Commun. Math. Phys. 246, 453–472 (2004)
Digital Object Identifier (DOI) 10.1007/s00220-003-0981-7

Communications in
Mathematical
Physics

Equivalence of Additivity Questions in Quantum Information Theory

Peter W. Shor*

AT&T Labs Research, Florham Park, NJ 07922, USA

Received: 8 May 2003 / Accepted: 17 July 2003
Published online: 18 November 2003 –

Abstract: We reduce the number of open additivity problems in quantum information theory by showing that four of them are equivalent. Namely, we show that the conjectures of additivity of the minimum output entropy of a quantum channel, additivity of the Holevo expression for the classical capacity of a quantum channel, additivity of the entanglement of formation, and strong superadditivity of the entanglement of formation, are either all true or all false.

1. Introduction

The study of quantum information theory has led to a number of seemingly related open questions that center around whether certain quantities are additive. We show that four of these questions are equivalent. In particular, we show that the four conjectures of

i. additivity of the minimum entropy output of a quantum channel,
ii. additivity of the Holevo capacity of a quantum channel,
iii. additivity of the entanglement of formation,
iv. strong superadditivity of the entanglement of formation,

are either all true or all false.

Two of the basic ingredients in our proofs are already known. The first is an observation of Matsumoto, Shimono and Winter [12] that the Stinespring dilation theorem relates a constrained version of the Holevo capacity formula to the entanglement of formation. The second is the realization that the entanglement of formation (or the constrained Holevo capacity) is a linear programming problem, and so there is also a dual linear formulation. This formulation was first presented by Audenaert and Braunstein [1], who expressed it in the language of convexity rather than that of linear programming. We noted this independently [16]. These two ingredients are explained in Sect. 3 and 5.

* *Current address*: Dept. of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

The rest of this paper is organized as follows. Sect. 2 gives some background in quantum information theory, describes the additivity questions we consider, and gives brief histories of them. Sect. 3 and 5 explain the two ingredients we describe above, and are positioned immediately before the first sections in which they are used. To show that the conditions (i) to (iv) are equivalent, in Sect. 4 we prove that (ii) $\rightarrow$ (iii): additivity of the Holevo capacity implies additivity of entanglement of formation. In Sect. 6 we prove (iii) $\rightarrow$ (iv): additivity of entanglement of formation implies strong superadditivity of entanglement of formation. This implication was independently discovered by Pomeransky [13]. In Sect. 7 we prove that (i) $\rightarrow$ (iii): additivity of minimum entropy output implies additivity of entanglement of formation. In Sect. 8, we give simple proofs showing that (iv) $\rightarrow$ (i), (iv) $\rightarrow$ (ii), and (iv) $\rightarrow$ (iii). The first implication is the only one that was not in the literature, and we assume this is mainly because nobody had tried to prove it. The second of these implications was already known, but for completeness we give a proof. The third of these implications is trivial.[1] In Sect. 9 we give proofs that (ii) $\rightarrow$ (i) and (iii) $\rightarrow$ (i): either additivity of the Holevo capacity or of the entanglement of formation implies additivity of the minimum entropy output. These implications complete the proof of equivalence. Strictly speaking, the only implications we need for the proof of equivalence are those in Sect. 6–9. We include the proof in Sect. 4 because it uses one of the techniques used later for Sect. 7 without introducing the extra complexity of the dual linear programming formulation. Finally, in Sect. 10 we comment on the implications of the results in our paper and give some open problems.

2. Background and Results

One of the important intellectual breakthroughs of the 20$^{\text{th}}$ century was the discovery and development of information theory. A cornerstone of this field is Shannon's proof that a communication channel has a well-defined information carrying capacity and his formula for calculating it. For communication channels that intrinsically incorporate quantum effects, this classical theory is no longer valid. The search for the proof of the analogous quantum formulae is a subarea of quantum information theory that has recently received much study.

In the generalization of Shannon theory to the quantum realm, the definition of a stochastic communication channel generalizes to a completely positive trace-preserving linear map (CPT map). We call such a map a *quantum channel*. In this paper, we consider only finite-dimensional CPT maps; these take $d_{\text{in}} \times d_{\text{in}}$ Hermitian matrices to $d_{\text{out}} \times d_{\text{out}}$ Hermitian matrices. In particular, these maps take density matrices (trace 1 positive semidefinite matrices) to density matrices. Note that the input dimension can be different from the output dimension, and that these dimensions are both finite. Infinite dimensional quantum channels (CPT maps) are both important and interesting, but dealing with them also introduces extra complications that are beyond the scope of this paper.

There are several characterizations of CPT maps. We need the characterization given by the Stinespring dilation theorem, which says that every CPT map can be described by an unitary embedding followed by a partial trace. In particular, given a finite-dimensional CPT map N, we can express it as

$$N(\rho) = \text{Tr}_B U(\rho),$$

[1] In fact, property (iv), strong superadditivity of E_F, seems to be in some sense the "strongest" of these equivalent statements, as it is fairly easy to show that strong superadditivity of entanglement of formation implies the other three additivity results whereas the reverse directions appear to require substantial work. Similarly, property (i) appears to be the "weakest" of these statements.

where $U(\rho)$ is a unitary embedding, i.e., there is some ancillary space $\mathcal{H}_B$ such that U takes $\mathcal{H}_{\text{in}}$ to $\mathcal{H}_{\text{out}} \otimes \mathcal{H}_B$ by

$$U(\rho) = V\rho V^\dagger$$

and V is a unitary matrix mapping $\mathcal{H}_{\text{in}}$ to range$(V) \subseteq \mathcal{H}_{\text{out}} \otimes \mathcal{H}_B$. We also need the operator sum characterization of CPT maps. This characterization says that any finite-dimensional CPT map N can be represented as

$$N(\rho) = \sum_k A_k \rho A_k^\dagger,$$

where the A_k are complex matrices satisfying

$$\sum A_k^\dagger A_k = I.$$

The Holevo information[2] χ is a quantity which is associated with a probabilistic ensemble of quantum states (density matrices). If density matrix ρ_i occurs in the ensemble with probability q_i, the Holevo information χ of the ensemble is

$$\chi = H\left(\sum_i q_i \rho_i\right) - \sum_i q_i H(\rho_i),$$

where H is the von Neumann entropy $H(\rho) = -\text{Tr}\,\rho \log \rho$. This quantity was introduced in [6, 11, 8] as a bound for the amount of information extractable by measurements from this ensemble of quantum states. The first published proof of this bound was given by Holevo [8]. It was much later shown that maximizing the Holevo capacity over all probabilistic ensembles of a set of quantum states gives the information transmission capacity of this set of quantum states; more specifically, this is the amount of classical information which can be transmitted asymptotically per quantum state by using codewords that are tensor products of these quantum states, as the length of these codewords goes to infinity [9, 15]. Optimizing χ over ensembles composed of states that are potential outputs of a quantum channel gives the quantum capacity of this quantum channel over a restricted set of protocols, namely those protocols which are not allowed to send inputs entangled between different channel uses. If the channel is N, we call this quantity χ_N; it is defined as

$$\chi_N = \max_{\{p_i, |\,v_i\rangle\}} H\left(N\left(\sum_i p_i |v_i\rangle\langle v_i|\right)\right) - \sum_i p_i H(N(|v_i\rangle\langle v_i|)), \tag{1}$$

where the maximization is over ensembles $\{p_i, |\,v_i\rangle\}$, where $\sum_i p_i = 1$ and $|\,v_i\rangle \in \mathcal{H}_{\text{in}}$, the input space of the channel N.

The regularized Holevo capacity is

$$\lim_{n\to\infty} \frac{1}{n} \chi_{N^{\otimes n}};$$

this gives the capacity of a quantum channel to transmit classical information when inputs entangled between different channel uses are allowed. The question of whether

[2] This has also been called the Holevo bound and the Holevo χ-quantity.

the quantum capacity is given by the single-symbol Holevo capacity χ_N is the question of whether the capacity χ_N is additive; that is, whether

$$\chi_{N_1 \otimes N_2} = \chi_{N_1} + \chi_{N_2}.$$

The $\geq$ relation is easy; the open question is the $\leq$ relation.

