we have the following prescription. Let W be a density operator with components (in some orthonormal basis)

$$W_{\mu\nu} = \mathrm{Tr}A_\mu^Q\rho^Q A_\nu^{Q\dagger}. \tag{71}$$

Then

$$S_e = S(W). \tag{72}$$

As explained in the Appendix, any two operator-sum representations for $\mathcal{E}^Q$ are related by a unitary matrix $U_{\mu\nu}$. This simply corresponds to the freedom to write the matrix $W_{\mu\nu}$ with respect to any basis (which obviously does not affect S_e). Let $P_\mu=W_{\mu\mu}$ be the diagonal elements of $W_{\mu\nu}$. These would be the probabilities given the state W for a complete measurement using the basis that yields the matrix elements $W_{\mu\nu}$. Therefore, $H(\vec{P})\geqslant S(W)$. But we could, by choosing the unitary matrix that diagonalizes $W_{\mu\nu}$, find a representation such that $H(\vec{P})=S(W)$. This yields another expression for S_e,

$$S_e = \min\left(-\sum_\mu\ P_\mu\log P_\mu\right), \tag{73}$$

where $P_\mu=\mathrm{Tr}A_\mu^Q\rho^Q A_\mu^{Q\dagger}$ and the minimum is taken over all operator-sum representations of $\mathcal{E}^Q$.

For a given input state ρ^Q, there is a ''diagonal'' operator-sum representation, in which $W_{\mu\nu}$ is diagonal. In this representation,

$$\mathrm{Tr}A_\mu^Q\rho^Q A_\nu^{Q\dagger}=0 \quad \text{for} \quad \mu\neq\nu. \tag{74}$$

If $\rho^Q=d^{-1}1^Q$ (the ''maximally mixed'' state), then this simply means that the various A_μ^Q operators are orthogonal in the operator inner product $\langle B,C\rangle=\mathrm{Tr}B^\dagger C$. This diagonal representation is minimal, in the sense that no other operator-sum representation includes a smaller number of A_μ^Q operators.

The evolution $\mathcal{E}^Q$ might in fact be due to unitary evolution of a larger system that includes an environment E, with E initially in a pure state and RQ initially in a pure entangled state. In this case the final state of RQE will be also be a pure state. Then $S(\rho^{E'})=S(\rho^{RQ'})=S_e$. In other words, the entropy exchange S_e is just the entropy produced in the environment, if it is initially in a pure state.

Note that the same $\rho^{E'}$ would have been obtained if we ignored the reference system R entirely and simply considered the unitary evolution of QE with an initial state ρ^Q for Q. The entropy produced in the environment does not depend on the dynamically isolated reference system R.

The assumption that the environment is initially in a pure state $|0^E\rangle$ at first seems too restrictive. For example, we may wish to consider environments that are initially in some thermal equilibrium state ρ^E. However, we may imagine that the environment consists of a ''near'' environment E_n and a ''far'' environment E_f. The system Q interacts only with the near environment E_n. The initial state of the full environment may be an entangled pure state, but the system Q will ''see'' a mixed state for E_n.

To summarize, the entropy exchange S_e has the following properties.

(i) S_e is a quantity intrinsic to the system Q and can be defined entirely in terms of the initial state ρ^Q and the superoperator $\mathcal{E}^Q$.

(ii) If the initial state ρ^Q arises because a larger system RQ is in a pure entangled state and if the reference system R has trivial dynamics, then the entropy exchange S_e is the entropy of the final state $\rho^{RQ'}$ of RQ. (It is easy to generalize this to the case when R itself can have arbitrary unitary evolution, i.e., when R is dynamically isolated but may have a nonzero internal Hamiltonian.)

(iii) If the nonunitary evolution of Q arises because Q interacts with an environment E that is initially in a pure state, then S_e is the entropy of the final state $\rho^{E'}$ of the environment.

(iv) If the initial state ρ^Q of the system Q is a pure state, we can adopt a unitary representation for $\mathcal{E}^Q$ in which E is also initially in a pure state. Then $\rho^{Q'}$ and $\rho^{E'}$ have the same eigenvalues. In this case, $S_e=S(\rho^{Q'})$, the entropy produced in the system Q.

B. Relation to other entropies

Once again, it is useful to emphasize what S_e is not. It is not, in general, the increase in the entropy of the system Q; in fact, this entropy may actually decrease, whereas S_e is never negative. It is also not always the entropy increase of the environment if the initial environment state is mixed. The entropy exchange S_e simply characterizes the information exchange between the system Q and the external world during the evolution given by $\mathcal{E}^Q$.

