Additivity Questions in Quantum Information Theory

Peter Shor
Dept. of Mathematics
MIT

There are a number of interesting, open additivity questions in quantum information theory. I have shown that four of them are equivalent. Namely,

1. Additivity of the minimum entropy of the output of a quantum channel (a completely positive trace-preserving operator, or CPT operator).
2. Additivity of the entanglement of formation E_F.
3. Additivity of the Holevo channel capacity χ.
4. Strong superadditivity of the entanglement of formation E_F (this probably should be called complete superadditivity of the entanglement of formation, but it's too late to change the name).

Easy implications:

(4) $\rightarrow$ (3)

(4) $\rightarrow$ (2)

(3) $\rightarrow$ (1)

(2) $\rightarrow$ (1)

Two other additivity questions have also been shown to be equivalent.

There are other additivity quesitons which are not known to be equivalent.

- Additivity of the quantum capacity of a quantum channel [we know at least one channel for which this is non-additive, but how general is this?].
- Additivity of the distillable entanglement [non-additive if there are non-distillable negative partial transpose states, so probably non-additive in general].
- Additivity of the classical capacity of a quantum channel assisted by limited entanglement.

Outline.

- Introduce the additivity problems we prove equivalent.
- Introduce three techniques that we use.
- Sketch one of the proofs.

Theorem (Holevo, Schumacher-Westmoreland)

The classical-information capacity obtainable using codewords composed of signal states ρ_i, where ρ_i has marginal probability p_i, is

$$\chi(\{\rho_i\};\{p_i\}) = H_{\mathrm{vN}}(\sum_i p_i \rho_i) - \sum_i p_i H_{\mathrm{vN}}(\rho_i)$$

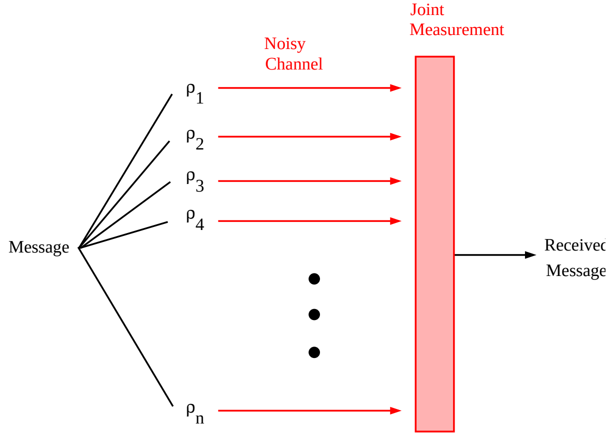
where $H_{\mathrm{vN}(\rho)} = -\mathrm{Tr}(\rho \log \rho)$.

Does this give the capacity of a quantum channel $\mathcal{N}$?

Possible capacity formula:
Maximize $\chi(\{\mathcal{N}(\rho_i)\};\{p_i\})$ over all output states $\mathcal{N}(\rho_i)$ of the channel.

Unentangled Inputs

Joint Measurements

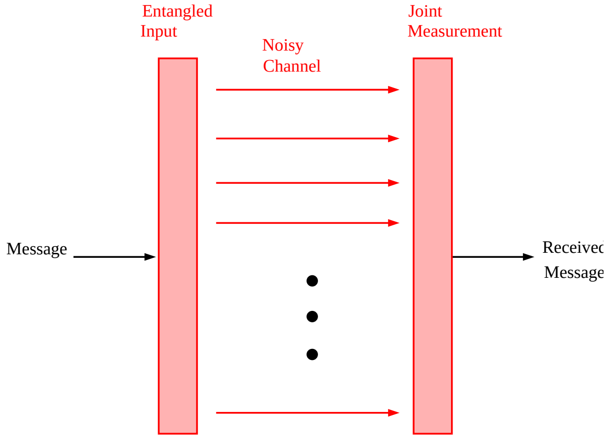


Maximize over probability distributions on inputs to the channel ρ_i, p_i, where ρ_i is in the input space of the channel:

$$\chi(\{\mathcal{N}(\rho_i)\}; \{p_i\})$$

Entangled Inputs

Joint Measurements



Maximize over probability distributions on inputs to the channel ρ_i, p_i where ρ_i is in the tensor product space of n channel inputs:

$$\lim_{n\to\infty} \frac{1}{n} \chi(\{\mathcal{N}^{\otimes n}(\rho_i)\}; \{p_i\})$$

Open Question

Is channel capacity additive?

Is $\max\ \chi(\mathcal{N}_1 \otimes \mathcal{N}_2) = \max\ \chi(\mathcal{N}_1) + \max\ \chi(\mathcal{N}_2)$?

If it is, then χ gives the classical-information capacity of a quantum channel.