The question of additivity of the minimum entropy output of a quantum channel was originally considered independently by several people, including the author, and appears to have been first considered in print in [10]. It was originally posed as a possible first step to proving additivity of the Holevo capacity χ_N. The question is whether

$$\min_{|\phi\rangle} H(N_1 \otimes N_2(|\phi\rangle\langle\phi|)) = \min_{|\phi\rangle} H(N_1(|\phi\rangle\langle\phi|)) + \min_{|\phi\rangle} H(N_2(|\phi\rangle\langle\phi|)),$$

where the minimization ranges over states $|\phi\rangle$ in the input space of the channel. Note that by the concavity of the von Neumann entropy, if we minimize over mixed states ρ – i.e., $\min_\rho H(N(\rho))$ – there will always be a rank one $\rho = |\phi\rangle\langle\phi|$ achieving the minimum.

The statements (iii) and (iv) in our equivalence theorem both deal with entanglement. This is one of the stranger phenomena of quantum mechanics. Entanglement occurs when two (or more) quantum systems are non-classically correlated. The canonical example of this phenomenon is an EPR pair. This is the state of two quantum systems (called qubits, as they are each two-dimensional):

$$\frac{1}{\sqrt{2}}\big(|\,01\rangle - |\,10\rangle\big).$$

Measurements on each of these two qubits separately can exhibit correlations which cannot be modeled by two separated classical systems [2].

A topic in quantum information theory that has recently attracted much study is that of quantifying entanglement. The entanglement of a bipartite pure state is easy to define and compute; this is the entropy of the partial trace over one of the two parts

$$E_{\text{pure}}(|v\rangle\langle v|) = H(\text{Tr}_B |v\rangle\langle v|).$$

Asymptotically, two parties sharing n copies of a bipartite pure state $|v\rangle\langle v|$ can use local quantum operations and classical communication (called *LOCC operations*) to produce $nE_{\text{pure}}(|v\rangle\langle v|) - o(n)$ nearly perfect EPR pairs, and can similarly form n nearly perfect copies of $|v\rangle\langle v|$ from $nE_{\text{pure}}(|v\rangle\langle v|) + o(n)$ EPR pairs [4]. This implies that for a pure state $|v\rangle\langle v|$, the entropy of the partial trace is the natural quantitative measure of the amount of entanglement contained in $|v\rangle\langle v|$.

For mixed states (density matrices of rank > 1), things become more complicated. The amount of pure state entanglement asymptotically extractable from a state using LOCC operations (the *distillable entanglement*) is now no longer necessarily equal to the amount of pure state entanglement asymptotically required to create a state using LOCC operations (the *entanglement cost*) [17]. In general, the entanglement cost must be at least the distillable entanglement, as LOCC operations cannot increase the amount of entanglement.

The *entanglement of formation* was introduced in [5]. Suppose we have a bipartite state σ on a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. The entanglement of formation is

$$E_F(\sigma) = \min_{\{p_i, |\,v_i\rangle\}} \sum_i p_i H(\text{Tr}_B |v_i\rangle\langle v_i|), \tag{2}$$

where the minimization is over all ensembles such that $\sum_i p_i |v_i\rangle\langle v_i| = \sigma$ with probabilities p_i satisfying $\sum_i p_i = 1$. The entanglement of formation must be at least the entanglement cost, as the decomposition of the state σ yielding $E_F(\sigma)$ can be used to create a prescription for asymptotically constructing $\sigma^{\otimes n}$ from $nE_F(\sigma) + o(n)$ EPR pairs. The regularized entanglement of formation

$$\lim_{n\to\infty} \frac{1}{n} E_F(\sigma^{\otimes n})$$

has been proven to give the entanglement cost of a quantum state [7]. As in the case of channel capacity, a proof of additivity, i.e., that

$$E_F(\sigma_1 \otimes \sigma_2) = E_F(\sigma_1) + E_F(\sigma_2),$$

would imply that regularization is not necessary.

The question of strong superadditivity of entanglement of formation has been previously considered in [3, 17, 12, 1]. This conjecture says that for all states σ over a quadripartite system $\mathcal{H}_{A1} \otimes \mathcal{H}_{A2} \otimes \mathcal{H}_{B1} \otimes \mathcal{H}_{B2}$, we have

$$E_F(\sigma) \geq E_F(\mathrm{Tr}_2\sigma) + E_F(\mathrm{Tr}_1\sigma),$$

where the entanglement of formation E_F is taken over the bipartite A-B division, as in (2). This question was originally considered in relation to the question of additivity of E_F. The strong superadditivity of entanglement of formation is known to imply both the additivity of entanglement of formation (trivially) and the additivity of Holevo capacity of a channel [12]. A proof similar to ours that additivity of E_F implies strong superadditivity of E_F was discovered independently; it appears in [13].

We can now state the main result of our paper.

Theorem 1. *The following are equivalent.*

i. The additivity of the minimum entropy output of a quantum channel. Suppose we have two quantum channels (CPT maps) N_1 (taking $\mathbb{C}^{d_{1,\mathrm{in}}\times d_{1,\mathrm{in}}}$ to $\mathbb{C}^{d_{1,\mathrm{out}}\times d_{1,\mathrm{out}}}$) and N_2 (taking $\mathbb{C}^{d_{2,\mathrm{in}}\times d_{2,\mathrm{in}}}$ to $\mathbb{C}^{d_{2,\mathrm{out}}\times d_{2,\mathrm{out}}}$). Then

$$\min_{|\phi\rangle} H((N_1 \otimes N_2)(|\phi\rangle\langle\phi|)) = \min_{|\phi\rangle} H(N_1(|\phi\rangle\langle\phi|)) + \min_{|\phi\rangle} H(N_2(|\phi\rangle\langle\phi|)),$$

where H is the von Neumann entropy and the minimization is taken over all vectors $|\phi\rangle$ in the input space of the channels.

ii. The additivity of the Holevo capacity of a quantum channel. Assume we have two quantum channels N_1 and N_2, as in (i). Then

$$\chi_{N_1\otimes N_2} = \chi_{N_1} + \chi_{N_2},$$

where χ is defined as in Eq. (1).

iii. Additivity of the entanglement of formation. Suppose we have two quantum states $\sigma_1 \in \mathcal{H}_{A1} \otimes \mathcal{H}_{B1}$ and $\sigma_2 \in \mathcal{H}_{A2} \otimes \mathcal{H}_{B2}$. Then

$$E_F(\sigma_1 \otimes \sigma_2) = E_F(\sigma_1) + E_F(\sigma_2),$$

where E_F is defined as in Eq. (2). In particular, the entanglement of formation is calculated over the bipartite A–B partition.

iv. The strong superadditivity of the entanglement of formation. Suppose we have a density matrix σ over a quadripartite system $\mathcal{H}_{A1} \otimes \mathcal{H}_{A2} \otimes \mathcal{H}_{B1} \otimes \mathcal{H}_{B2}$. Then

$$E_F(\sigma) \geq E_F(\mathrm{Tr}_2\sigma) + E_F(\mathrm{Tr}_1\sigma),$$

where the entanglement of formation is calculated over the bipartite A–B partition. Here, the operator Tr_1 traces out the space $\mathcal{H}_{A1} \otimes \mathcal{H}_{B1}$, and Tr_2 traces out the space $\mathcal{H}_{A2} \otimes \mathcal{H}_{B2}$.

3. The Correspondence of Matsumoto, Shimono and Winter

Recall the definition of the Holevo capacity for a channel N:

$$\chi_N = \max_{\{p_i, |\phi_i\rangle\}} H(N(\sum_i p_i |\phi_i\rangle\langle\phi_i|)) - \sum_i p_i H(N(|\phi_i\rangle\langle\phi_i|)).$$

Recall also the definition of entanglement of formation. For a bipartite state σ on $\mathcal{H}_A \otimes \mathcal{H}_B$, the entanglement of formation is

$$E_F(\sigma) = \min_{\substack{\{p_i, |v_i\rangle\} \\ \sum p_i |v_i\rangle\langle v_i| = \sigma}} \sum_i p_i H(\mathrm{Tr}_B |v_i\rangle\langle v_i|).$$

Let us define a constrained version of the Holevo capacity, which is just the Holevo capacity over ensembles whose average input is ρ,

$$\chi_N(\rho) = \max_{\substack{\{p_i, |\phi_i\rangle\} \\ \sum_i p_i |\phi_i\rangle\langle\phi_i| = \rho}} H(N(\sum_i p_i |\phi_i\rangle\langle\phi_i|)) - \sum_i p_i H(N(|\phi_i\rangle\langle\phi_i|)). \tag{3}$$

The paper of Matsumoto, Shimono and Winter [12] gives a connection between this constrained version of the Holevo capacity and the entanglement of formation, which we now explain. The Stinespring dilation theorem says that any quantum channel can be realized as a unitary transformation followed by a partial trace. Suppose we have a channel N taking $\mathcal{H}_{\mathrm{in}}$ to $\mathcal{H}_A$. We can find a unitary embedding $U(\rho) = V\rho V^\dagger$ that takes $\mathcal{H}_{\mathrm{in}}$ to $\mathcal{H}_A \otimes \mathcal{H}_B$ such that

$$N(\mu) = \mathrm{Tr}_B U(\mu)$$

for all density matrices $\mu \in \mathcal{H}_{\mathrm{in}}$. Now, U maps an ensemble of input states $\{p_i, |\phi_i\rangle\}$ with $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$ to an ensemble of states $\{p_i, |v_i\rangle = V|\phi_i\rangle\}$ on the bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ such that $\sum_i p_i |v_i\rangle\langle v_i| = \sigma = U(\rho)$.