There are, however, inequalities relating S_e to entropy changes in Q and E. First we will relate the entropy exchange to changes in the entropy of Q. Suppose an evolution superoperator $\mathcal{E}^Q$ is given, together with an initial state ρ^Q of Q. We can always find a representation for $\mathcal{E}^Q$ as a unitary evolution on a larger system QE with an initial pure state $|0^E\rangle$ for the environment system. With this representation, the entropy of the joint initial state $S(\rho^{QE})=S(\rho^Q)$. The joint system QE evolves unitarily, so the entropy of the joint state remains unchanged. Thus $S(\rho^{QE'})=S(\rho^Q)$. The entropy exchange in this case is the final entropy of the environment $S(\rho^{E'})$. The triangle inequality [Eq. (29)] yields

$$S(\rho^Q)\geqslant S(\rho^{Q'})-S(\rho^{E'}), \quad S_e\geqslant S(\rho^{Q'})-S(\rho^Q). \tag{75}$$

In other words, the entropy exchange is no less than the increase in entropy of the system Q. We can also in this way establish that

$$S_e\leqslant S(\rho^Q)+S(\rho^{Q'}). \tag{76}$$

Now we relate S_e to the entropy change in the environment. In this case, we are given a particular (possibly mixed) initial state ρ^E for the environment and a particular unitary evolution U^{QE} for the joint system QE. Again, the initial state of Q is ρ^Q, but now we will imagine that this is a partial state of a pure entangled state $|\Psi^{RQ}\rangle$, where R is an isolated reference system. The entropy of the joint system RQE is initially $S(\rho^{RQE})=S(\rho^E)$ and remains unchanged during the unitary evolution of the joint system. By definition, the entropy exchange is just the entropy $S(\rho^{RQ'})$ of the final state of RQ. Thus

$$S(\rho^E)\geqslant S(\rho^{E'})-S(\rho^{RQ'}), \quad S_e\geqslant S(\rho^{E'})-S(\rho^E), \tag{77}$$

so that the entropy exchange is no less than the increase in the entropy of the environment. We can also derive

$$S_e\leqslant S(\rho^E)+S(\rho^{E'}), \tag{78}$$

which, for a large environment, is probably not very useful.

Similar arguments based on the subaddtivity of the entropy functional [Eq. (28)], also demonstrate that S_e is no smaller than the entropy *decrease* in either the system Q or the environment E. To summarize the lower bounds for S_e,

$$S_e\geqslant|\Delta S^Q|, \tag{79}$$

$$S_e\geqslant|\Delta S^E|, \tag{80}$$

where ΔS^Q and ΔS^E are the changes in entropy of the system Q and environment E, respectively.

C. Entropy exchange and eavesdropping

There is a simple application of these ideas to quantum cryptography [16]. Suppose Alice prepares the state ρ_k^Q of Q with probability p_k and then conveys the system Q to Bob as part of a quantum cryptographic protocol. (Alternatively, we could imagine that Alice prepares Q in a state entangled with a system R, which she retains, as part of an entanglement-based protocol [17]. But, in such protocols, Alice usually later makes a measurement on R, giving rise to an ensemble of relative states of Q.) Along the way Q may interact with the rest of the world, represented by the environment system E, producing some level of ''noise'' in Q. The environment, however, may also contain the measuring

apparatus of an eavesdropper Eve. We will assume that the environment is initially in a pure state (but see the remark above about the possibility of an entangled state of near and far zones within the environment).

The dynamical evolution of Q is given by the evolution superoperator $\mathcal{E}^Q$. Let $S_{e,k}$ be the entropy exchange in Q for the input state ρ_k^Q which equals the entropy of the final environment state $\rho_k^{E'}$ resulting from the input of ρ_k^Q and let S_e be the entropy exchange associated with the ''average'' input state $\rho^Q=\Sigma_k p_k \rho_k^Q$ which equals the entropy of the average final environment state $\rho^{E'}$.

The eavesdropper Eve will try to infer the preparation ρ_k^Q by examining the state of her measuring apparatus, that is, by trying to distinguish the various environment states $\rho_k^{E'}$ Denote Alice's preparation, and thus the final environment state produced by that preparation, by the random variable X and the reading on Eve's measuring apparatus by Y. Then a theorem of Kholevo [18] limits the mutual information $I(X:Y)$, which is the amount of information about X that Eve obtains from a knowledge of Y. This limit is

$$I(X:Y)\leqslant S(\rho^{E'})-\sum_k p_k S(\rho_k^{E'})=S_e-\sum_k p_k S_{e,k} \quad (81)$$

$$\leqslant S_e . \quad (82)$$

[If the eavesdropper Eve only has access to part of the environment system E, then she will be able to do no better and $I(X:Y)$ will still be bounded in this way.]

Thus the entropy exchange associated with the ensemble of input states and the evolution superoperator $\mathcal{E}^Q$, both of which can be determined, in principle, from repeated use of the channel Q, limits the amount of information that any eavesdropper might obtain about the input. Put another way, any process by which the eavesdropper obtains information about the channel system Q disturbs the system, leaving traces in the evolution superoperator $\mathcal{E}^Q$. The disturbance produced by the eavesdropper (and other interactions with the environment) is characterized by the entropy exchange S_e.

VI. THE QUANTUM FANO INEQUALITY

A. Classical theorem

In classical information theory, there is a simple relation between the noise in a channel and probability of error in that channel [15]. This relation is Fano's inequality. We will derive an analogous quantum relation.

Let X be a classical random variable representing the input of a noisy channel and suppose that X can take on up to N different values. The output of the noisy channel is represented by the random variable Y. The channel itself is represented by the conditional probabilities $p(y_k|x_j)$ of an output value y_k given an input value x_j. These probabilities, together with the input probability distribution $p(x_j)$, characterize the situation. The receiver makes an estimate $\hat{X}$ of the input X based only on the channel output Y. The probability of error P_E is the total likelihood that $\hat{X}\neq X$.

