

---

# Additivity Questions in QIT: Recent Results and Outlook

Koenraad M.R. Audenaert

University of Wales Bangor

---

September 2, 2003

---

# Part 1: Additivity Questions

---

# Entanglement Cost

- One of the Big Open Problems of QIT: how to calculate  $E_C$ ?
- $E_C$  defined in an operational way, nearly impossible to calculate
- First theoretical breakthrough (Hayden, Horodecki and Terhal):  
 $E_C$  is equal to the *regularisation* of  $E_F$ , the entanglement of formation (EoF):

$$E_C(\rho) = \lim_{n \rightarrow \infty} E_F(\rho^{\otimes n})/n.$$

- EoF defined in a mathematical and non-operational way (see below)
- Much more amenable to calculation than  $E_C$
- For 2-qubit mixed states, a closed formula for  $E_F$  exists (Wootters).
- $E_C$  still requires calculations over infinite-dimensional states.

---

# Is EoF additive?

- The regularisation  $\rho \mapsto \rho^{\otimes n}$  is about calculating potential “wholesale discounts”
- We would love it if there were no such discounts
- We want **Additivity**...

$$E_F(\rho_1 \otimes \rho_2) \stackrel{?}{=} E_F(\rho_1) + E_F(\rho_2)$$

- ... because then  $E_C = E_F$
  - Additivity has been proven in specific instances.
  - Some of these additivity results are sufficiently powerful to allow calculating  $E_C$  for certain classes of mixed states.
  - The much sought-after general proof, however, remains elusive for the time being and, in fact, general additivity is still a conjecture.
-

---

# Strong Superadditivity of EoF?

- It is very easy to show that the EoF is **subadditive**:

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

- Additivity would then follow from **superadditivity**,

$$E_F(\rho_1 \otimes \rho_2) \geq? E_F(\rho_1) + E_F(\rho_2).$$

- Vollbrecht and Werner conjectured a stronger property implying superadditivity:

## **Strong Superadditivity**

$$E_F(\rho) \geq? E_F(\rho_I) + E_F(\rho_{II})$$

Here  $\rho$  is a general state over a duplicated Hilbert space and  $\rho_I$  and  $\rho_{II}$  are its reductions to the different copies of that space.

---

# Entanglement of Formation Defined

- Any state  $\rho$  can be realised by an **ensemble** of pure states
- An ensemble is specified by a set of pairs  $\{(p_i, \psi_i)\}_{i=1}^N$ 
  - of  $N$  state vectors  $\psi_i$  and statistical weights  $p_i$
  - with  $p_i \geq 0$  and  $\sum_i p_i = 1$
- The entanglement of formation (EoF) of a bipartite state  $\rho$  (over the bi-partite Hilbert space  $\mathcal{H}_A \otimes \mathcal{H}_B$ ), is

$$E_F(\rho) = \min_{\{(p_i, \psi_i)\}} \left\{ \sum_i p_i S(\text{Tr}_A \Psi_i) : \sum_i p_i \Psi_i = \rho \right\}.$$

- This messy formula says that EoF is a convex closure...

---

# Convex Closures

- The convex closure of a set  $S$ , denoted  $\text{Conv}(S)$ , is the smallest convex set containing  $S$ .
- The epigraph of a function  $y = f(x)$  is the set of points

$$\text{Epi}(f) := \{(x, y) : y \geq f(x)\}$$

- The convex closure  $\hat{f}$  of a function  $f$  is defined by

$$\text{Epi}(\hat{f}) = \text{Conv}(\text{Epi}(f))$$

- The convex closure of  $f$  can be calculated by taking convex combinations

$$\hat{f}(x) = \min_{\{(a_i, x_i)\}} \left\{ \sum_i a_i f(x_i) : \sum_i a_i x_i = x \right\}$$

- Dually,  $\hat{f}$  is the pointwise supremum of all affine functions majorised by  $f$

$$\hat{f}(x) = \sup_{a, b} \{a^T x + b : (\forall y : a^T y + b \leq f(y))\}$$

---

# EoF is a Convex Closure

- **Observation 1:** The EoF is the **convex closure** of the entanglement function

$$E(\Psi) := S(\text{Tr}_A \Psi):$$

$$E_F(\rho) = \min_{\{(p_i, \rho_i)\}} \left\{ \sum_i p_i E(\rho_i) : \sum_i p_i \rho_i = \rho \right\} = \hat{E}(\rho)$$