Conversely, if we are given a bipartite state $\sigma \in \mathcal{H}_A \otimes \mathcal{H}_B$, we can find an input space $\mathcal{H}_{\mathrm{in}}$ with $\dim \mathcal{H}_{\mathrm{in}} = \mathrm{rank}\,\sigma$, a density matrix $\rho \in \mathcal{H}_{\mathrm{in}}$, and a unitary embedding $U : \mathcal{H}_{\mathrm{in}} \to \mathcal{H}_{\mathrm{out}}$ such that $U(\rho) = \sigma$. We can then define N by

$$N(\mu) = \mathrm{Tr}_B U(\mu),$$

establishing the same relation between N, U, ρ and σ. Note that since we chose $\dim \mathcal{H}_{\mathrm{in}} = \mathrm{rank}\,\sigma = \mathrm{rank}\,\rho$, ρ has full rank in $\mathcal{H}_{\mathrm{in}}$.

Since $N(|\phi_i\rangle\langle\phi_i|) = \mathrm{Tr}_B |v_i\rangle\langle v_i|$, we have

$$\chi_N(\rho) = H(N(\rho)) - E_F(\sigma).$$

Now, suppose $E_F(\sigma)$ is additive. I claim that $\chi_N(\rho)$ is as well, and vice versa. Let us take $N_1(\rho) = \mathrm{Tr}_B U_1(\rho)$ and $N_2(\rho) = \mathrm{Tr}_B U_2(\rho)$. If $U_1(\rho_1) = \sigma_1$ and $U_2(\rho_2) = \sigma_2$, then we have

$$\begin{aligned}\chi_{N_1\otimes N_2}(\rho_1 \otimes \rho_2) &= H(N_1 \otimes N_2(\rho_1 \otimes \rho_2)) - E_F(\sigma_1 \otimes \sigma_2) \\ &= H(N_1(\rho_1)) + H(N_2(\rho_2)) - E_F(\sigma_1 \otimes \sigma_2).\end{aligned}$$

The first term on the right-hand side is additive, so the entanglement of formation E_F is additive if and only if the constrained capacity $\chi_N(\rho)$ is.

4. Additivity of χ Implies Additivity of E_F

Recall the definition of the Holevo capacity for a channel N:

$$\chi_N = \max_{\{p_i, |\phi_i\rangle\}} H\left(N\left(\sum_i p_i |\phi_i\rangle\langle\phi_i|\right)\right) - \sum_i p_i H(N(|\phi_i\rangle\langle\phi_i|)),$$

where the maximization is over ensembles $\{p_i, |\phi_i\rangle\}$ with $\sum_i p_i = 1$. Recall also our definition of a constrained version of the Holevo capacity, which is just the definition of the Holevo capacity with the maximization only over ensembles whose average input is ρ,

$$\chi_N(\rho) = \max_{\substack{\{p_i, |\phi_i\rangle\} \\ \sum_i p_i |\phi_i\rangle\langle\phi_i| = \rho}} H\left(N\left(\sum_i p_i |\phi_i\rangle\langle\phi_i|\right)\right) - \sum_i p_i H(N(|\phi_i\rangle\langle\phi_i|)).$$

Let σ be the state whose entanglement of formation we are trying to compute. The MSW correspondence yields a channel N and an input state ρ so that

$$N(\rho) = \mathrm{Tr}_B \sigma$$

and

$$\chi_N(\rho) = H(N(\rho)) - E_F(\sigma).$$

This is very nearly the channel capacity, the only difference being that the ρ above is not necessarily the ρ that maximizes χ_N. Only one element is missing for the proof that additivity of channel capacity implies additivity of entanglement of formation: namely making sure that the average density matrix for the ensemble giving the optimum channel capacity is equal to a desired matrix ρ_0. This cannot be done directly [14], but we solve the problem indirectly.

We now give the intuition for our proof. Suppose we could define a new channel N' which, instead of having capacity

$$\chi_N = \max_\rho \chi_N(\rho),$$

has capacity

$$\chi_{N'} = \max_\rho \chi_N(\rho) + \mathrm{Tr}\,\rho\tau \tag{4}$$

for some fixed Hermitian matrix τ. For a proper choice of τ, this will ensure that the maximum of this channel occurs at the desired ρ. Consider two entangled states σ_1 and σ_2 which we wish to show are additive. We can find the associated channels N_1' and N_2',

with the capacity maximized when the average input density matrix is ρ_1 and ρ_2, respectively. By our hypothesis of additivity of channel capacity, the tensor product channel $N_1' \otimes N_2'$ has capacity equal to the sum of the capacities of N_1' and N_2'. If we can now analyze the capacity of the channel $N_1' \otimes N_2'$ carefully, we might be able to show that the entanglement of formation of $E_F(\sigma_1 \otimes \sigma_2)$ is indeed the sum of $E_F(\sigma_1)$ and $E_F(\sigma_2)$. We do not know how to define such a channel N' satisfying (4). What we actually do is find a channel whose capacity is close to (4), or more precisely a sequence of channels approximating (4) in the asymptotic limit. It turns out that this will be adequate to prove the desired theorem.

We now give the definition of our new channel N'. It takes as its input, the input to the channel N, along with k additional classical bits (formally, this is actually a 2^k-dimensional Hilbert space on which the first action of the channel is to measure it in the canonical basis). With probability q the channel N' sends the first part of its input through the channel N and discards the classical bits; with probability $1-q$ the channel N makes a measurement on the first part of the input, and uses the results of this measurement to decide whether or not to send the auxiliary classical bits. When the auxiliary classical bits are not sent, an erasure symbol is sent to the receiver instead. When the auxiliary classical bits are sent, they are labeled, so the receiver knows whether he is receiving the output of the original channel or the auxiliary bits.

What is the capacity of this new channel N'? Let $\mathbf{E}$ be the element of the POVM measurement in the case that we send the auxiliary bits (so $I - \mathbf{E}$ is the element of the POVM in the case that we do not send these bits). Now, we claim that for some set of vectors $|v_i\rangle$ and some associated set of probabilities p_i, the optimum signal states of this new channel N' will be $|v_i\rangle\langle v_i| \otimes |b\rangle\langle b|$ with associated probabilities $p_i/2^k$, where b ranges over all values of the classical bits.[3]

We now can find bounds on the capacity of N'. Let $|v_i\rangle$ and p_i be the optimal signal states and probabilities for $\chi_{N'}(\rho)$. We compute

$$\begin{aligned}\chi_{N'}(\rho) = q\left(H\left(N\left(\sum_i p_i |v_i\rangle\langle v_i|\right)\right) - \sum_i p_i H(N(|v_i\rangle\langle v_i|))\right)\\ +(1-q)k\sum_i p_i \operatorname{Tr}\mathbf{E}|v_i\rangle\langle v_i|\\ +(1-q)\left(H_2\left(\operatorname{Tr}\mathbf{E}\sum_i p_i|v_i\rangle\langle v_i|\right) - \sum_i p_i H_2(\operatorname{Tr}\mathbf{E}|v_i\rangle\langle v_i|)\right), \quad (5)\end{aligned}$$

where H_2 is the binary entropy function $H_2(x) = -x\log x - (1-x)\log(1-x)$. The first term is the information associated with the channel N, the second is that associated with the auxiliary classical bits, and the third is the information associated with the measurement $\mathbf{E}$.

