Quantum data processing and error correction

Benjamin Schumacher[1,2,*] and M. A. Nielsen[1]
[1]*Center for Advanced Studies, Department of Physics and Astronomy, University of New Mexico, Albuquerque, New Mexico 87131*
[2]*Theoretical Astrophysics, T-6, M.S. B288, Los Alamos National Laboratory, Los Alamos, New Mexico 87545*
(Received 26 April 1996)

This paper investigates properties of noisy quantum information channels. We define a quantity called *coherent information*, which measures the amount of quantum information conveyed in the noisy channel. This quantity can never be increased by quantum information processing, and it yields a simple necessary and sufficient condition for the existence of perfect quantum error correction. [S1050-2947(96)03809-7]

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

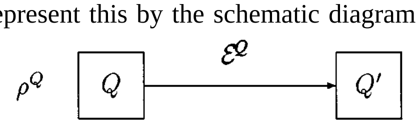
I. INTRODUCTION

This paper reports some results relating to the transmission of quantum information through noisy channels, that is, channels that are not isolated from their environments. It builds upon an earlier investigation of this situation by one of us [1]. We begin with a brief general discussion of noisy quantum processes and their mathematical descriptions.

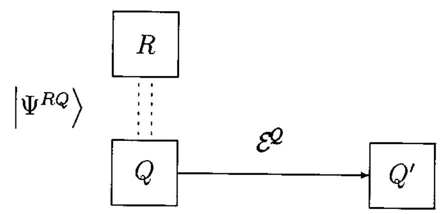
Suppose a quantum system Q is subjected to a dynamical evolution, which may represent the transmission of Q via a noisy quantum channel. In general, the evolution of Q will be represented by a *superoperator* $\mathcal{E}^Q$, which gives the mapping from initial states (represented by density operators ρ^Q) to final states

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

where we use primes to denote states after the evolution. The mapping represented by $\mathcal{E}^Q$ is linear in ρ^Q and preserves both the trace and the positivity of its arguments. The evolution of Q will be unitary only if it is isolated from other systems. We might represent this by the schematic diagram



We might imagine, however, that the system Q is part of a larger system RQ and that this compound system is initially in a pure state $|\Psi^{RQ}\rangle$. Then $\rho^Q = \mathrm{Tr}_R|\Psi^{RQ}\rangle\langle\Psi^{RQ}|$. (We say that $|\Psi^{RQ}\rangle$ is a ''purification'' of ρ^Q.) The system R is isolated and has a zero internal Hamiltonian. This situation might be represented by a slightly more complicated diagram



We will call R the ''reference'' system. Q may in fact initially be in a pure entangled state with some external system, but from our point of view R is introduced simply as a mathematical device to purify the initial state.

The overall system RQ evolves according to the ''extended'' superoperator $I^R \otimes \mathcal{E}^Q$, where I^R is the identity. That is,

$$\rho^{RQ'} = I^R \otimes \mathcal{E}^Q(\rho^{RQ}). \tag{2}$$

The extended superoperator $I^R \otimes \mathcal{E}^Q$ is also trace preserving and if it is to be a legitimate quantum evolution it had also better preserve the positivity of the density operator. This second condition is in fact a nontrivial requirement on the original superoperator $\mathcal{E}^Q$ called *complete positivity* [2]. The physical requirement that Q dynamics be extensible in this trivial way to dynamics for the compound system RQ imposes the mathematical requirement that the superoperator $\mathcal{E}^Q$ be completely positive.

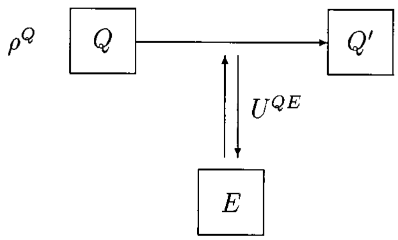
It turns out that every completely positive $\mathcal{E}^Q$ has a representation as a *unitary* evolution on a larger system [3]. That is, if $\mathcal{E}^Q$ is an allowable quantum evolution for Q (one that is extensible as indicated above), then we can introduce an ''environment'' system E, initially in a pure state, such that

$$\mathcal{E}^Q(\rho^Q) = \mathrm{Tr}_E U^{QE}(\rho^Q \otimes |0^E\rangle\langle 0^E|) U^{QE\dagger} \tag{3}$$

for a unitary operator U^{QE}. This might be represented as

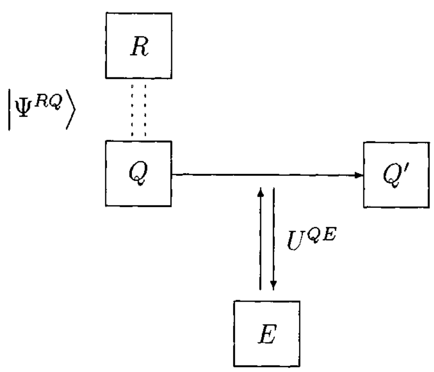
*Permanent address: Department of Physics, Kenyon College, Gambier, OH 43022.