Fano's inequality (in its stronger form) states that

$$h(P_E)+P_E\log(N-1)\geqslant H(X|Y), \quad (83)$$

where $h(P_E)=-P_E\log P_E-(1-P_E)\log P_E$ and $H(X|Y)$ is the Shannon conditional entropy of X given Y. $H(X|Y)$, the average residual information uncertainty about the input given the output, is a measure of the noise in the channel. $H(X|Y)=0$ for a noiseless channel, in which the input X can be exactly determined by the output Y. Noting that $h(P_E)\leqslant 1$ (since our logarithms are base 2), we can derive a simpler but slightly weaker form of Fano's inequality,

$$1+P_E\log N>H(X|Y). \quad (84)$$

Fano's inequality is used to prove the ''weak converse'' of the classical noisy coding theorem, which states that information cannot be sent at a rate greater than the channel capacity with arbitrarily low probability of error [15].

B. Quantum theorem

We now turn to the quantum problem. As before, we suppose that the system RQ is initially in the entangled state $|\Psi^{RQ}\rangle$ and that Q is subjected to an evolution described by $\mathcal{E}^Q$. The reference system R is isolated and has trivial dynamics described by $\mathcal{I}^R$. The dimensions of $\mathcal{H}_Q$ and $\mathcal{H}_R$ are both finite and equal to d. After the evolution, the system is described by a joint state $\rho^{RQ'}$.

Now suppose that we subject the final state $\rho^{RQ'}$ to a measurement of a complete ordinary observable on the system RQ, which is described by a basis of d^2 orthogonal states for RQ. Let the random variable X represent the outcome of this measurement. Then we know [from Eq. (32)] that

$$S_e=S(\rho^{RQ'})\leqslant H(X). \quad (85)$$

Further suppose that one of these basis vectors is chosen to be the original state $|\Psi^{RQ}\rangle$. Then the fidelity $F_e=\langle\Psi^{RQ}|\rho^{RQ'}|\Psi^{RQ}\rangle$ is just the probability of this outcome. Given this probability, the largest possible value of $H(X)$ would occur when all of the d^2-1 other outcomes have equal probability. Then

$$\begin{aligned}\max H(X)&=-F_e\log F_e-(d^2-1)\frac{1-F_e}{d^2-1}\log\frac{1-F_e}{d^2-1}\\&=-F_e\log F_e-(1-F_e)\log(1-F_e)\\&\quad+(1-F_e)\log(d^2-1). \quad (86)\end{aligned}$$

Therefore we can conclude that

$$h(F_e)+(1-F_e)\log(d^2-1)\geqslant S_e . \quad (87)$$

This is our quantum version of the Fano inequality, relating the entanglement fidelity F_e with the entropy exchange S_e. Although we have made use of the reference system R in deriving this inequality, both F_e and S_e have meanings that are intrinsic to the system Q.

As before, we can give a slightly weaker form of the inequality:

$$1+2(1-F_e)\log d\geqslant S_e . \quad (88)$$

It is instructive to compare the form of this equation to that of Eq. (84). The number N of possible input states is analogous the dimension d of $\mathcal{H}_Q$. The probability of error P_E roughly corresponds $1-F_e$, the amount by which the final entangled state fails to correspond to the initial one. The noise term $H(X|Y)$ is replaced by the entropy exchange S_e. Finally, a factor of 2 appears in the error term in the quantum case, which in fact corresponds to replacing N by d^2, the dimension of $\mathcal{H}_Q\otimes\mathcal{H}_R$.

We can strengthen the quantum Fano inequality in a number of ways. First, if the reference system R has a Hilbert space of dimension $d_R<d$, the quantity d^2 can be replaced by the product d_Rd. The required dimension d_R is in fact just the dimension of the subspace that supports ρ^R and so $d_R\leqslant d$ even if R is much larger than Q. Since we wish to consider F_e and S_e to be quantities intrinsic to Q, though, we will simply adopt $d_R=d$.

Finally, we note that the fidelity F_e can be lowered by *internal dynamics* of Q as well as by information exchange with the environment. To take this into account, we could allow the final state of the system to be ''processed'' via any unitary transformation U^Q on Q and define

$$\hat{F}_e=\max_{U^Q}\langle\Psi^{RQ}|(1^R\otimes U^Q)\rho^{RQ'}(1^R\otimes U^Q)^\dagger|\Psi^{RQ}\rangle. \quad (89)$$

($\hat{F}_e$ is also independent of the particular purification for ρ^Q and is thus an quantity intrinsic to Q.) Clearly $\hat{F}_e\geqslant F_e$. A derivation very similar to the one we have given allows us to replace F_e by $\hat{F}_e$ in Eq. (87), obtaining

$$h(\hat{F}_e)+(1-\hat{F}_e)\log(d^2-1)\geqslant S_e, \quad (90)$$

$$1+2(1-\hat{F}_e)\log d\geqslant S_e. \quad (91)$$

We could further extend this by allowing Q to be subjected to a second arbitrary completely positive map after $\mathcal{E}^Q$ and obtain a similar relation. However, in this case the relevant entropy exchange $\hat{S}_e$ would be that due to the total evolution, both $\mathcal{E}^Q$, and the subsequent ''processing.'' Since it is possible that $\hat{S}_e<S_e$, we do not obtain a useful general relation. (This is precisely what happens in quantum error-correcting codes, as explained below.)