Let $\rho = \sum_i p_i |v_i\rangle\langle v_i|$ and let σ be the associated entangled state. We can now deduce from (5) that

$$\chi_{N'}(\rho) = q\chi_N(\rho) + (1-q)k\operatorname{Tr}\mathbf{E}\rho + (1-q)\delta, \quad (6)$$

[3] This just says that we want to use the classical part of the channel as efficiently as possible. The formal proof is straightforward: First, we show that it doesn't help to send superpositions of the auxiliary bits, so we can assume that the signal states are indeed of the form $|v_i\rangle\langle v_i| \otimes |b\rangle\langle b|$. Next, we show that if two signals $|v_i\rangle\langle v_i| \otimes |b_1\rangle\langle b_1|$ and $|v_i\rangle\langle v_i| \otimes |b_2\rangle\langle b_2|$ do not have the same probabilities associated with them, a greater capacity can be achieved by making these probabilities equal.

where δ is defined as

$$\delta = H_2(\mathrm{Tr}\,\mathbf{E}\rho) - \sum_i p_i H_2(\langle v_i \mid \mathbf{E} \mid v_i \rangle).$$

Note that $0 \leq \delta \leq 1$, since δ is positive by the concavity of the entropy function H_2, and is at most 1 since $H_2(p) \leq 1$ for $0 \leq p \leq 1$. Similarly, if we use the optimal states for $\chi_N(\rho)$, we find that

$$\chi_{N'}(\rho) \geq \chi_N(\rho) + (1-q)k\mathrm{Tr}\,\mathbf{E}\rho. \tag{7}$$

From Eq. (6) and (7), if we find the ρ_0 that maximizes the quantity

$$q\chi_N(\rho) + (1-q)k\mathrm{Tr}\,\mathbf{E}\rho; \tag{8}$$

we are guaranteed to be within $1-q$ of the capacity of N'.

We next show that we can find a measurement $\mathbf{E}$ such that an arbitrary density matrix ρ_0 is a maximum of (8).

Lemma 2. *For any probability $0 < q < 1$, any channel N, and any fixed positive matrix ρ_0 over the input space of N, there is a sufficiently large k_0 such that for $k \geq k_0$ we can find an $\mathbf{E}$ so that the maximum of (8) occurs at ρ_0. (This maximum need not be unique. If $\chi_N(\rho)$ is not strictly concave at ρ_0, then ρ_0 will be just one of several points attaining the maximum.)*

Proof. It follows from the concavity of von Neumann entropy that $\chi_N(\rho)$ is concave in ρ. The intuition is that we must choose $\mathbf{E}$ so that the derivative [4] of (8) with respect to ρ at ρ_0 is 0. Because we only vary over matrices with $\mathrm{Tr}\,\rho = 1$, we can add any multiple of I to $\mathbf{E}$ and not change the derivative. Suppose that in the neighborhood of ρ_0,

$$\chi_N(\rho) \leq \chi_N(\rho_0) + \mathrm{Tr}\,\tau(\rho - \rho_0). \tag{9}$$

That such an expression exists follows from the concavity of $\chi_N(\rho)$ and the assumption that ρ_0 is not on the boundary of the state space, i.e., has no zero eigenvalues. A full rank ρ_0 is guaranteed by the MSW correspondence.

To make ρ_0 a maximum for Eq. (8), we see from Eq. (9) that we need to find $\mathbf{E}$ so that

$$\frac{(1-q)}{q}k\mathbf{E} = \lambda I - \tau$$

with $0 \leq \mathbf{E} \leq I$. This can be done by choosing k and λ appropriately. □

Now, suppose we have two entangled states σ_1 and σ_2 for which we want to show that the entanglement of formation is additive. We create the channels N_1' and N_2' as detailed above. By the additivity of channel capacity (which we're assuming), the signal states of the tensor product channel can be taken to be $|v_i^{(1)}\rangle|b_1\rangle \otimes |v_j^{(2)}\rangle|b_2\rangle$ for b_1, b_2 any k-bit strings, with probability $p_i^{(1)}p_j^{(2)}/2^{2k}$. This gives a bound on the channel capacity of at most

$$\begin{aligned}\chi_{N_1'\otimes N_2'} \leq\ & q\,(H(N_1(\rho_1)) - E_F(\sigma_1)) + (1-q)k\mathrm{Tr}\,\mathbf{E}_1\rho_1 \\ & + q\,(H(N_2(\rho_2)) - E_F(\sigma_2)) + (1-q)k\mathrm{Tr}\,\mathbf{E}_2\rho_2 + 2(1-q).\end{aligned} \tag{10}$$

[4] This is the intuition. This derivative need not actually exist.

The $2(1-q)$ term at the end comes from the fact that the formula (8) is within $1-q$ of the capacity. Now, we want to show that we can find a larger capacity than this if there is a better decomposition of $\sigma_1 \otimes \sigma_2$, i.e., if the entanglement of formation of $\sigma_1 \otimes \sigma_2$ is not additive. The central idea here is to let q go to 1; this forces k to simultaneously go to ∞. There is a contribution from entangled states, which goes as q^2, a contribution from the auxiliary k-bit classical channel, which goes as $(1-q)k$, but which is equal in both cases, and a contribution from unentangled states, which goes as $q(1-q)$. As q goes to 1, the contribution from the entangled states dominates the difference.

Suppose there is a set of entangled states which gives a smaller entanglement of formation for $\sigma_1 \otimes \sigma_2$ than $E_F\sigma_1 + E_F\sigma_2$. By the MSW correspondence, this gives a set of signal states for the map $N_1 \otimes N_2$ which yields a larger constrained capacity than $\chi_{N_1}(\rho_1) + \chi_{N_2}(\rho_2)$. We define this set of signal states for $N_1 \otimes N_2$ to be the states $|\phi_i\rangle\langle\phi_i|$, and let the associated probabilities be π_i. Now, using the $|\phi_i\rangle$ as signal states in $N_1' \otimes N_2'$ shows that

$$\chi_{N_1' \otimes N_2'} \geq q^2 H(N_1 \otimes N_2(\rho_1 \otimes \rho_2)) - q^2 E_F(\sigma_1 \otimes \sigma_2) + (1-q)k\mathrm{Tr}\,\mathbf{E}_2\rho_2.$$

This estimate comes from considering the information transmitted by the signal states $|\phi_i\rangle\langle\phi_i|$ in the case (occurring with probability q^2) when the channels operate as $N_1 \otimes N_2$, as well as the information transmitted by the k classical bits.

We now consider the difference between this lower bound (11) for the capacity of $N_1' \otimes N_2'$ and the upper bound (10) we showed for the capacity using tensor product signal states. In this difference, the terms containing $(1-q)k$ cancel out. The remaining terms give

$$\begin{aligned} 0 \geq\ & qE_F(\sigma_1) + qE_F(\sigma_2) - q^2E_F(\sigma_1 \otimes \sigma_2) - 2(1-q) \\ & -q(1-q)H(N_1(\rho_1)) - q(1-q)H(N_2(\rho_2)). \end{aligned}$$

For q sufficiently close to 1, the $(1-q)$ terms can be made arbitrarily small, and q and q^2 are both arbitrarily close to 1. This difference can thus be made positive if the entanglement of formation is strictly subadditive, contradicting our assumption that the Holevo channel capacity is additive.

5. The Linear Programming Formulation

We now give the linear programming dual formulation for the constrained capacity problem. Recall the definition of the constrained Holevo capacity

$$\chi_N(\rho) = \max_{\substack{\{p_i, |\phi_i\rangle\} \\ \sum_i p_i|\phi_i\rangle\langle\phi_i| = \rho}} H\left(N\left(\sum_i p_i|\phi_i\rangle\langle\phi_i|\right)\right) - \sum_i p_i H(N(|\phi_i\rangle\langle\phi_i|)). \tag{11}$$

This is a linear program, and as such it has a formulation of a dual problem that also gives the maximum value. This dual problem is crucial to several of our proofs. For this paper, we only deal with channels having finite dimensional input and output spaces. For infinite dimensional channels, the duality theorem fails unless the maxima are replaced by suprema. We have not analyzed the effects this has on the proof of our equivalence theorem, but even if it still holds the proofs will become more complicated.