 © 1996 The American Physical Society



The environment system E and operator U^{QE} might be chosen to be the actual physical environment and its interaction with Q, but this is not really necessary. The only thing that matters for our purposes is the dynamics of Q, and E is introduced only as a mathematical artifice. There are many choices of E, $|0^E\rangle$, and U^{QE} that will do the same job. We will call a representation of $\mathcal{E}^Q$ in terms of a unitary evolution of a larger system (with the environment E initially in a pure state) a *unitary representation* of $\mathcal{E}^Q$. Every allowable $\mathcal{E}^Q$ admits such a representation.

If we introduce both the reference system R to purify the initial state and the environment E to give a unitary representation for $\mathcal{E}^Q$, the situation looks like



The initial pure state of the joint system RQE is

$$|\Psi^{RQE}\rangle = |\Psi^{RQ}\rangle \otimes |0^E\rangle. \tag{4}$$

Since the overall evolution is unitary, the final state is also a pure state

$$|\Psi^{RQE'}\rangle = (1^R \otimes U^{QE})|\Psi^{RQE}\rangle. \tag{5}$$

The states of the various subsystems before and after the evolution may be obtained from these states by partial traces.

It is also possible to represent $\mathcal{E}^Q$ in an ''intrinsic'' way, one that does not introduce any additional quantum systems. One particularly useful representation of this sort is the *operator-sum representation*, which involves a collection of operators A_μ^Q that act in the Hilbert space $\mathcal{H}_Q$ describing Q. This is

$$\rho^{Q'} = \mathcal{E}^Q(\rho^Q) = \sum_\mu A_\mu^Q \rho^Q A_\mu^{Q\dagger}. \tag{6}$$

The operators A_μ^Q must satisfy a normalization condition

$$\sum_\mu A_\mu^{Q\dagger} A_\mu^Q = 1^Q. \tag{7}$$

If we have an operator-sum representation for $\mathcal{E}^Q$, then we can easily write down an operator-sum representation for the extended superoperator $I^R \otimes \mathcal{E}^Q$ using the operators $1^R \otimes A_\mu^Q$

The following three conditions are equivalent [3].

(i) $\mathcal{E}^Q$ is a trace-preserving, completely positive linear map on density operators of Q.
(ii) $\mathcal{E}^Q$ has a unitary representation.
(iii) $\mathcal{E}^Q$ has a normalized operator-sum representation.

For a given $\mathcal{E}^Q$, neither the unitary representation nor the operator-sum representation is unique.

II. ENTANGLEMENT FIDELITY

From now on, we will suppose that the system Q, initially in the state ρ^Q, is subjected to the evolution operator $\mathcal{E}^Q$. We may introduce a reference system R to purify the initial state to $|\Psi^{RQ}\rangle$ and we may introduce a unitary representation for $\mathcal{E}^Q$ involving an environment system E, as convenient. Nevertheless, our focus will be on quantities that are *intrinsic* to Q, depending only on ρ^Q and $\mathcal{E}^Q$.

Given a pure state $|\psi\rangle$ of a quantum system, we can define the *fidelity* F of an arbitrary (possibly mixed) state ρ of the system as

$$F = \langle\psi|\rho|\psi\rangle. \tag{8}$$

F is a measure of ''how close'' ρ is to $|\psi\rangle\langle\psi|$ and is equal to unity if and only if $\rho = |\psi\rangle\langle\psi|$. (It is possible to extend the definition of fidelity to a measure of closeness between two arbitrary density operators ρ_1 and ρ_2, but this simpler definition is sufficient for our purposes [4].)

The first important intrinsic property of Q we will define is the *entanglement fidelity* F_e. This is [1]

$$F_e = \langle\Psi^{RQ}|\rho^{RQ'}|\Psi^{RQ}\rangle = \sum_\mu (\mathrm{Tr}\rho^Q A_\mu^Q)(\mathrm{Tr}\rho^Q A_\mu^{Q\dagger}). \tag{9}$$

According to the first expression, F_e measures how faithfully the entangled state $|\Psi^{RQ}\rangle$ is preserved by the dynamics of Q. The second expression emphasizes that this is a quantity intrinsic to Q, i.e., depending only on ρ^Q and $\mathcal{E}^Q$. The exact way that ρ^Q is ''purified'' into $|\Psi^{RQ}\rangle$ is irrelevant. It is useful to explore the relation between F_e and various other fidelities that may be defined for Q.