VII. REMARKS

One possible application of entanglement fidelity and entropy exchange is in the study of nonideal quantum computers [19]. In a typical state of a quantum computer, the different parts of the computer are in a highly entangled state. The elements of the computer's memory must maintain their states in such a fashion that this entanglement is preserved. The considerations in these notes are thus particularly suited to studying the effects of noise and decoherence in this context.

What we have found is that the capability of a system Q to preserve its entanglement with some other system R can be determined from the initial state and the dynamics of Q itself. Destruction or distortion of entanglement, and information exchange with the environment, leave distinct traces in the dynamics of the system itself. We can characterize these by the entanglement fidelity F_e and the entropy exchange S_e.

F_e is properly thought of not as the fidelity of one state with another (though it can be given that interpretation by including a reference system R) but as the fidelity of a *process* given by the input state ρ^Q and the system dynamics $\mathcal{E}^Q$. F_e does not just measure how *well* the state of Q is preserved by $\mathcal{E}^Q$, but also how *coherently*. If the input state is a pure state, these amount to the same thing; but otherwise, F_e is a stronger measure of the amount of disturbance the state experiences.

S_e is also properly thought of not as the entropy of some state but as the entropy associated with the dynamical process given by ρ^Q and $\mathcal{E}^Q$. Information exchange with the environment, even if it does not change the entropy of either the system Q or the environment E, can lead to nonzero entropy exchange S_e. Entropy exchange is therefore a clearer measure of this exchange than the changes in entropy of either system.

The relationship between F_e and S_e amounts to a quantum Fano inequality, connecting the information exchange with the environment to the disturbance of the state. This illustrates very clearly a general principle: In quantum information theory, noise is exactly information exchange with an external system. In a classical system, information can be ''leaked'' into the environment with arbitrarily little disturbance to the system: the environment can simply make a copy of the information, leaving the original intact within the system. But quantum information cannot be copied. Any departure of information into the environment necessarily yields an irreducible disturbance of the system. (This is the fundamental idea behind quantum cryptography see [20].) The departing information leaves its ''footprints'' behind in the entropy exchange S_e and associated imperfect entanglement fidelity F_e.

These ideas shed an interesting light on the recently discovered quantum error-correcting codes [6]. In these codes, input quantum states are represented by massively entangled states of a system Q composed of many qubits: $Q=Q_1\cdots Q_n$. The environment is assumed to act independently on these systems, which in our language corresponds to the requirement that the evolution superoperator for the system Q factorizes:

$$\mathcal{E}^Q=\mathcal{E}^{Q_1}\otimes\cdots\otimes\mathcal{E}^{Q_2}. \quad (92)$$

The resulting state is then subjected to a second process, which typically involves an incomplete measurement on Q followed by a unitary evolution (which depends on the measurement result). Under certain circumstances, the original state of the system may be restored with very high fidelity.

The action of the channel and the subsequent restoration process of the sequence of qubits can be written as a single superoperator for $Q_1\cdots Q_n$. Since the fidelity of this combined process is high, we can conclude, rather surprisingly, that the total entropy exchange is quite low. At first this seems paradoxical since the individual entropy exchanges of the noise process and the restoration measurement may both be high.

But this is not too difficult to understand. Let E represent the environment system that interacts with the qubits during

the noise stage and let M represent the apparatus that performs the restoration process. To begin with, we might imagine that E and M are in pure states. After Q interacts with E (and thus exchanges information), the state of QE becomes entangled. In the second stage, M interacts and exchanges information with Q, and the entanglement of Q with the rest of the world is reduced: it is passed to M. At the end of the process, both Q and the ''rest of the world'' EM are in near-pure states, but E and M have now become entangled.

Thus the process of quantum error correction can be thought of as a process of passing entanglement (produced by a previous interaction with the environment) to the apparatus, in such a way that the entropy exchange for the total process (noise followed by restoration) on Q is very low. If S_e is very low, then the overall dynamics for Q is nearly unitary, so that the original state of Q can be approximately recovered. It is not yet known under what general circumstances, and to what fidelity, this can be accomplished.

ACKNOWLEDGMENTS

The author is indebted to many people for extensive conversations about the issues discussed in this paper, including H. Barnum, C. H. Bennett, C. M. Caves, I. Chuang, A. Ekert, C. A. Fuchs, E. H. Knill, R. Jozsa, R. Laflamme, J. Smolin, M. D. Westmoreland, W. K. Wootters, and W. H. Zurek. He also wishes to acknowledge the hospitality and support of the Theoretical Astrophysics group (T-6) at Los Alamos National Laboratory.

APPENDIX: REPRESENTATION THEOREMS

1. Index states and relative states

In this appendix we will use some of the ideas from the main text to show that any trace-preserving, completely positve linear map has both an operator-sum representation and a unitary representation. This derivation is somewhat more direct than that found in [9]. We will also suggest a useful characterization of all such representations.