Minimum entropy output (of a quantum channel)

Is

$$\min_{\rho} \; H((\mathcal{N}_1 \otimes \mathcal{N}_2)(\rho)) \quad = \quad \min_{\rho} \; H(\mathcal{N}_1(\rho)) \quad + \quad \min_{\rho} \; H(\mathcal{N}_2(\rho))?$$

This comes from the idea that we want to minimize the second term in the expression for the Holevo capacity.

Additivity of channel capacity implies additivity of minimum entropy output.

Suppose we have two channels $\mathcal{N}_1$ and $\mathcal{N}_2$ and we want to show that their minimum entropy output is additive. Consider the channels $\mathcal{N}'_a$ with input space augmented by a classical variable x with $1 \leq x \leq d_{\text{in}}^2$ defined as

$$\mathcal{N}'_a(\rho, x) = U_x \mathcal{N}(\rho) U'_x$$

where the U_x are unitary and satisfy

$$\sum_{x=1}^{d_{\text{in}}^2} U_x \rho U'_x = I/d \quad \forall \rho$$

This extra variable x specifies a unitary transformation to be applied on the channel output of U.

Then for $\mathcal{N}'$ the capacity is

$$\max \chi \mathcal{N}'_a = \log d_{\text{in}} - \min_{\rho} H(\mathcal{N}_a(\rho))$$

since we can take any input giving minimum entropy output on $\mathcal{N}$, and symmetrize it so that we get d^2 input states to $\mathcal{N}'$ whose average entropy output is I/d and each individual output has entropy $\min_\rho H(\mathcal{N}(\rho)$, and similarly for the tensor product $\mathcal{N}'_1 \otimes \mathcal{N}'_2$.

Thus, if Holevo capacity is additive for $\mathcal{N}'_1$ and $\mathcal{N}'_2$, minimimum entropy output is additive for $\mathcal{N}_1$ and $\mathcal{N}_2$.

Entanglement cost: $E_C(\rho)$

$$E_C(\rho) = \lim_{n\to\infty} \frac{1}{n} \begin{pmatrix} \text{Number of EPR pairs needed to} \\ \text{make an approximation of } \rho^{\otimes n}. \end{pmatrix}$$

Distillable entanglement: $E_D(\rho)$

$$E_D(\rho) \lim_{n\to\infty} \frac{1}{n} \begin{pmatrix} \text{Number of approximate EPR} \\ \text{pairs obtainable from } \rho^{\otimes n}. \end{pmatrix}$$

The protocols above may use only local operations and classical communication.

Entanglement of formation.

$$E_F = \min_{\rho=\sum_i p_i \rho_i} \sum_i p_i E_P(\rho_i)$$

and the ρ_i are pure states (rank 1).

Conjecture: entanglement of formation is additive.

$$E_F(\rho_1 \otimes \rho_2) = E_F(\rho_1) + E_F(\rho_2).$$

where

$$E_F = \min_{\rho = \sum_i p_i \rho_i} \sum_i p_i E_P(\rho_i)$$

and the ρ_i are pure states (rank 1).

Strong Superadditivity of Entanglement of Formation

Instead of

$$E_F(\rho_1 \otimes \rho_2) = E_F(\rho_1) + E_F(\rho_2),$$

we generalize to

$$E_F(\rho) \geq E_F(\mathrm{Tr}_2\rho) + E_F(\mathrm{Tr}_1\rho).$$

Other direction ($\leq$) is easy for tensor products, not true for general mixed states.

Entanglement of Formation and Holevo capacity

Theorem (Stinespring) Any CPT map $\rho \rightarrow \mathcal{N}(\rho)$ can be implemented by first applying a unitary embedding of ρ into a larger Hilbert space

$$\mathcal{U}(\rho) = \rho \rightarrow U(\rho \otimes |\,0\rangle\langle 0\,|)U^{\dagger}$$

and then tracing out part of the larger Hilbert space

$$\rho \rightarrow \mathrm{Tr}_2 U(\rho \otimes |\,0\rangle\langle 0\,|)U^{\dagger}.$$

If $\rho_i = |\,\psi\rangle\langle\psi\,|$ is a pure state, then

$$\begin{aligned} H(\mathcal{N}(\rho_i)) &= H(\mathrm{Tr}_2 U(\rho_i \otimes |\,0\rangle\langle 0\,|)U^\dagger) \\ &= E_P(\mathcal{U}(\rho_i)). \end{aligned}$$

Thus

$$\begin{aligned} E_F(\mathcal{U}(\rho)) &= \min_{\rho=\sum_i p_i\rho_i} \sum_i p_i E_P(\mathcal{U}\rho_i) \\ &= \min_{\rho=\sum_i p_i\rho_i} \sum_i p_i H(\mathcal{N}(\rho_i)) \end{aligned}$$

This is the second term in the Holevo capacity.