Suppose we have an ensemble $\mathcal{E}$ of pure states, in which the ith state $|\psi_i^Q\rangle$ occurs with probability p_i. The ensemble is described by the density operator

$$\rho^Q = \sum_i p_i |\psi_i^Q\rangle\langle\psi_i^Q|. \tag{10}$$

If we subject the ith state to the dynamical superoperator $\mathcal{S}^Q$, the resulting state is $\rho_i^{Q'} = \mathcal{E}^Q(|\psi_i^Q\rangle\langle\psi_i^Q|)$. The ''input-output'' fidelity of this process is

$$F_i = \langle\psi_i^Q|\rho_i^{Q'}|\psi_i^Q\rangle. \tag{11}$$

The average fidelity $\overline{F}$ for the ensemble $\mathcal{E}$ is given by

$$\overline{F}=\sum_i p_i F_i=\sum_i p_i\langle\psi_i^Q|\rho_i^{Q'}|\psi_i^Q\rangle. \tag{12}$$

Given ρ^Q and $\mathcal{E}^Q$ we can also define the entanglement fidelity F_e. It turns out that this entanglement fidelity is never greater than the average fidelity [1]

$$F_e\leqslant\overline{F}. \tag{13}$$

Thus the entanglement fidelity is a lower bound for the average fidelity of an ensemble of pure states.

We will briefly sketch the reasons for this connection between F_e and $\overline{F}$. Given a purification $|\Psi^{RQ}\rangle$ for ρ^Q, we can always realize the ensemble $\mathcal{E}$ as an ensemble of relative states of Q given by the outcomes of the measurement of an observable on R. In other words, the entangled state of RQ allows us to create the ensemble $\mathcal{E}$ of Q states by a procedure that affects only R. This procedure commutes with the dynamics of the system Q given by $\mathcal{E}^Q$ and so could be performed after Q has undergone its dynamical evolution. This allows us to express $\overline{F}$ as the probability of a measurement outcome on the evolved state $\rho^{RQ'}$, and this condition turns out to be weaker than the condition that expresses F_e. Thus $F_e\leqslant\overline{F}$.

Now, given any state $|\phi^Q\rangle$ in the subspace that supports ρ^Q, it is always possible to find an ensemble $\mathcal{E}$ for ρ^Q in which $|\phi^Q\rangle$ is a component with nonvanishing probability. This has an interesting implication. Let

$$F=\langle\phi^Q|\mathcal{E}^Q(|\phi^Q\rangle\langle\phi^Q|)|\phi^Q\rangle \tag{14}$$

be the input-output fidelity associated with $|\phi^Q\rangle$. Then $F_e=1$ only if $F=1$ for all states $|\phi^Q\rangle$ in the support of ρ^Q. This is because we can find an ensemble for ρ^Q containing $|\phi^Q\rangle$ and the average fidelity $\overline{F}$ of that ensemble must be unity. It follows that the fidelity of every component of the ensemble is unity.

Another connection between the pure state fidelity and the entanglement fidelity is this: Let $\eta\geqslant 0$ and suppose $F\geqslant 1-\eta$ for all $|\phi^Q\rangle$ in the support of ρ^Q. Then it can be shown that [5] $F_e\geqslant 1-3\eta/2$ (a similar result was also pointed out to us by Barnum [6]). Thus we can conclude that $F_e=1$ if and only if $F=1$ for every pure state $|\psi^Q\rangle$ in the support of ρ^Q.

The entanglement fidelity F_e, which depends only on ρ^Q and $\mathcal{E}^Q$, thus has some useful relations to the other fidelities of the system Q. We might informally summarize these by saying that a high entanglement fidelity F_e implies a high ensemble average fidelity $\overline{F}$ and a high minimum fidelity on the supporting subspace of ρ^Q implies that the entanglement fidelity F_e cannot be too much lower.

III. ENTROPY EXCHANGE

The second important intrinsic quantity that we will define is the *entropy exchange* S_e [1]. Let $S(\rho)=-\mathrm{Tr}\rho\log\rho$ be the von Neumann entropy of a density operator ρ (where the logarithm is taken to be base 2). Then

$$S_e=S(\rho^{RQ'})=S(\rho^{E'})=S(W), \tag{15}$$

where W is a density operator with components (in an orthonormal basis)

$$W_{\mu\nu}=\mathrm{Tr}A_\mu^Q\rho^Q A_\nu^{Q\dagger}. \tag{16}$$

Once again, S_e has an easy interpretation in terms of the entangled state $|\Psi^{RQ}\rangle$, as the entropy of the joint system RQ after the evolution (or, equivalently, the entropy of the environment E afterward if the environment starts out in a pure state). Nevertheless, S_e is an intrinsic property of Q, depending only on ρ^Q and $\mathcal{E}^Q$.

The entropy exchange is not in general equal to the changes in entropy of either the system Q or the actual physical environment of Q. It is a measure of the information exchanged between Q and the rest of the world during the evolution $\mathcal{E}^Q$. It has several useful properties; for example, it limits the amount of information that an eavesdropper might acquire in a quantum cryptographic protocol [1].