Suppose R and Q are quantum systems with $\dim\mathcal{H}_R=\dim\mathcal{H}_Q=d$ and let $|\alpha_k^R\rangle$ and $|\beta_k^Q\rangle$ be orthonormal basis vectors for $\mathcal{H}_R$ and $\mathcal{H}_Q$. We can write down a maximally entangled pure state of RQ,

$$|\Psi^{RQ}\rangle=\frac{1}{\sqrt{d}}\sum_k |\alpha_k^R\rangle\otimes|\beta_k^Q\rangle. \tag{A1}$$

It will be convenient to consider instead the non-normalized vector

$$|\widetilde{\Psi}^{RQ}\rangle=\sqrt{d}|\Psi^{RQ}\rangle=\sum_k |\alpha_k^R\rangle\otimes|\beta_k^Q\rangle. \tag{A2}$$

(Using $|\widetilde{\Psi}^{RQ}\rangle$ rather than $|\Psi^{RQ}\rangle$ will eliminate some factors of $\sqrt{d}$ in our expressions.)

For every state $|\zeta^R\rangle$ of R there is a unique state $|\xi^Q\rangle$ such that

$$\frac{1}{\sqrt{d}}|\xi^Q\rangle=\langle\zeta^R|\Psi^{RQ}\rangle \tag{A3}$$

$$|\xi^Q\rangle=\langle\zeta^R|\widetilde{\Psi}^{RQ}\rangle. \tag{A4}$$

The relation between $|\zeta^R\rangle$ and $|\xi^Q\rangle$ is a one-to-one correspondence. We call $|\xi^Q\rangle$ the *relative state* in Q to $|\zeta^R\rangle$ and we call $|\zeta^R\rangle$ the *index state* in R that yields $|\xi^Q\rangle$.

Given a state $|\phi^Q\rangle$, let us denote the associated index state in R by $|\phi^{*R}\rangle$. We can give a simple prescription for finding $|\phi^{*R}\rangle$ from $|\phi^Q\rangle$. Suppose

$$|\phi^Q\rangle=\sum_k c_k|\beta_k^Q\rangle. \tag{A5}$$

Then

$$|\phi^{*R}\rangle=\sum_k c_k^*|\alpha_k^R\rangle, \tag{A6}$$

as can be easily seen:

$$\langle\phi^{*R}|\widetilde{\Psi}^{RQ}\rangle=\sum_{kl} c_k\langle\alpha_k^R|\alpha_l^R\rangle|\beta_l^Q\rangle$$

$$=\sum_k c_k|\beta_k^Q\rangle=|\phi^Q\rangle. \tag{A7}$$

It is also clear that

$$|\phi^{*R}\rangle\langle\phi^{*R}|\otimes|\phi^Q\rangle\langle\phi^Q|$$

$$=(|\phi^{*R}\rangle\langle\phi^{*R}|\otimes 1^Q)|\widetilde{\Psi}^{RQ}\rangle\langle\widetilde{\Psi}^{RQ}|(|\phi^{*R}\rangle\langle\phi^{*R}|\otimes 1^Q), \tag{A8}$$

a relation that will be useful later on.

The function that takes $|\phi^Q\rangle$ to $|\phi^{*R}\rangle$ is conjugate linear. If $|\phi^Q\rangle=a_1|\phi_1^Q\rangle+a_2|\phi_2^Q\rangle$, then

$$|\phi^{*R}\rangle=a_1^*|\phi_1^{*R}\rangle+a_2^*|\phi_2^{*R}\rangle, \tag{A9}$$

$$\langle\phi^{*R}|=a_1\langle\phi_1^{*R}|+a_2\langle\phi_2^{*R}|. \tag{A10}$$

2. Operator-sum representations

Let $\mathcal{E}^Q$ be the trace-preserving, completely positive linear map that describes the dynamical evolution of the system Q. Since $\mathcal{E}^Q$ is completely positive, any trivial extension of it is positive; in particular, the superoperator $\mathcal{I}^R\otimes\mathcal{E}^Q$ is positive. Thus the state

$$\rho^{RQ'}=\mathcal{I}^R\otimes\mathcal{E}^Q(|\Psi^{RQ}\rangle\langle\Psi^{RQ}|) \tag{A11}$$

is a positive operator, as is

$$D^{RQ'}=d\rho^{RQ'}=\mathcal{I}^R\otimes\mathcal{E}^Q(|\widetilde{\Psi}^{RQ}\rangle\langle\widetilde{\Psi}^{RQ}|). \tag{A12}$$

Of course, $\rho^{RQ'}$ has unit trace, so it is a normalized density operator, while $\mathrm{Tr}D^{RQ'}=d$.

The operation of realizing a state of Q via choosing an index state of R commutes with the dynamical operation given by $\mathcal{I}^R\otimes\mathcal{E}^Q$. In other words, if we wish to write down

the final state $\rho^{Q'}=\mathcal{E}^Q(\rho^Q)$, where $\rho^Q=|\phi^Q\rangle\langle\phi^Q|$, we can either apply the index state $|\phi^{*R}\rangle$ to $|\tilde{\Psi}^{RQ}\rangle$ and then apply $\mathcal{E}^Q$ or we can apply the extended superoperator $\mathcal{I}^R\otimes\mathcal{E}^Q$ to the joint state and then apply the index state; thus

$$\rho^{Q'}=\langle\phi^{*R}|D^{RQ'}|\phi^{*R}\rangle. \tag{A13}$$

This makes sense on physical grounds. A measurement of an observable on R involves a completely different system than the dynamical evolution of Q, and the two operations might take place arbitrarily far apart. The time order of the two should irrelevant to the result.