This shows that entanglement of formation is equivalent to constrained Holevo capacity, where constrained Holevo capacity is defined as

$$\chi_\rho(\mathcal{N}) = \max_{\sum_i p_i \rho_i = \rho} H(\mathcal{N}(\rho)) - \sum_i p_i H(\mathcal{N}(\rho_i))$$

This doesn't immediately imply that entanglement of formation is equivalent to Holevo capacity because we can't arrange for the maximum over ρ to occur at the point where $\mathcal{U}(\rho) = \sigma$, where σ is the state for which we want fo find the entanglement of formation.

Linear Programming Duality

We need to compute

$$\min_{\rho=\sum_i p_i |\, v_i\rangle\langle v_i \,|} \sum_i p_i H(\mathcal{N}(|\, v_i\rangle\langle v_i \,|))$$

Consider the problem as one of finding the p_i corresponding to every possible pure state v_i (so $H(|\, v_i\rangle\langle v_i \,|)$ is known). That is,

$$\begin{array}{ll} \displaystyle\min_{p_i \geq 0} & \displaystyle\sum_i p_i H(\mathcal{N}(|\, v_i\rangle\langle v_i \,|)) \\ \text{subject to} & \displaystyle\sum_i p_i |\, v_i\rangle\langle v_i \,| = \rho \end{array}$$

This is a linear program in the p_i.

Every linear program has a dual linear program which has the same optimum value. For

$$\begin{array}{ll} \min\limits_{p_i \geq 0} & \sum\limits_i p_i H(\mathcal{N}(|\, v_i \rangle \langle v_i \,|)) \\ \text{subject to} & \sum\limits_i p_i |\, v_i \rangle \langle v_i \,| = \rho \end{array}$$

The dual program is

$$\begin{array}{ll} \max\limits_{\tau} & \operatorname{Tr} \tau \rho \\ \text{subject to} & \langle v \,|\, \tau \,|\, v \rangle \leq H(N(|\, v \rangle \langle v \,|)) \end{array}$$

where the last inequality must hold for all $|\, v \rangle$, and τ is maximized over Hermitian matrices.

Showing that these two lp's give the same value has one easy direction:

$$\begin{aligned}\min_{p_i \geq 0} \sum_i p_i H(\mathcal{N}(|\, v_i\rangle\langle v_i \,|)) &\geq \sum_i p_i \,\langle v_i \,|\, \tau \,|\, v_i\rangle \\ &= \operatorname{Tr} \sum_i p_i \tau |\, v_i\rangle\langle v_i \,| \\ &= \operatorname{Tr} \tau\rho\end{aligned}$$

The other direction requires use of the duality theorem for LP's

We now sketch the proof that additivity of the minimum entropy output of a quantum channel implies additivity of entanglement of formation.

This is equivalent to additivity of constrained Holevo capacity

$$\chi_\rho(\mathcal{N}) = \max_{\sum_i p_i \rho_i = \rho} H(\mathcal{N}(\rho)) - \sum_i p_i H(\mathcal{N}(\rho_i))$$

Recall by the lp formulation that there is a matrix τ such that

$$\operatorname{Tr} \rho_i \tau \leq H(\mathcal{N}(\rho_i))$$

with equality for signal states ρ_i.

If we could find another channel related to $\mathcal{N}$ such that

$$H(\mathcal{N}'(\rho)) = H(\mathcal{N}(\rho)) + C - \operatorname{Tr} \rho_i \tau$$

then for signal states ρ_i, we have equality

$$H(\mathcal{N}'(\rho_i)) = H(\mathcal{N}(\rho_i)) + C - \operatorname{Tr} \rho_i \tau = C$$

and for other states, we have inequality

$$H(\mathcal{N}'(\rho_i)) = H(\mathcal{N}(\rho_i)) + C - \operatorname{Tr} \rho_i \tau \geq C$$

so the signal states for this channel are exactly the minimum entropy output states.

Now suppose we have two channels $\mathcal{N}_1$ and $\mathcal{N}_2$. We find $\mathcal{N}_1'$ and $\mathcal{N}_2'$ as on the previous slide. Now, the additivity of minimum entropy output for $\mathcal{N}_1'$ and $\mathcal{N}_2'$ implies the additivity of the constrained Holevo capacity for $\mathcal{N}_1'$ and $\mathcal{N}_2'$. This is because

$$\begin{aligned} \chi_{\rho_1 \otimes \rho_2}(\mathcal{N}_1 \otimes \mathcal{N}_2) \quad &\geq \quad H((\mathcal{N}_1 \otimes N_2)(\rho_1 \otimes \rho_2)) \\ &\qquad - \min_{\sigma} H((\mathcal{N}_1 \otimes \mathcal{N}_2)(\sigma)) \end{aligned}$$

which is additive by assumption of additivity of minimum entropy output.