A connection between F_e and S_e is given by the *quantum Fano inequality* [1], which states that, if the Hilbert space $\mathcal{H}_Q$ describing system Q has d complex dimensions,

$$h(F_e)+(1-F_e)\log(d^2-1)\geqslant S_e, \tag{17}$$

where $h(p)=-p\log p-(1-p)\log(1-p)$. This means, among other things, that if $F_e=1$, then $S_e=0$. (The quantum Fano inequality is analogous to the classical Fano inequality [7], which gives a roughly similar relation between the probability of error in a classical channel and an entropy term describing the noise in the channel.)

IV. COHERENT QUANTUM INFORMATION

We now define a third intrinsic quantity of interest, which we will call *coherent (quantum) information* I_e. This may be defined as

$$I_e=S(\rho^{Q'})-S(\rho^{RQ'})=S(\rho^{Q'})-S_e. \tag{18}$$

(This obviously depends only on ρ^Q and $\mathcal{E}^Q$.) I_e may be positive, negative, or zero. An analogous quantity for classical systems can never be positive since the entropy of the joint system RQ can never be less than the entropy of the subsystem Q. Thus we can think of I_e as measuring the ‘‘nonclassicity'' of the final joint state $\rho^{RQ'}$, the degree of quantum entanglement retained by R and Q. Phrased in this way, I_e is a natural measure of the degree to which quantum coherence is retained by the dynamical process $\mathcal{E}^Q$.

We will begin exploring the properties of I_e by making use of the *subadditivity* of the von Neumann entropy [8]. Consider a compound system AB composed of subsystems A and B. Then

$$S(\rho^{AB})\leqslant S(\rho^A)+S(\rho^B). \tag{19}$$

Equality holds if and only if AB is in a product state $\rho^{AB}=\rho^A\otimes\rho^B$.

A second useful fact applies if AB is in a pure state. In this case ρ^A and ρ^B have exactly the same nonzero eigenvalues (as can be easily seen from the Schmidt decomposition of $|\Phi^{AB}\rangle$) and thus $S(\rho^A)=S(\rho^B)$.

Now suppose that we have a unitary representation for $\mathcal{E}^Q$ involving an environment system E initially in a pure state. The total system RQE is thus initially in a pure state, and since it evolves according to unitary dynamics, the final state of RQE is also pure. The coherent information I_e is thus

$$\begin{aligned} I_e &= S(\rho^{Q'})-S_e \\ &= S(\rho^{RE'})-S(\rho^{E'}) \\ &\leqslant S(\rho^{R'}), \end{aligned} \tag{20}$$

where the last inequality follows by subadditivity. But R is not affected by the interaction between Q and E, so $\rho^{R'}=\rho^R$. Since RQ is initially in a pure state, we conclude that

$$S(\rho^Q)\geqslant \underbrace{S(\rho^{Q'})-S_e}_{I_e}. \tag{21}$$

The coherent information can be no greater than the initial entropy of Q, which measures the initial degree of entanglement of R and Q. [$S(\rho^Q)$ also measures the resources necessary to faithfully store this entanglement [11].] Equality holds if and only if $\rho^{RE'}=\rho^R\otimes\rho^{E'}$. This is a special case of a more general property of the coherent information I_e, which we will demonstrate in the next section.

V. QUANTUM DATA PROCESSING INEQUALITY

Suppose X, Y, and Z are classical random variables and suppose that

$$X\rightarrow Y\rightarrow Z \tag{22}$$

is a Markov process, so that Z depends only on Y and not on X directly. For example, X and Y might be the input and output of a noisy communication channel and Z might be the result of some (possibly stochastic) processing of the output. It is possible to prove a ''data processing inequality'' [7] for classical information theory, which states that

$$I(X:Z)\leqslant I(X:Y), \tag{23}$$

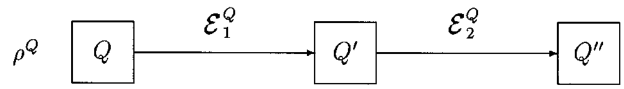
where $I(X:Z)$ is the mutual information between X and Z, etc. This means that the mutual information between the input and output of a channel cannot be increased by processing the output in any way.

We can establish a similar inequality for the coherent information I_e. Suppose the initial state of Q is ρ^Q (which has a purification $|\Psi^{RQ}\rangle$) and further suppose that Q undergoes two successive dynamical evolutions, described by superoperators $\mathcal{E}_1^Q$ and $\mathcal{E}_2^Q$. Then

$$\rho^{Q'}=\mathcal{E}_1^Q(\rho^Q), \tag{24}$$

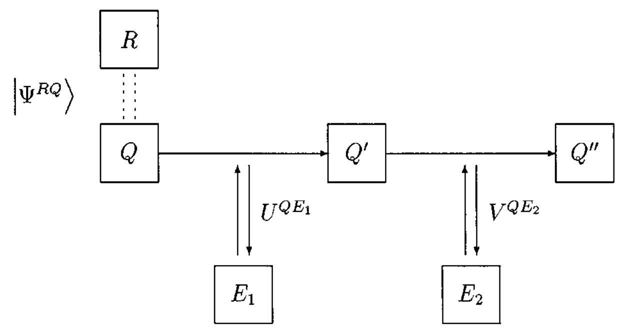
$$\begin{aligned} \rho^{Q''} &= \mathcal{S}_2^Q(\rho^{Q'}) \\ &= \mathcal{S}_2^Q\circ\mathcal{S}_1^Q(\rho^Q). \end{aligned} \tag{25}$$