By the duality theorem for linear programming there is another expression for $E_F(\sigma_1)$. This was observed in [1, 16]. It is

$$\chi_N(\rho) = H(N(\rho)) - f(\rho), \tag{12}$$

where f is the linear function defined by the maximization

$$\max_f f(\rho) \text{ such that } f(|v\rangle\langle v|) \leq H(N(|v\rangle\langle v|)) \quad \text{for all } |v\rangle \in \mathcal{H}_{\text{in}}. \tag{13}$$

Here $\mathcal{H}_{\text{in}}$ is the input space for N and the maximum is taken over all linear functions

$$f(\rho) = \operatorname{Tr} \tau\rho.$$

Equations (12) and (13) can be proved if ρ is full rank by using the duality theorem of linear programming. The duality theorem applies directly if there are only a finite number of possible signal states allowed, showing the equality of the modified version of Eqs. (11) and (12) where the constraints in (13) are limited to a finite number of possible signal states $|v_i\rangle$, which are also the only signal states allowed in the capacity calculation (11). To extend from all finite collections of signal states $|v_i\rangle\langle v_i|$ to all $|v\rangle\langle v|$, we need to show that we can find a compact set of linear functions $f(\rho) = \operatorname{Tr} \tau\rho$ which suffice to satisfy Eq. (13). We can then use compactness to show that a limit of these functions exists, where in the limit Eqs. (11) and (13) must hold on a countable set of possible signal states $|v_i\rangle$ dense in the set of unit vectors, thus showing that they hold on the set of all unit vectors $|v\rangle$. The compactness follows from ρ being full rank, and $H(N(|v\rangle\langle v|)) \leq \log d_{\text{out}}$ for all $|v\rangle\langle v|$, where d_{out} is the dimension of the output space of N. The case where ρ is not full rank can be proved by using the observation that the only values of the function f which are relevant in this case are those in the support of ρ.

Equality must hold in (13) for those $|v\rangle$ which are signal states in an optimal decomposition. This can be seen by considering the inequalities

$$\begin{aligned}
\chi_N(\rho) &= H(N(\rho)) - \sum_i p_i H(N(|v_i\rangle\langle v_i|)) \\
&\leq H(N(\rho)) - \sum_i p_i f(|v_i\rangle\langle v_i|) \\
&= H(N(\rho)) - f(\rho).
\end{aligned}$$

For equality to hold, it must hold in all the terms in the summation, which are exactly the signal states $|v_i\rangle$.

6. Additivity of E_F Implies Strong Superadditivity of E_F

In this section, we will show that additivity of entanglement of formation implies strong superadditivity of entanglement of formation. Another proof was discovered independently by Pomeransky [13]; it is quite similar, although it is expressed using different terminology.

We first give the statement of strong superadditivity. Assume we have a quadripartite density matrix σ whose four parts are $A1$, $A2$, $B1$ and $B2$. The statement of strong superadditivity is that

$$E_F(\sigma) \geq E_F(\operatorname{Tr}_2\sigma) + E_F(\operatorname{Tr}_1\sigma), \tag{14}$$

where E_F is the entanglement of formation when the state is considered as a bipartite state where the two parts are A and B; that is,

$$E_F(\sigma) = \min_{\substack{\{p_i, |\phi_i\rangle\} \\ \sum_i p_i |\phi_i\rangle\langle\phi_i| = \sigma}} \sum_i p_i H(\operatorname{Tr}_B |\phi_i\rangle\langle\phi_i|). \tag{15}$$

First, we show that it is sufficient to prove this when σ is a pure state. Consider the optimal decomposition of $\sigma = \sum_i \pi_i |\phi_i\rangle\langle\phi_i|$. We can apply the theorem of strong subadditivity to the pure states $|\phi_i\rangle\langle\phi_i|$ to obtain decompositions $\mathrm{Tr}_1|\phi_i\rangle\langle\phi_i| = \sum_j p_{i,j}^{(1)} |v_{i,j}^{(1)}\rangle\langle v_{i,j}^{(1)}|$ and $\mathrm{Tr}_2|\phi_i\rangle\langle\phi_i| = \sum_j p_{i,j}^{(2)} |v_{i,j}^{(2)}\rangle\langle v_{i,j}^{(2)}|$ so that

$$H(\mathrm{Tr}_B|\phi_i\rangle\langle\phi_i|) \geq \sum_j p_{i,j}^{(1)} H(\mathrm{Tr}_B|v_{i,j}^{(1)}\rangle\langle v_{i,j}^{(1)}|) + \sum_j p_{i,j}^{(2)} H(\mathrm{Tr}_B|v_{i,j}^{(2)}\rangle\langle v_{i,j}^{(2)}|).$$

Summing these inequalities over i gives the desired inequality.

We now show that additivity of E_F implies strong superadditivity of E_F. Let $|\phi\rangle$ be a quadripartite pure state for which we wish to show strong superadditivity. We define $\sigma_1 = \mathrm{Tr}_2|\phi\rangle\langle\phi|$ and $\sigma_2 = \mathrm{Tr}_1|\phi\rangle\langle\phi|$. Now, let us use the MSW correspondence to find channels N_1 and N_2 and density matrices ρ_1 and ρ_2 such that

$$N_1(\rho_1) = \mathrm{Tr}_B\sigma_1 \quad \text{and} \quad N_2(\rho_2) = \mathrm{Tr}_B\sigma_2$$

and

$$\chi_{N_1}(\rho_1) = H(N_1(\rho_1)) - E_F(\sigma_1),$$
$$\chi_{N_2}(\rho_2) = H(N_2(\rho_2)) - E_F(\sigma_2).$$

We first do an easy case which illustrates how the proof works without introducing additional complexities. Let d_1 and d_2 be the dimensions of the input spaces of N_1 and N_2. In the easy case, we assume that there are d_1^2 linearly independent signal states in an optimal decomposition of ρ_1 for $\chi_{N_1}(\rho_1)$, and d_2^2 linearly independent signal states in an optimal decomposition of ρ_2 for $\chi_{N_2}(\rho_2)$. Let these sets of signal states be $|v_i^{(1)}\rangle\langle v_i^{(1)}|$ with probabilities $p_i^{(1)}$, and $|v_j^{(2)}\rangle\langle v_j^{(2)}|$ with probabilities $p_j^{(2)}$, respectively. It now follows from our assumption of the additivity of entanglement of formation that an optimal ensemble of signal states for $\chi_{N_1\otimes N_2}(\rho_1\otimes\rho_2)$ is $|v_i^{(1)}\rangle\otimes|v_j^{(2)}\rangle$ with probability $p_i^{(1)}p_j^{(2)}$.

Now, let us consider the dual linear function f_T for the tensor product channel $N_1 \otimes N_2$. Since we assumed that entanglement of formation is additive, by the MSW correspondence $\chi_N(\rho)$ is also additive. We claim that the dual function f_T must satisfy

$$f_T(|v_i^{(1)}\rangle\langle v_i^{(1)}| \otimes |v_j^{(2)}\rangle\langle v_j^{(2)}|) = H(N_1(|v_i^{(1)}\rangle\langle v_i^{(1)}|)) + H(N_2(|v_j^{(2)}\rangle\langle v_j^{(2)}|)) \qquad (16)$$

for all signal states $|v_i^{(1)}\rangle|v_j^{(2)}\rangle$. This is simply because equality must hold in the inequality (13) for all signal states. However, we now have that f_T is a linear function in a $d_1^2d_2^2 - 1$ dimensional space which has been specified on $d_1^2d_2^2$ linearly independent points; this implies that the linear function f_T is uniquely defined. It is easy to see that it thus must be the case that

$$f_T(\rho) = f_1(\mathrm{Tr}_2\rho) + f_2(\mathrm{Tr}_1\rho), \qquad (17)$$

as this holds for the $d_1^2d_2^2$ signal states We now let $|\psi\rangle\langle\psi|$ be the preimage of $\mathrm{Tr}_B|\phi\rangle\langle\phi|$ under the channel $N_1 \otimes N_2$. We have, from. Eq. (13) and (17), that

$$f_1(\mathrm{Tr}_2|\psi\rangle\langle\psi|) + f_2(\mathrm{Tr}_1|\psi\rangle\langle\psi|) \leq H(N_1 \otimes N_2(|\psi\rangle\langle\psi|)). \qquad (18)$$

But recall that

$$f_1(\mathrm{Tr}_2|\psi\rangle\langle\psi|) = E_F(\sigma_1),$$
$$f_2(\mathrm{Tr}_1|\psi\rangle\langle\psi|) = E_F(\sigma_2), \tag{19}$$

because (13) holds with equality for signal states, and that

$$N_1 \otimes N_2(|\psi\rangle\langle\psi|) = \mathrm{Tr}_B|\phi\rangle\langle\phi|.$$

Thus, substituting into (18), we find that

$$E_F(\sigma_1) + E_F(\sigma_2) \leq H(\mathrm{Tr}_B|\phi\rangle\langle\phi|),$$

which is the statement for the strong superadditivity of entanglement of formation of the pure state $|\phi\rangle\langle\phi|$.