A more formal argument runs as follows. Let Φ^R be the superoperator (i.e., a linear map on operators on $\mathcal{H}_R$) associated with multiplication by $|\phi^{*R}\rangle\langle\phi^{*R}|$ on both sides. That is, if T^R is an operator on $\mathcal{H}_R$, then $\Phi^R(T^R)=|\phi^{*R}\rangle\langle\phi^{*R}|T^R|\phi^{*R}\rangle\langle\phi^{*R}|$. The superoperator $\Phi^R\otimes\mathcal{I}^Q$ (which is just multiplication on both sides by $|\phi^{*R}\rangle\langle\phi^{*R}|\otimes 1^Q$) obviously commutes with the dynamical superoperator $\mathcal{I}^R\otimes\mathcal{E}^Q$. Therefore,

$$\begin{aligned}\Phi^R\otimes\mathcal{I}^Q[D^{RQ'}]&=\Phi^R\otimes\mathcal{I}^Q[\mathcal{I}^R\otimes\mathcal{E}^Q(|\tilde{\Psi}^{RQ}\rangle\langle\tilde{\Psi}^{RQ}|)]\\&=\mathcal{I}^R\otimes\mathcal{E}^Q[\Phi^R\otimes\mathcal{I}^Q(|\tilde{\Psi}^{RQ}\rangle\langle\tilde{\Psi}^{RQ}|)]\\&=\mathcal{I}^R\otimes\mathcal{E}^Q[(|\phi^{*R}\rangle\langle\phi^{*R}|\otimes 1^Q)|\tilde{\Psi}^{RQ}\rangle\\&\quad\times\langle\tilde{\Psi}^{RQ}|(|\phi^{*R}\rangle\langle\phi^{*R}|\otimes 1^Q)]\\&=\mathcal{I}^R\otimes\mathcal{E}^Q(|\phi^{*R}\rangle\langle\phi^{*R}|\otimes|\phi^Q\rangle\langle\phi^Q|)\\&=|\phi^{*R}\rangle\langle\phi^{*R}|\otimes\rho^{Q'}.\end{aligned} \tag{A14}$$

From this we can see that

$$\rho^{Q'}=\mathcal{E}^Q(|\phi^Q\rangle\langle\phi^Q|)=\langle\phi^{*R}|D^{RQ'}|\phi^{*R}\rangle \tag{A15}$$

as we wished to show.

The operator $D^{RQ'}$ is positive; thus we can find a set of vectors $|\tilde{\mu}^{RQ'}\rangle$ such that

$$D^{RQ'}=\sum_\mu |\tilde{\mu}^{RQ'}\rangle\langle\tilde{\mu}^{RQ'}|. \tag{A16}$$

These vectors, for example, might be constructed from the eigenvectors of $D^{RQ'}$, normalized by their eigenvalues; but there are many such decompositions. In fact, it is easy to see that the $|\tilde{\mu}^{RQ'}\rangle$ vectors are simply related to the representation of $\rho^{RQ'}$ by an ensemble of pure states. That is, given such a representation

$$\rho^{RQ'}=\sum_\mu p_\mu|\psi_\mu^{RQ'}\rangle\langle\psi_\mu^{RQ'}|, \tag{A17}$$

we can simply set $|\tilde{\mu}^{RQ'}\rangle=\sqrt{p_\mu d}\,|\psi_\mu^{RQ'}\rangle$. It is also clear that there is a decomposition of $D^{RQ'}$ with no more than d^2 vectors $|\tilde{\mu}^{RQ'}\rangle$, since the dimension of the space $\mathcal{H}_R\otimes\mathcal{H}_Q$ is d^2.

Here comes the essential trick. Define the operator A_μ^Q by

$$A_\mu^Q|\phi^Q\rangle=\langle\phi^{*R}|\tilde{\mu}^{RQ'}\rangle \tag{A18}$$

for each state $|\phi^Q\rangle$ of Q. Because of the conjugate linear relation between $|\phi^Q\rangle$ and $|\phi^{*R}\rangle$, each A_μ^Q thus defined is a perfectly good linear operator on $\mathcal{H}_Q$. Furthermore,

$$\begin{aligned}\sum_\mu A_\mu^Q|\phi^Q\rangle\langle\phi^Q|A_\mu^{Q\dagger}&=\sum_\mu\langle\phi^{*R}|\tilde{\mu}^{RQ'}\rangle\langle\tilde{\mu}^{RQ'}|\phi^{*R}\rangle\\&=\langle\phi^{*R}|D^{RQ'}|\phi^{*R}\rangle\\&=\mathcal{E}^Q(|\phi^Q\rangle\langle\phi^Q|).\end{aligned} \tag{A19}$$

We have thus derived an operator-sum representation for the completely positive map $\mathcal{E}^Q$ for all pure input states $|\phi^Q\rangle\langle\phi^Q|$. Extending this to mixed state inputs is trivial, of course, since every mixed state is a linear (convex) combination of pure states. We can further see that each completely positive map $\mathcal{E}^Q$ has an operator-sum representation with no more than d^2 terms.