We then will have to show (using the construction of $\mathcal{N}_i'$) that additivity of constrained Holevo capacity for $\mathcal{N}_1'$ and $\mathcal{N}_1'$ implies its additivity for $\mathcal{N}_1$ and $\mathcal{N}_1$.

We actually cannot construct $\mathcal{N}'$ as advertised. We just construct a sequence of such $\mathcal{N}'$s that come close. Recall we wanted

$$H(\mathcal{N}'(\rho)) = H(\mathcal{N}(\rho)) + C - \operatorname{Tr} \rho\tau.$$

We choose $\mathcal{N}'$ to be the channel that with probability q, outputs $\mathcal{N}(\rho)$, and with probability $1-q$, makes a POVM measurement with elements $\mathbf{E}$ and $I - \mathbf{E}$. If the measurement outcome is $\mathbf{E}$, then $\mathcal{N}'$ outputs a pure state signifying the result was $\mathbf{E}$ tensored with a maximally mixed state on k qubits. If the result is $I - \mathbf{E}$, it outputs only a pure state signifying this fact. Then

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

First term: because $\mathcal{N}'$ outputs $\mathcal{N}(\rho)$ with probability q.

Second term: coin flip with probabilities q & $1-q$

Third term: we output a maximally mixed state on k qubits with probability $(1-q)\mathrm{Tr}\,\mathbf{E}\rho$.

Last term: from the measurement $\mathbf{E}$.

We wanted a channel $\mathcal{N}'$ with

$$H(\mathcal{N}'(\rho)) = H(\mathcal{N}(\rho)) + C - \mathrm{Tr}\,\rho\tau.$$

We found a channel $\mathcal{N}'$ with

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

If it weren't for the last term, we would be able to choose $\mathbf{E}$ to obtain exactly what we wanted (up to a constant factor).

By taking k large and q close to 1, we can make this last term go to zero while keeping the other terms the right relative sizes.

We still have to show that additivity for $\mathcal{N}_1'$ and $\mathcal{N}_2'$ implies additivity for $\mathcal{N}_1$ and $\mathcal{N}_2$. This is not hard, and completes our proof that (1) $\rightarrow$ (3).

Recall the four questions to be shown equivalent.

1. Additivity of the minimum entropy of the output of a quantum channel (a completely positive trace-preserving operator, or CPT operator).
2. Additivity of the entanglement of formation E_F.
3. Additivity of the Holevo channel capacity χ.
4. Strong superadditivity of the entanglement of formation E_F (this probably should be called complete superadditivity of the entanglement of formation, but it's too late to change the name).

(1) $\rightarrow$ (2) LP duality, Stinespring dilation, channel extension.

(2) $\rightarrow$ (4) LP duality

(2) $\rightarrow$ (3) Stinespring dilation, channel extension.

Formula for entanglement-assisted capacity

Theorem (Bennett, Shor, Smolin, Thapliyal)

$$\max_{\rho} H_{\mathrm{vN}}(\mathcal{N}(\rho)) + H_{\mathrm{vN}}(\rho) - H_{\mathrm{vN}}((\mathcal{N} \otimes \mathcal{I}))(\Phi_\rho))$$

Φ_ρ is a pure state on the tensor product of the input space of the channel and a quantum space that the sender keeps, with

$$\mathrm{Tr}_B \Phi_\rho = \rho.$$

When the channel is classical, this formula turns into the entropy of the input plus the entropy of the output less the entropy of the joint system.

Generalization

Suppose that the sender and the receiver have a limited amount of entanglement (E ebits) they share. How much can capacity can they obtain from a quantum channel?

If the sender is not allowed to use entanglement between different channel uses, the answer is:

$$\max_{\rho_i : \bar{H}(\rho_i) \leq E} \bar{H}(\rho_i) + H(\mathcal{N}(\bar{\rho_i})) - \bar{H}((\mathcal{N} \otimes \mathcal{I})\Phi_{\rho_i})$$

Here $\bar{H}$ means average over the entropy, and $\bar{\rho_i}$ means average over the state; Φ_{ρ_i} is the pure entangled state (shared between sender and receiver) whose partial traces are ρ_i. This formula interpolates between the Holevo-Schumacher-Westmoreland capacity and the entanglement-assisted capacity.

Is this quantity additive? We can reduce this question to that of whether the quantity

$$\max_{\rho} \lambda H(\rho) - H(\mathcal{E}(\rho))$$

is additive, where $\mathcal{E}$ is a CPT map. If $\lambda = 0$, this is the additivity of the minimum entropy output of a quantum channel. If $\lambda = 1$, this is the additivity of entanglement-assisted capacity. For $0 < \lambda < 1$, this may be a stronger conjecture than the other additivity conjectures.