We will call the evolution by $\mathcal{E}_1^Q$ the ''first stage'' of the evolution and the evolution by $\mathcal{E}_2^Q$ the ''second stage.'' These might represent, for example, the transmission of the information in Q through a noisy channel (described by $\mathcal{E}_1^Q$) followed by some quantum information processing such as error correction (described by $\mathcal{E}_2^Q$). Our schematic is



The overall process is represented by the composition of these two processes, so that $\mathcal{E}_{12}^Q=\mathcal{E}_2^Q\circ\mathcal{E}_1^Q$

We adopt adopt unitary representations for these processes. That is, we imagine that there are two environment systems E_1 and E_2, initially in pure states $|0^{E_1}\rangle$ and $|0^{E_2}\rangle$, which interact in succession with Q via unitary operators U^{QE_1} and V^{QE_2}. The full schematic diagram, including the reference system R, looks like



The initial state of the whole system is

$$|\Psi^{RQE_1E_2}\rangle=|\Psi^{RQ}\rangle\otimes|0^{E_1}\rangle\otimes|0^{E_2}\rangle. \tag{26}$$

In the first stage of the dynamics, this evolves to

$$\begin{aligned} |\Psi^{RQE_1E_2{}'}\rangle &= (1^R\otimes U^{QE_1}\otimes 1^{E_2})|\Psi^{RQE_1E_2}\rangle \\ &= |\Psi^{RQE_1{}'}\rangle\otimes|0^{E_2}\rangle. \end{aligned} \tag{27}$$

In the second stage, this evolves to

$$|\Psi^{RQE_1E_2{}''}\rangle=(1^R\otimes 1^{E_1}\otimes V^{QE_2})|\Psi^{RQE_1E_2{}'}\rangle. \tag{28}$$

The states of the subsystems can be derived by partial traces of these.

To analyze this two-stage process, we make use of a property of the von Neumann entropy called *strong subadditivity* [8]. Let ABC be a compound system composed of three subsystems A, B, and C. Then

$$S(\rho^{ABC})+S(\rho^B)\leqslant S(\rho^{AB})+S(\rho^{BC}). \tag{29}$$

This property is logically stronger than simple subadditivity; if B is supposed to be in a pure state (so that $\rho^{ABC}=\rho^{AB}\otimes|\phi^B\rangle\langle\phi^B|$), then we recover ordinary subadditivity for A and C.

We will apply this inequality to the compound system RE_1E_2 after both stages of the dynamics have taken place. This yields

$$S(\rho^{RE_1E_2''})+S(\rho^{E_1''})\leqslant S(\rho^{RE_1''})+S(\rho^{E_1E_2''}). \tag{30}$$

Each term in this inequality may be rewritten in a different form. For example, since the overall state of RQE_1E_2 is pure at every stage, it follows that

$$S(\rho^{RE_1E_2''})=S(\rho^{Q''}). \tag{31}$$

Neither of the systems R or E_1 is involved in the second stage of the dynamics, in which Q and E_2 interact. Thus their state does not change during this stage: $\rho^{RE_1''}=\rho^{RE_1'}$. After the first stage, as noted above, the compound system RQE_1 is in a pure state. Thus

$$S(\rho^{RE_1''})=S(\rho^{RE_1'})=S(\rho^{Q'}). \tag{32}$$

The remaining two terms can both be recognized as entropy exchanges of various processes. That is,

$$S(\rho^{E_1''})=S(\rho^{E_1'})=S_{e1}, \tag{33}$$

$$S(\rho^{E_1E_2''})=S_{e12}, \tag{34}$$

where S_{e1} is the entropy exchange of the first stage and S_{e12} is the overall entropy exchange of both stages. Note that, in general, $S_{e12}\neq S_{e1}+S_{e2}$. In fact, the overall entropy exchange S_{e12} can be less than either of the individual entropy exchanges S_{e1} and S_{e2}.

Making these substitutions, the strong subadditivity inequality (30) for RE_1E_2 after both stages of the dynamics yields

$$S(\rho^{Q''})+S_{e1}\leqslant S(\rho^{Q'})+S_{e12}, \tag{35}$$

$$S(\rho^{Q''})-S_{e12}\leqslant S(\rho^{Q'})-S_{e1}. \tag{36}$$

That is, $I_{e12}\leqslant I_{e1}$. The coherent information in the first stage cannot be increased by the additional dynamics of the second stage. We thus can summarize our results so far as

$$S(\rho^Q)\geqslant \underbrace{S(\rho^{Q'})-S_{e1}}_{I_{e1}}\geqslant \underbrace{S(\rho^{Q''})-S_{e12}}_{I_{e12}}. \tag{37}$$

This is the quantum data processing inequality. [The first inequality, of course, is a special case of the second, since $S(\rho^Q)$ is the coherent information in the trivial process given by $\mathcal{E}^Q=I^Q$.]