We also find that, for our operator-sum representation for $\mathcal{E}^Q$,

$$\begin{aligned}\sum_\mu\langle\phi^Q|A_\mu^QA_\mu^{Q\dagger}|\phi^Q\rangle&=\mathrm{Tr}\sum_\mu A_\mu^Q|\phi^Q\rangle\langle\phi^Q|A_\mu^{Q\dagger}\\&=\mathrm{Tr}\rho^{Q'}\\&=1\end{aligned} \tag{A20}$$

since $\mathcal{E}^Q$ is trace preserving by assumption. Since this is true for all states $|\phi^Q\rangle$, including the eigenstates of the positive operator $\Sigma_\mu A_\mu^{Q\dagger}A_\mu^Q$, we conclude that

$$\sum_\mu A_\mu^{Q\dagger}A_\mu^Q=1^Q. \tag{A21}$$

3. Unitary representations

Having derived an operator-sum representation for $\mathcal{E}^Q$, it is easy to arrive at a unitary representation. Add an extra quantum system E and write down a purification $|\tilde{\Upsilon}^{RQE'}\rangle$ for $D^{RQ'}$ as

$$|\tilde{\Upsilon}^{RQE'}\rangle=\sum_\mu|\tilde{\mu}^{RQ'}\rangle\otimes|\epsilon_\mu^E\rangle \tag{A22}$$

for an orthonormal set of vectors $|\epsilon_\mu^E\rangle$ in $\mathcal{H}_E$. (Again, finding a purification for $D^{RQ'}$ is equivalent to finding a purification for $\rho^{RQ'}$, but it is slightly easier to work with the nonnormalized states.) We note that we require no more than d^2 dimensions in $\mathcal{H}_E$ to construct this purification since there are decompositions of $D^{RQ'}$ with no more than d^2 vectors $|\tilde{\mu}^{RQ'}\rangle$. Fix some state $|0^E\rangle$ of E. We can define an operator U^{QE} on a subspace of $\mathcal{H}_Q\otimes\mathcal{H}_E$ by

$$\begin{aligned}U^{QE}(|\phi^Q\rangle\otimes|0^E\rangle)&=\langle\phi^{*R}|\tilde{\Upsilon}^{RQE'}\rangle=\sum_\mu\langle\phi^{*R}|\tilde{\mu}^{RQ'}\rangle\otimes|\epsilon_\mu^E\rangle\\&=\sum_\mu A_\mu^Q|\phi^Q\rangle\otimes|\epsilon_\mu^E\rangle=|\Phi^{QE'}\rangle\end{aligned} \tag{A23}$$

for all $|\phi^Q\rangle$ in $\mathcal{H}_Q$. Once again, the conjugate linear relation of index state and relative state guarantees that this is a linear operator. Furthermore, given two states $|\phi_1^Q\rangle$ and $|\phi_2^Q\rangle$,

$$\begin{aligned}\langle\Phi_1^{QE'}|\Phi_2^{QE'}\rangle &= \langle\widetilde{\Upsilon}^{RQE'}|\phi_1^{*R}\rangle\langle\phi_2^{*R}|\widetilde{\Upsilon}^{RQE'}\rangle \\ &= \sum_{\mu,\nu}\langle\phi_1^Q|A_\mu^{Q\dagger}A_\nu^Q|\phi_2^Q\rangle\langle\epsilon_\mu^Q|\epsilon_\nu^E\rangle \\ &= \sum_{\mu}\langle\phi_1^Q|A_\mu^{Q\dagger}A_\mu^Q|\phi_2^Q\rangle \\ &= \langle\phi_1^Q|\phi_2^Q\rangle. \end{aligned} \tag{A24}$$

The operator U^{QE} preserves inner products on this subspace of states; it can therefore be extended to a unitary operator on the entire space $\mathcal{H}_Q\otimes\mathcal{H}_E$.

Thus we have a unitary representation for $\mathcal{E}^Q$,

$$\begin{aligned}&\mathrm{Tr}_E U^{QE}(|\phi^Q\rangle\langle\phi^Q|\otimes|0^E\rangle\langle 0^E|)U^{QE\dagger} \\ &= \mathrm{Tr}_E\sum_{\mu,\nu}(A_\mu^Q|\phi^Q\rangle\langle\phi^Q|A_\nu^{Q\dagger})\otimes|\epsilon_\mu^E\rangle\langle\epsilon_\nu^E| \\ &= \sum_{\mu,\nu}(A_\mu^Q|\phi^Q\rangle\langle\phi^Q|A_\nu^{Q\dagger})\langle\epsilon_\nu^E|\epsilon_\mu^E\rangle \\ &= \sum_{\mu}A_\mu^Q|\phi^Q\rangle\langle\phi^Q|A_\nu^{Q\dagger} = \mathcal{E}^Q(|\phi^Q\rangle\langle\phi^Q|). \end{aligned} \tag{A25}$$

Once again, we can extend this unitary representation to mixed state inputs since these are linear (convex) combinations of pure states.