We now consider the case where there are fewer than d_i^2 signal states for $\chi_{N_i}(\rho_i)$, $i = 1, 2$. We still know that the average density matrices of the signal states for N_1 and N_2 are ρ_1 and ρ_2, and that the support of these two matrices are the entire input spaces $\mathcal{H}_{1,\mathrm{in}}$ and $\mathcal{H}_{2,\mathrm{in}}$. The argument will go as before if we can again show that the dual function f_T must be $f_1(\mathrm{Tr}_2\rho) + f_2(\mathrm{Tr}_1\rho)$. In this case we do not know $d_1^2 d_2^2$ points of the function f_T, and thus cannot use the same argument as above to show that f_T is determined. However, there is more information that we have available. Namely, we know that in the neighborhood of the signal states $|v_i^{(1)}\rangle$, the entropy $H(N_1(|v\rangle\langle v|))$ must be at least the dual function $f_1 = \mathrm{Tr}\,\tau_1|v\rangle\langle v|$, and that these two functions are equal at the signal states. If we assume that the derivative of $H(N_1(|v\rangle\langle v|))$ exists at $|v_i^{(1)}\rangle\langle v_i^{(1)}|$, then we can conclude that this is also the derivative of $f_1 = \mathrm{Tr}\,\tau_1|v\rangle\langle v|$. For the time being we will assume that the first derivative of this entropy function does in fact exist.[5]

We need a lemma.

Lemma 3. *Suppose that we have a set of unit vectors $|v_i\rangle$ that span a Hilbert space $\mathcal{H}$. If we are given the value of f at all the vectors $|v_i\rangle$ as well as the value of the first derivative of f,*

$$\lim_{\epsilon\to 0}\frac{1}{\epsilon}\Big(f(|v_i\rangle\langle v_i|) - f\big((\sqrt{(1-\epsilon^2}\,|v_i\rangle + \epsilon\,|w_i\rangle)(\sqrt{1-\epsilon^2}\,\langle v_i| + \epsilon\,\langle w_i|)\big)\Big)$$

at all the vectors $|v_i\rangle$ and for all orthogonal $|w\rangle$, then f is completely determined.

Proof. Let us use the representation $f(\rho) = \mathrm{Tr}\,\tau\rho$ (we do not need a constant term on the right-hand side because we need only specify f on trace 1 matrices). Suppose that $\langle v_i|w\rangle = 0$. We compute the derivative at $|v_i\rangle$ in the $|w\rangle$ direction:

$$\Big(\sqrt{1-\epsilon^2}\langle v_i| + \epsilon\langle w|\Big)\ \tau\ \Big(\sqrt{1-\epsilon^2}|v_i\rangle + \epsilon|w\rangle\Big) - \langle v_i|\tau|v_i\rangle$$
$$\approx \epsilon\left(\langle v_i|\tau|w\rangle + \langle w|\tau|v_i\rangle\right). \tag{20}$$

The derivative in the $i|w\rangle$ direction gives

$$i\left(\langle v_i|\tau|w\rangle - \langle w|\tau|v_i\rangle\right), \tag{21}$$

[5] In fact, I believe the function is smooth enough that these derivatives do exist. However, we find it easier to deal with the cases where $N_1(|v\rangle\langle v|)$ has zero eigenvalues by expressing N_1 and N_2 as a limit of nonsingular completely positive maps.

so a linear combination of (20) and (21) shows that the value of $\langle v_i \mid \tau \mid w\rangle$ is determined for all $\mid w\rangle$ orthogonal to $\mid v_i\rangle$. We also know the value of

$$\langle v_i \mid \tau \mid v_i\rangle;$$

it follows that the value of

$$\langle v_i \mid \tau \mid w\rangle$$

is determined for all $\mid w\rangle$. Since the $\langle v_i \mid$ span the vector space, this determines the value of

$$\langle u \mid \tau \mid w\rangle$$

for all $\langle u \mid$ and all $\mid w\rangle$, thus determining the matrix τ. □

We now need to compute the derivative of the entropy of N_1. Let

$$N_1(\rho) = \sum_i A_i \rho A_i^\dagger$$

with $\sum_i A_i^\dagger A_i = I$. Then if $\operatorname{Tr}\sigma = 0$,

$$\begin{aligned} H(N_1(\rho + \epsilon\sigma)) - H(N_1(\rho)) &\approx -\epsilon \operatorname{Tr}\left[(I + \log(N(\rho))N_1(\sigma)\right] \\ &= -\epsilon \operatorname{Tr}\left(\sigma \sum_k A_k^\dagger \big(\log N_1(\rho)\big) A_k\right). \end{aligned} \tag{22}$$

Now, if the entanglement of formation is additive, then the derivative of $H(N_1 \otimes N_2)$ at the tensor product signal states $|v_i^{(1)}\rangle\langle v_i^{(1)}| \otimes |v_j^{(2)}\rangle\langle v_j^{(2)}|$ must also match the derivative of the function f_T at these points. We calculate:

$$\begin{aligned} &H(N_1 \otimes N_2(\rho + \epsilon\sigma)) - H(N_1 \otimes N_2(\rho)) \\ &\quad \approx -\epsilon \operatorname{Tr}\left(\sigma \sum_{k_1,k_2} (A_{k_1}^{(1)\dagger} \otimes A_{k_2}^{(2)\dagger})(\log(N_1 \otimes N_2(\rho)))(A_{k_1}^{(1)} \otimes A_{k_2}^{(2)})\right). \end{aligned}$$

Now at a point $\rho = \rho_1 \otimes \rho_2$,

$$\begin{aligned} &\sum_{k_1,k_2} (A_{k_1}^{(1)\dagger} \otimes A_{k_2}^{(2)\dagger})(\log N_1 \otimes N_2(\rho))(A_{k_1}^{(1)} \otimes A_{k_2}^{(2)}) \\ &\quad = \left(\sum_{k_1} A_{k_1}^{(1)\dagger} \log N_1(\rho_1) A_{k_1}^{(1)}\right) \otimes I + I \otimes \left(\sum_{k_2} (A_{k_2}^{(2)\dagger} \log N_2(\rho_2) A_{k_2}^{(2)}\right), \end{aligned}$$

showing that at the states $\mid v_i^{(1)}\rangle \otimes \mid v_j^{(2)}\rangle$, we have not only that $f_T = f_1 + f_2$, but that the first derivatives (for directions σ with $\operatorname{Tr}\sigma = 0$) are equal as well. Since the states $\mid v_i^{(1)}\rangle \otimes \mid v_j^{(2)}\rangle$ span the vector space, Lemma 3 shows that $f_T = f_1 + f_2$ everywhere, giving us the last element of the proof.

The one thing remaining to do to show that the assumption that the first derivative of entropy exists everywhere is unnecessary. It suffices to show that there are dual functions $f_T = f_1 + f_2$ such that Eq. (18) holds. We do this by taking limits. For $x = 1, 2$ let $N_x^{(q)}$ be the quantum channel

$$N_x^{(q)}(\rho) = N_x(\rho) + (1-q)\frac{1}{d_{\text{out},x}} I$$

which averages the map N_x with the maximally mixed state $I/d_{\text{out},x}$. Let $N_T^{(q)} = N_1^{(q)} \otimes N_2^{(q)}$. We need to show that some limits of the dual functions $f_1^{(q)}$, $f_2^{(q)}$ and $f_T^{(q)}$ exist. By continuity of $N_x^{(q)}$, they will be forced to have the desired properties (17), (18), and (19). Let $\rho_T = \rho_1 \otimes \rho_2$. Now, $f_T^{(q)}$ is a linear function with $f_T^{(q)}(\rho_T) \geq 0$ and $f_T^{(q)}(\rho) \leq \log d_{\text{out},T}$ for all ρ, so the $f_T^{(q)}$ lie in a compact set. Thus, some subsequence of $f_T^{(q)}$ has a limit as $q \to 1$. The same argument applies to $f_1^{(q)}$ and $f_2^{(q)}$, so by taking these limits we find that the functions $f_x^{(1)}$ have the desired properties, completing our proof.