VI. ERROR CORRECTION

Suppose $\mathcal{E}_1^Q$ represents the transmission of quantum information via a noisy channel. $\mathcal{E}_1^Q$ may involve ''decoherence'' and other noise processes, which will reduce the entanglement fidelity F_{e1} of the channel. However, it has been shown that under some circumstances it is possible to do *quantum error correction* on the output of the channel, restoring the initial state of the system either exactly or very nearly by an allowable quantum process [9]. This error correction process typically consists of an incomplete measurement performed on Q followed by a unitary evolution of Q that depends on the measurement outcome. We will describe our quantum error correction scheme by the evolution superoperator $\mathcal{E}_2^Q$, so the overall process of channel dynamics plus error correction is given by $\mathcal{E}_{12}^Q=\mathcal{E}_2^Q\circ\mathcal{E}_1^Q$

The following question naturally arises: Under what circumstances can quantum error correction be performed? We will consider an interesting special case of this question: Given some channel dynamics $\mathcal{E}_1^Q$, when is it possible to find a subsequent quantum evolution $\mathcal{E}_2^Q$ that gives *perfect* error correction?

We will take perfect error correction to mean that the entanglement fidelity F_{e12} of the overall process is unity. In other words, we require that the error correction scheme be able to perfectly restore the entanglement of Q with the system R. (This is a reasonable definition since we know that the entanglement fidelity equals unity if and only if every pure state in the subspace supporting ρ^Q has fidelity unity.) If $F_e=1$ then the final (mixed) state of Q must equal the initial state: $\rho^{Q''}=\rho^Q$. From the quantum Fano inequality we can also infer that the entropy exchange S_{e12} of the overall process must be zero.

The quantum data processing inequality allows us to establish a necessary condition for the existence of a perfect error correction scheme. If $\mathcal{S}_2^Q$ is such a scheme for the initial state ρ^Q and the channel dynamics $\mathcal{S}_1^Q$, then

$$\begin{aligned} S(\rho^Q)&\geqslant S(\rho^{Q'})-S_{e1}\\ &\geqslant S(\rho^{Q''})-S_{e12}\\ &=S(\rho^Q), \end{aligned}$$

$$S(\rho^Q)=S(\rho^{Q'})-S_{e1}=I_{e1}. \tag{38}$$

Thus perfect error correction is possible only if the coherent information of the channel equals the entropy of the input state.

We will next show that $S(\rho^Q)=I_{e1}$ is also a *sufficient* condition for the existence of a perfect error correction scheme. We begin by writing down the Schmidt decomposition of the initial pure entangled state $|\Psi^{RQ}\rangle$ of the system RQ

$$|\Psi^{RQ}\rangle=\sum_k \sqrt{\lambda_k}|\alpha_k^R\rangle\otimes|\beta_k^Q\rangle, \tag{39}$$

where we take the sum to include all of the nonzero eigenvalues λ_k of ρ^Q (and thus also ρ^R). If $S(\rho^Q)=I_{e1}$, then we have already shown that $\rho^{RE_1'}=\rho^R\otimes\rho^{E_1'}$. This means that

$$\rho^{RE_1'}=\sum_{k,l}\lambda_k\mu_l|\alpha_k^R\rangle\langle\alpha_k^R|\otimes|\gamma_l^{E_1}\rangle\langle\gamma_l^{E_1}|, \tag{40}$$

where the μ_l are the nonzero eigenvalues of $\rho^{E_1'}$ and $|\gamma_l^{E_1}\rangle$ are the corresponding eigenstates.

The overall state of RQE_1 is a pure state $|\Psi^{RQE_1'}\rangle$. We can use our expression for $\rho^{RE_1'}$ to write down a Schmidt decomposition of this overall state (separating into subsystems Q and RE_1):

$$|\Psi^{RQE_1'}\rangle=\sum_{k,l}\sqrt{\lambda_k\mu_l}|\alpha_k^R\rangle\otimes|\phi_{kl}^Q\rangle\otimes|\gamma_l^{E_1}\rangle. \tag{41}$$