4. Remarks

In the above arguments, we arrived at an operator-sum representation for $\mathcal{E}^Q$ by a decomposition of $D^{RQ'}$, that is, by a pure state ensemble for $\rho^{RQ'}$. It is also easy to see that every operator-sum representation for $\mathcal{E}^Q$, when extended and applied to $|\Psi^{RQ}\rangle$, will yield such a decomposition. [Simply define $|\widetilde{\mu}^{RQ'}\rangle = (1^R\otimes A_\mu^Q)|\Psi^{RQ}\rangle$.] Thus the operator-sum representations for $\mathcal{E}^Q$ are in a one-to-one correspondence with the pure state ensembles for $\rho^{RQ'}$.

Similarly, we obtained a unitary representation for $\mathcal{E}^Q$ by finding a purification for $D^{RQ'}$ or equivalently for $\rho^{RQ'}$. But every unitary representation will be associated with such a purification because the initial total state $|\Psi^{RQ}\rangle\otimes|0^E\rangle$ of RQE will evolve unitarily to a pure state, from which the state $\rho^{RQ'}$ is obtained by a partial trace over E. Now, any such purification of $\rho^{RQ'}$ can be obtained from any other by means of a unitary transformation that acts on $\mathcal{H}_E$, which corresponds to an internal rotation of the environment system E that acts *after* the interaction of Q and E.

The nonuniqueness of the operator-sum representation and the unitary representations are related since every pure state ensemble for $\rho^{RQ'}$ can be realized by fixing a purification $|\Upsilon^{RQE'}\rangle$ and choosing a complete ordinary measurement for E (i.e., an orthonormal basis for $\mathcal{H}_E$). Equivalently, we might fix a measurement basis for $\mathcal{H}_E$ and a particular purification. A change of representation in each case will be associated with a unitary matrix corresponding to a rotation in $\mathcal{H}_E$. That is, suppose that for all ρ^Q,

$$\mathcal{E}^Q(\rho^Q) = \sum_\mu A_\mu^Q\rho^Q A_\mu^{Q\dagger} = \sum_\nu B_\nu^Q\rho^Q B_\nu^{Q\dagger}, \tag{A26}$$

so that the A_μ^Q and the B_ν^Q operators both form operator-sum representations for $\mathcal{E}^Q$. Then there is a unitary matrix $U_{\mu\nu}$ so that

$$A_\mu^Q = \sum_\nu U_{\mu\nu}B_\nu^Q. \tag{A27}$$

(Note that we may have to extend one operator-sum representation by a finite number of zero operators so that the two representations have the same number of operators.) The matrix $U_{\mu\nu}$ is in fact the matrix that relates two different bases in E, corresponding to two purifications related, in the sense outlined above, to the two operator-sum representations.

[1] C. H. Bennett, Physics Today **48**, 24 (1995).

[2] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).

[3] R. Jozsa and B. Schumacher, J. Mod. Opt. **41**, 2343 (1994); B. Schumacher Phys. Rev. A **51**, 2738 (1995); H. Barnum, C. A. Fuchs, R. Jozsa, and B. Schumacher (unpublished).

[4] R. Jozsa, J. Mod. Opt. **41**, 2315 (1995).

[5] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *ibid.* **69**, 2881 (1992).

[6] P. W. Shor, Phys. Rev. A **52**, 2493 (1995); A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996); A. Steane, Phys. Rev. Lett. **77**, 793 (1996); R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, *ibid.* **77**, 198 (1996).

[7] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[8] W. F. Stinespring, Proc. Am. Math. Soc. **6**, 211 (1955); K. Kraus, Ann. of Phys. (N.Y.) **64**, 311 (1971).

[9] K. Hellwig and K. Kraus, Commun. Math. Phys. **16**, 142 (1970); M.-D. Choi, Linear Algebra Appl. **10**, 285 (1975); K. Kraus, *States, Effects, and Operations: Fundamental Notions of Quantum Theory* (Springer-Verlag, Berlin, 1983).

[10] L. P. Hughston, R. Jozsa, and W. K. Wooters, Phys. Lett. A **183**, 14 (1993).

[11] H. Everett III, Rev. Mod. Phys. **29**, 454 (1957).

[12] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976), A. Peres, Found. Phys. **20**, 1441 (1990).

[13] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, translated by E. T. Beyer (Princeton University Press, Princeton, 1955).

[14] A. Wehrl, Rev. Mod. Phys. **50**, 221 (1978).

[15] T. M. Cover and J. A. Thomas, *Elements of Information*

Theory (Wiley, New York, 1991).

[16] C. H. Bennett and G. Brassard, *Proceedings of the IEEE Conference on Computers, Systems, and Signal Processing, Bangalore, 1984* (IEEE, New York, 1984), p. 175; C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Crypt. **5**, 3 (1992).

[17] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[18] A. S. Kholevo, Prob. Peredachi Info. **9**, 3 (1973) Prob. Info. Transm. (USSR) **9**, 177 (1973); C. Caves and C. Fuchs, Phys. Rev. Lett. **73**, 3047 (1994); B. Schumacher, M. D. Westmoreland, and W. K. Wootters, Phys. Rev. Lett. **76**, 3452 (1996).

[19] S. Lloyd, Sci. Am. **273**, 140 (1995); A. Ekert and R. Jozsa, Rev. Mod. Phys. (to be published).

[20] C. A. Fuchs, Ph.D. thesis, The University of New Mexico, Albuquerque, NM (1996); C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2308 (1996).