7. Additivity of min $H(N)$ Implies Additivity of E_F

Suppose that we have two bipartite states for which we wish to prove that the entanglement of formation is additive. We use the MSW correspondence to convert this problem to a question about the Holevo capacity with a constrained average signal state. We thus now have two quantum channels N_1 and N_2, and two states ρ_1 and ρ_2. We want to show that

$$\chi_{N_1 \otimes N_2}(\rho_1 \otimes \rho_2) = \chi_{N_1}(\rho_1) + \chi_{N_2}(\rho_2).$$

In fact, we need only prove the $\leq$ direction of the inequality, as the $\geq$ direction is easy.

Let $|v_i^{(1)}\rangle$ and $|v_i^{(2)}\rangle$ be optimal sets of signal states for $\chi_{N_1}(\rho_1)$ and $\chi_{N_2}(\rho_2)$, so that

$$\chi_{N_1}(\rho_1) = H(N_1(\rho_1)) - \sum_i p_i^{(1)} N(|v_i^{(1)}\rangle\langle v_i^{(1)}|),$$

where $\rho_1 = \sum_i p_i^{(1)} |v_i^{(1)}\rangle\langle v_i^{(1)}|$, and similarly for N_2. By the linear programming dual formulation in Sect. 5, we have that there is a matrix τ_1 such that

$$\chi_{N_1}(\rho_1) = H(N_1(\rho_1)) - \operatorname{Tr} \tau_1 \rho_1$$

and

$$\operatorname{Tr} \tau_1 \rho \leq H(N_1(\rho)$$

for all ρ, with equality for signal states $\rho = |v_i^{(1)}\rangle\langle v_i^{(1)}|$, and similarly for τ_2 and N_2. Suppose we could find a channel N_1' and N_2' such that

$$H(N_1'(|v\rangle\langle v|)) = H(N_1(|v\rangle\langle v|)) + C_1 - \langle v \mid \tau \mid v \rangle \tag{23}$$

for all vectors $|v\rangle$ (similarly for N_2). We know from the linear programming duality theorem that

$$\begin{aligned} H(N_1'(\rho)) &= H(N_1(\rho)) + C_1 - \operatorname{Tr}\tau_1\rho \\ &\geq C_1 \end{aligned}$$

for all input states ρ, with equality holding for the signal states $\rho = |v_i^{(1)}\rangle\langle v_i^{(1)}|$. Thus, the minimum entropy output of N_1' is C_1 and of N_2' is C_2. Also,

$$\begin{aligned} \chi_{N_1'}(\rho_1) &= H(N_1'(\rho_1))) - \sum_i p_i^{(1)} H(N_1'(|v_i^{(1)}\rangle\langle v_i^{(1)}|)) \\ &= H(N_1'(\rho_1))) - C_1, \end{aligned}$$

and similarly for N_2'. Now, if we assume the additivity of minimum entropy, we know that the minimum entropy output of $N_1' \otimes N_2'$ has entropy $C_1 + C_2$. We have for some probability distribution π_i on signal states $|\phi_i\rangle$, that

$$\begin{aligned} \chi_{N_1'\otimes N_2'}(\rho_1 \otimes \rho_2) &= H(N_1' \otimes N_2'(\rho_1 \otimes \rho_2)) - \sum_i \pi_i H(N_1' \otimes N_2'(|\phi_i\rangle\langle\phi_i|)) \\ &\leq H(N_1'(\rho_1)) + H(N_2'(\rho_2)) - C_1 - C_2 \\ &= \chi_{N_1'}(\rho_1) + \chi_{N_2'}(\rho_2). \end{aligned}$$

Now, if we can examine the construction of the channels N_1' and N_2' and show that the additivity of the constrained Holevo capacity for N_1' and N_2' implies the additivity of the constrained Holevo capacity for N_1 and N_2, we will be done.

We will not be able to achieve Eq. (23) exactly, but will be able to achieve this approximately, in much the same way we defined N' in Sect. 4.

Given a channel N, we define a new channel N'. On input ρ, with probability q the channel N' outputs $N(\rho)$. With probability $1-q$ the channel makes a POVM measurement with elements $\mathbf{E}$ and $I - \mathbf{E}$. If the measurement outcome is $\mathbf{E}$, N' outputs the tensor product of a pure state signifying that the result was $\mathbf{E}$ and the maximally mixed state on k qubits. If the result is $I - \mathbf{E}$ the channel N' outputs only a pure state signifying this fact. We have

$$H(N'(\rho)) = qH(N(\rho)) + H_2(q) + (1-q)k\operatorname{Tr}\mathbf{E}\rho + (1-q)H_2(\operatorname{Tr}\mathbf{E}\rho).$$

If we choose k and $\mathbf{E}$ such that

$$\frac{(1-q)}{q}k\mathbf{E} = \lambda I - \tau,$$

we will have

$$H(N'(|v\rangle\langle v|)) = qH(N(|v\rangle\langle v|)) - q\,\langle v \mid \tau \mid v\rangle + q\lambda + H_2(q) + (1-q)H_2(\langle v \mid \mathbf{E} \mid v\rangle).$$

The minimum entropy $H(N'(|v\rangle\langle v|))$ is thus at least $q\lambda + H_2(q)$. For signal states $|v_i\rangle$ of N, $H(N'(|v_i\rangle\langle v_i|))$ is at least $q\lambda + H_2(q)$ and at most $q\lambda + H_2(q) + 1 - q$. As q goes to 0, this is approximately a constant. We thus see that

$$H(N_1'(\rho_1)) - q\lambda_1 - H_2(q) - (1-q) \leq \chi_{N_1'}(\rho_1)$$

$$\leq H(N_1'(\rho_1)) - q\lambda_1 - H_2(q). \tag{24}$$

Now, given two channels N_1 and N_2, we can prepare N_1' and N_2' as above. If we assume the additivity of minimum entropy, this implies the constrained channel capacity satisfies, for the optimal input ensembles $|\phi_i\rangle, \pi_i$,

$$\begin{aligned}\chi_{N_1'\otimes N_2'}(\rho_1\otimes\rho_2) &= H(N_1'(\rho_1)) + H(N_2'(\rho_2)) - \sum_i \pi_i H(N_1'\otimes N_2'(|\phi_i\rangle\langle\phi_i|))\\ &\leq H(N_1'(\rho_1)) + H(N_2'(\rho_2)) - q\lambda_1 - q\lambda_2 - 2H_2(q)\\ &\leq \chi_{N_1'}(\rho_1) + \chi_{N_2'}(\rho_2) + 2(1-q),\end{aligned}$$

where the first inequality follows from the assumption of additivity of the minimum entropy output, and the second from Eq. (24).

We now need to relate $\chi_{N_1'}(\rho_1)$ and $\chi_{N_1}(\rho_1)$. Suppose we have an ensemble of signal states $|v_i\rangle\langle v_i|$ with associated probabilities p_i, and such that $\sum_i p_i|v_i\rangle\langle v_i| = \rho$. Define C_{N_1} ($C_{N_1'}$) to be the information transmitted by channel N_1 (N_1') using these signal states. We then have

$$C_{N_1'} = qC_{N_1} + (1-q)\delta_1,$$

where

$$\delta_1 = H_2(\mathrm{Tr}\,\mathbf{E}\rho) - \sum_i p_i H_2(\langle v_i\,|\,\mathbf{E}\,|\,v_i\rangle).$$

This shows that

$$q\chi_{N_1}(\rho_1) \leq \chi_{N_1'}(\rho_1) \leq q\chi_{N_1}(\rho_1) + (1-q).$$

Also, by using the optimal set of signal states for $\chi_{N_1\otimes N_2}(\rho_1\otimes\rho_2)$ as signal states for the channel $N_1'\otimes N_2'$, we find that

$$\chi_{N_1'\otimes N_2'}(\rho_1\otimes\rho_2) \geq q^2\chi_{N_1\otimes N_2}(\rho_1\otimes\rho_2),$$

since with probability q^2, the channel $N_1'\otimes N_2'$ simulates $N_1\otimes N_2$. Thus, we have that

$$\begin{aligned}\chi_{N_1\otimes N_2}(\rho_1\otimes\rho_2) &\leq q^{-2}\chi_{N_1'\otimes N_2'}(\rho_1\otimes\rho_2)\\ &\leq q^{-2}(\chi_{N_1'}(\rho_1) + \chi_{N_2'}(\rho_2)) + 2(1-q)q^{-2}\\ &\leq q^{-1}(\chi_{N_1}(\rho_1) + \chi_{N_2}(\rho_2)) + 4(1-q)q^{-2}\end{aligned}$$

holds for all q, $0 < q < 1$. Letting q go to 1, we have subadditivity of the constrained Holevo capacity, implying additivity of the entanglement of formation.