(This yields a sort of "triple Schmidt decomposition" because the eigenstates of $\rho^{RQ'}$ are product states.) Here the Q states $|\phi_{kl}^Q\rangle$ are orthonormal and span a subspace of $\mathcal{H}_Q$. Let Π^Q be the projection onto the subspace perpendicular to this one, so that

$$\Pi^Q+\sum_{k,l}|\phi_{kl}^Q\rangle\langle\phi_{kl}^Q|=1^Q. \tag{42}$$

We will now explicitly construct an operator-sum representation for the error correction process $\mathcal{E}_2^Q$ and show that it is a perfect error-correction scheme. Let

$$A_0^Q=\Pi^Q, \tag{43}$$

$$A_l^Q=\sum_k|\beta_k^Q\rangle\langle\phi_{kl}^Q|. \tag{44}$$

Intuitively, for each l the operator A_l^Q represents a projection onto the subspace spanned by the vectors $|\phi_{kl}^Q\rangle$ (for all values of k), followed by a unitary transformation that takes $|\phi_{kl}^Q\rangle$ to $|\beta_k^Q\rangle$. It is easy to see that

$$A_0^Q|\phi_{kl}^Q\rangle=0, \tag{45}$$

$$A_l^Q|\phi_{kl'}^Q\rangle=\delta_{ll'}|\beta_k^Q\rangle. \tag{46}$$

To yield an allowable dynamical evolution of Q, these must be properly normalized. That is,

$$\begin{aligned}A_0^{Q\dagger}A_0^Q+\sum_l A_l^{Q\dagger}A_l^Q&=\Pi^Q+\sum_l\sum_{k,k'}|\phi_{kl}^Q\rangle\langle\beta_k^Q|\beta_{k'}^Q\rangle\langle\phi_{k'l}^Q|\\&=\Pi^Q+\sum_{k,l}|\phi_{kl}^Q\rangle\langle\phi_{kl}^Q|=1^Q.\end{aligned} \tag{47}$$

Thus the operators A_0^Q and A_l^Q yield an operator-sum representation of an allowed quantum evolution superoperator $\mathcal{E}_2^Q$.

To see that $\mathcal{E}_2^Q$ specifies a perfect error-correction scheme, consider the effect on $|\Psi^{RQE_1'}\rangle$ of the extended superoperator $I^R\otimes\mathcal{E}^Q\otimes I^{E_1}$. The operator-sum representation of $I^R\otimes\mathcal{E}^Q\otimes I^{E_1}$ is composed of operators of the form $1^R\otimes A_l^Q\otimes 1^{E_1}$,

$$\begin{aligned}1^R\otimes A_0^Q\otimes 1^{E_1}|\Psi^{RQE_1'}\rangle&=\sum_{k,l}\sqrt{\lambda_k\mu_l}|\alpha_k^R\rangle\otimes(A_0^Q|\phi_{kl}^Q\rangle)\otimes|\gamma_l^{E_1}\rangle\\&=0,\end{aligned} \tag{48}$$

$$\begin{aligned}1^R\otimes A_l^Q\otimes 1^{E_1}|\Psi^{RQE_1'}\rangle&=\sum_{k,l'}\sqrt{\lambda_k\mu_{l'}}|\alpha_k^R\rangle\otimes(A_l^Q|\phi_{kl'}^Q\rangle)\\&\quad\otimes|\gamma_{l'}^{E_1}\rangle\\&=\sum_k\sqrt{\lambda_k\mu_l}|\alpha_k^R\rangle\otimes|\beta_k^Q\rangle\otimes|\gamma_l^{E_1}\rangle\\&=\sqrt{\mu_l}\left(\sum_k\sqrt{\lambda_k}|\alpha_k^R\rangle\otimes|\beta_k^Q\rangle\right)\otimes|\gamma_l^{E_1}\rangle\\&=\sqrt{\mu_l}|\Psi^{RQ}\rangle\otimes|\gamma_l^{E_1}\rangle.\end{aligned} \tag{49}$$

Therefore,

$$\begin{aligned}\rho^{RQE_1''}&=I^R\otimes\mathcal{E}_2^Q\otimes I^{E_1}(|\Psi^{RQE_1'}\rangle\langle\Psi^{RQE_1'}|)\\&=(1^R\otimes A_0^Q\otimes 1^{E_1})|\Psi^{RQE_1'}\rangle\langle\Psi^{RQE_1'}|(1^R\otimes A_0^Q\otimes 1^{E_1})^\dagger\\&\quad+\sum_l(1^R\otimes A_l^Q\otimes 1^{E_1})|\Psi^{RQE_1'}\rangle\langle\Psi^{RQE_1'}|\\&\quad\times(1^R\otimes A_l^Q\otimes 1^{E_1})^\dagger\\&=\sum_l\mu_l|\Psi^{RQ}\rangle\langle\Psi^{RQ}|\otimes|\gamma_l^{E_1}\rangle\langle\gamma_l^{E_1}|\\&=|\Psi^{RQ}\rangle\langle\Psi^{RQ}|\otimes\rho^{E_1'}.\end{aligned} \tag{50}$$

The final state of RQ is $\rho^{RQ''}=\mathrm{Tr}_{E_1}\rho^{RQE_1''}=|\Psi^{RQ}\rangle\langle\Psi^{RQ}|$, which is exactly the original entangled state. Therefore the entanglement fidelity of the entire process is $F_{e12}=1$. Our superoperator $\mathcal{S}^Q$ thus gives a perfect error correction scheme. Once again we emphasize that, although we made use of the particular input state ρ^Q (with purification $|\Psi^{RQ}\rangle$) to construct our perfect error-correction scheme, this is equivalent to perfect error correction for all pure states in the support of ρ^Q or indeed for any other entangled state with the same support in $\mathcal{H}_Q$.