8. Implications of Strong Superadditivity of E_F

All three additivity properties (i) to (iii) follow easily from the assumption of strong superadditivity of E_F. The additivity of E_F follows trivially from this assumption. That the additivity of χ_N follows is known [12]. We repeat this argument below for completeness. Recall the definition of χ_N:

$$\chi_N = \max_{\{p_i, |\phi_i\rangle\}} H\left(N\left(\sum_i p_i |\phi_i\rangle\langle\phi_i|\right)\right) - \sum_i p_i H(N(|\phi_i\rangle\langle\phi_i|)). \tag{25}$$

Suppose that this maximum is attained at an ensemble $p_i, |\phi_i\rangle$ that is not a tensor product distribution. If we replace this ensemble with the product of the marginal ensembles, the concavity of von Neumann entropy implies that the first term increases, and the superadditivity of entanglement of formation implies that the second term decreases, showing that we can do at least as well by using a tensor product distribution, and that χ_N is thus additive.

Finally, the proof that strong superadditivity of E_F implies additivity of minimum output entropy is equally easy, although I am not aware of its being in the literature. Suppose that we have a minimum entropy output $\chi_{N_1\otimes N_2}(|\phi\rangle\langle\phi|)$. The strong superadditivity of E_F implies that there are ensembles $p_i^{(1)}, |v_i^{(1)}\rangle$ and $p_i^{(2)}, |v_i^{(2)}\rangle$ such that

$$H(N_1 \otimes N_2(|\phi\rangle\langle\phi|)) \geq \sum_i p_i^{(1)} H(N_1(|v_i^{(1)}\rangle\langle v_i^{(1)}|)) + \sum_i p_i^{(2)} H(N_2(|v_i^{(2)}\rangle\langle v_i^{(2)}|)).$$

But the two sums on the right-hand side are averages, so there must be one quantum state in each of these sums which has smaller output entropy than the average output entropy; this shows additivity of the minimum entropy output.

9. Additivity of χ_N or of E_F Implies Additivity of min $H(N)$

Suppose we have two channels N_1 and N_2 which map their input onto d-dimensional output spaces. We can assume that the two output dimensions are the same by embedding the smaller dimensional output space into a larger dimensional one.[6] We will define two new channels N_1' and N_2'. The channel N_1' will take as input the tensor product of the input space of channel N_1 and an integer between 0 and d^2-1. Now, let $X_0 \ldots X_{d^2-1}$ be the d-dimensional generalization of the Pauli matrices: $X_{da+b} = T^a R^b$, where T takes $|j\rangle$ to $|j+1 (\mathrm{mod}\ d)\rangle$ and R takes $|j\rangle$ to $e^{2\pi i j/d}|j\rangle$. Let

$$N_1'(\rho \otimes |i\rangle\langle i|) = X_i N_1(\rho) X_i^\dagger.$$

Now, suppose that $|v_1\rangle\langle v_1|$ is the input giving the minimal entropy output $N_1(|v_1\rangle\langle v_1|)$. We claim that a good ensemble of signal states for the channel N_1' is $|v_1\rangle\langle v_1| \otimes |i\rangle\langle i|$, where $i = 0, 1, \ldots, d^2-1$, with equal probabilities. This is because for this set of signal states, the first term in the formula for Holevo capacity (1) is maximized (taking any state ρ and averaging over all $X_i \rho X_i^\dagger$ gives the maximally mixed state, which has the largest possible entropy in d dimensions), and the second term is minimized. The same holds

[6] This is not necessary for the proof, but it reduces the number of subscripts required to express it.

for the channel N_2'. Now, suppose there is some state $|w\rangle\langle w|$ which has smaller output entropy for the channel $N_1 \otimes N_2$ than $H(N_1(|v_1\rangle\langle v_1|)) + H(N_2(|v_2\rangle\langle v_2|))$. We can use the ensemble containing states $|w\rangle\langle w| \otimes |i_1, i_2\rangle\langle i_1, i_2|$, for $i_1, i_2 = 0 \ldots d^2 - 1$, with equal probabilities, to obtain a larger capacity for the tensor product channel $N_1' \otimes N_2'$.

The above argument works equally well to show that additivity of entanglement of formation implies additivity of minimum entropy output. We know that to achieve the maximum capacity, the average output state must be the maximally mixed state, so we can equally well use the fact that the constrained Holevo capacity $\chi_N(\rho)$ is additive to show that the minimum entropy output is additive.

10. Discussion

We have shown that four open additivity questions are equivalent. This makes these questions of even greater interest to quantum information theorists. Unfortunately, our techniques do not appear to be powerful enough to resolve these questions.

The relative difficulty of the proofs of the implications given in this paper would seem to imply that of these equivalent conjectures, additivity of minimum entropy output is in some sense the "easiest" and strong superadditivity of E_F is in some sense the "hardest." One might thus try to prove additivity of the minimum entropy output as a means of solving all of these equivalent conjectures. One step towards solving this problem might be a proof that the tensor product of states producing locally minimum output entropy gives a local minimum of output entropy in the tensor product channel.

Acknowledgement. I would like to thank Beth Ruskai for calling my attention to the papers [1, 12] and for helpful discussions, and to Beth Ruskai, Keiji Matsumoto, and an anonymous referee for useful comments on drafts of this paper.

References

1. Koenraad, M.R., Audenaert, Braunstein, S.L.: On strong superadditivity of the entanglement of formation. quant-ph/0303045
2. Bell, J.: On the Einstein Podolsky Rosen paradox. Physics **1**, 195–200 (1964)
3. Benatti, F., Narnhofer, H.: Additivity of the entanglement of formation. Phys. Rev. A **63**, art. 042306 (2001)
4. Bennett, C.H., Bernstein, H.J., Popescu, S., Schumacher, B.: Concentrating partial entanglement by local operations. Phys. Rev. A **53**, 2046–2052 (1996)
5. Bennett, C.H., DiVincenzo, D.P., Smolin, J.A., Wootters, W.K.: Mixed-state entanglement and quantum error correction. Phys. Rev. A **54**, 3824–3851 (1996), quant-ph/9604024
6. Gordon, J.P.: Noise at optical frequencies: Information theory. In: *Proceedings of the International School of Physics Enrico Fermi. Course XXXI: Quantum Electronics and Coherent Light,* P.A. Mills, (ed.), New York: Academic Press, 1964), pp. 156–181
7. Hayden, P.M., Horodecki, M., Terhal, B.M.: The asymptotic entanglement cost of preparing a quantum state. J. Phys. A: Math. Gen. **34**, 6891–6898 (2001)
8. Holevo, A.S.: Bounds for the quantity of information transmitted by a quantum communication channel. Probl. Peredachi Inf. **9**(3), 3–11 (1973) [in Russian; English translation in Probl. Inf. Transm. (USSR) **9**, 177–183 (1973)]
9. Holevo, A.S.: The capacity of the quantum channel with general signal states. IEEE Trans. Info. Theory **44**, 269–273 (1998)
10. King, C., Ruskai, M.B.: Minimal entropy of states emerging from noisy quantum channels. IEEE Trans. Info. Theory **47**, 192–209 (2001)
11. Levitin, L.B.: On the quantum measure of the amount of information. In: *Proceedings of the Fourth All-Union Conference on Information Theory*, Tashkent (1969), pp. 111–115, (in Russian)
12. Matsumoto, K., Shimono, T., Winter, A.: Remarks on additivity of the Holevo channel capacity and of the entanglement of formation. quant-ph/0206148

13. Pomeransky, A.: Strong superadditivity of the entanglement of formation follows from its additivity. quant-ph/0305056
14. Ruskai, M.B.: Some bipartite states do not arise from channels. quant-ph/0303141
15. Schumacher, B., Westmoreland.: Sending classical information via a noisy quantum channel. Phys. Rev. A **56**, 131–138 (1997)
16. Shor, P.W.: Capacities of quantum channels and how to find them. quant-ph/0304102
17. Vidal, G., Dür, W., Cirac, J.I.: Entanglement cost of mixed states. Phys. Rev. Lett. **89**, art. 027901 (2002)

Communicated by M.B. Ruskai