We may compare our result to a classical theorem [7]. Suppose the random variables X and Y represent the inputs and outputs of a classical information channel. Then the input may be reconstructed from the output with zero probability of error if and only if $H(X)=I(X:Y)$, where $H(X)$ is the Shannon entropy of the input variable.

VII. REMARKS

The condition $S(\rho^Q)=I_e$, which is necessary and sufficient for perfect quantum error correction, has some interesting implications, which we will briefly mention here. Suppose that the state ρ^Q is due to an ensemble $\mathcal{E}$ in which the pure state $|\psi_i^Q\rangle$ appears with probability p_i. As we remarked before, we can realize such an ensemble by starting with a purification $|\Psi^{RQ}\rangle$ and performing a measurement of a suitable R observable. The ith outcome of this measurement will appear with probability p_i and the relative state of Q given that measurement will be $|\psi_i^Q\rangle$. The question "Which Q state?" is then equivalent to the question "Which R measurement outcome?"

As we showed, the equality $S(\rho^Q)=I_e$ means that

$\rho^{RE'}=\rho^R\otimes\rho^{E'}$. If R and E are in a product state after the dynamical evolution, then measurement results on E have no statistical correlation with measurement results on R. In other words, no observable on E alone will be able to provide any information about the outcome of a measurement performed on R. Therefore, no E observable can provide any information about which Q state from the ensemble $\mathcal{E}$ is present. In short, perfect quantum error correction is possible only if the environment obtains no information about the state of the system Q.

We summarize our main points and conclusions here.

(i) For a given initial state ρ^Q and dynamical superoperator $\mathcal{S}^Q$, we may define several intrinsic quantities of interest, including the entanglement fidelity F_e, the entropy exchange S_e, and the coherent information I_e. F_e and S_e are related by a quantum version of the Fano inequality of classical information theory.

(ii) The entanglement fidelity is closely related to various input-output fidelities for pure states of Q.

(iii) The coherent information is a measure of the amount of ''distinctively quantum'' information that passes through a channel. In general, $S(\rho^Q)\geqslant I_e$.

(iv) The coherent information can never be increased by the action of further dynamics, so that for successive independent processes (1) and (2) we obtain the quantum data processing inequality, $I_{e1}\geqslant I_{e12}$.

(v) Perfect quantum error correction is possible if and only if $S(\rho^Q)=I_e$, in which case the environment has obtained no information about the state of Q via its interaction with Q.

In general, we believe that the coherent information I_e will play a role in quantum information theory analogous to that played by the mutual information $I(X:Y)$ in the classical theory. There are many differences between the two. For one thing, the coherent information has a built-in ''time asymmetry,'' being defined for an input state ρ^Q and a process $\mathcal{E}^Q$, while the mutual information $I(X:Y)$ is a symmetric quantity built out of a joint probability distribution for X and Y in which time does not explicitly appear. For another, $I_e=S(\rho^{Q'})-S(\rho^{RQ'})$ is a quantity that can never be positive classically, so that no classical channel can convey a positive amount of coherent quantum information.

Recent work by Lloyd [10] indicates that I_e is related to the capacity of a noisy quantum channel in a way that parallels the relation of the mutual information to the classical capacity. That is, he defines the capacity C to be

$$C=\max_{\rho^Q} I_e . \tag{51}$$

According to Lloyd, quantum information can be transmitted through a noisy channel at any rate less than C with arbitrarily good fidelity. This is very much in accord with our own results and speculations.

The paper continues the program of finding useful ''intrinsic'' quantities by ''extrinsic'' means, introducing a reference system R to purify the initial state and an environment E to make the overall dynamics unitary. This approach appears to yield many important insights into quantum information theory.

ACKNOWLEDGMENTS

The authors wish to acknowledge the help of many people during the course of this work, including H. Barnum, C. H. Bennett, C. M. Caves, C. A. Fuchs, E. H. Knill, R. Laflamme, A. Peres, J. Smolin, M. D. Westmoreland, and W. H. Zurek. This work was supported in part by the Office of Naval Research (Grant No. N00014-93-1-0116). M.N. would like to thank the Australian-American Education Foundation (Fulbright Commission) for financial support.

[1] B. Schumacher, preceding paper, Phys. Rev. A **54**, 2614 (1996).

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

[3] 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).

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

[5] E. Knill and R. Laflamme (unpublished).

[6] H. Barnum (private communication).

[7] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).

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

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

[10] S. Lloyd (unpublished).

[11] R. Jozsa and B. Schumacher, J. Mod. Opt. **41**, 2343 (1994); B. Schumacher, Phys. Rev. A **51**, 2738 (1995).