- **Observation 2:** By the dual formulation of the convex closure, the EoF is the pointwise supremum of all affine functions on  $\mathcal{S}(\mathcal{H})$  majorised by  $E$

$$E_F(\rho) = \sup_{X \in \mathcal{B}(\mathcal{H})} \left\{ \text{Tr}[\rho X] : (\forall \sigma \in \mathcal{S}(\mathcal{H}) : \text{Tr}[\sigma X] \leq E(\sigma)) \right\}$$

- Moreover, this definition can be pulled apart into two identical parts, based on the concept of the **conjugate function**
-

---

# Conjugate function

- Given a function  $f$ , its **conjugate function**  $f^*$  is:

$$f^*(X) = \max_{\rho \in \mathcal{S}(\mathcal{H})} \text{Tr}[\rho X] - f(\rho)$$

- If  $f$  is continuous this is called the **Legendre transform** of  $f$ .
- The conjugate is convex in  $X$ : pointwise maximum of affine functions
- The conjugate and convex closure determine each other completely

$$f \xrightarrow{*} f^* \xleftarrow{*} \hat{f}$$

- The convex closure of  $f$  is the conjugate of the conjugate of  $f$ :  $\hat{f} = f^{**}$
- The conjugate of the convex closure of  $f$  is the conjugate of  $f$ :  $\hat{f}^* = f^*$

---

# Result 1

Define  $g$  on  $\mathcal{B}^+(\mathcal{H})$  by

$$g(A) = E^*(\log(A)) = \max_{\psi \in \mathcal{H}} \text{Tr}[|\psi\rangle\langle\psi| \log(A)] - E(|\psi\rangle\langle\psi|).$$

**Theorem 1** *Strong superadditivity of the EoF,*

$$E_F(\rho) \geq? E_F(\rho_I) + E_F(\rho_{II}),$$

*is equivalent to subadditivity of  $g$ ,*

$$g(A_1 \otimes A_2) \leq? g(A_1) + g(A_2).$$

---

# Relation to quantum channels

Let  $\|\cdot\|_q$  be the Schatten  $q$ -norm  $\|X\|_q = (\text{Tr}(|X|^q))^{1/q}$

Define the **Maximal Output Purity** or **MOP** (Amosov, Holevo and Werner) of a quantum channel  $\Lambda$ :

$$\nu_q(\Lambda) = \max_{\phi \in \mathcal{H}} \|\Lambda(|\phi\rangle\langle\phi|)\|_q$$

**Theorem 2** *If there exists a number  $q_0$  such that  $\nu_q(\Lambda)$  is multiplicative for all  $1 \leq q \leq q_0$  and for all completely positive maps:*

$$\nu_q(\Lambda_1 \otimes \Lambda_2) = \nu_q(\Lambda_1)\nu_q(\Lambda_2),$$

*then the EoF is strongly superadditive.*

---

---

# Further Relations between Additivities

- Abovementioned results are in Audenaert and Braunstein ([quant-ph/0303045](#))
- Multiplicativity of MOP  $\nu_q$  of channels for all  $1 \leq q \leq q_0$  leads to additivity of the entropic MOP  $\nu_S$  (minimal output entropy). (Amosov, Holevo and Werner, [quant-ph/0003002](#)).
- Peter Shor ([quant-ph/0305035](#)) proved the equivalence of:
  - Strong Superadditivity of EoF
  - Additivity of EoF
  - Additivity of entropic MOP
  - Additivity of Holevo capacity
- A combination of the AHW and Shor results leads to a slightly stronger version of Theorem 2: need to deal with channels only (trace-preserving maps).

---

# Relation to Quantum Cryptography

- Cryptographic setting: Alice uses source ensemble  $\mathcal{E} = \{p_i, |\psi_i\rangle\}$ . Eve measures Alice's signals using a POVM  $\{E_b\}$  and sends fake signals  $\{\phi_b\}$  to Bob.
- The **Accessible Fidelity** (AF) of the ensemble  $\mathcal{E}$  is defined as

$$F(\mathcal{E}) = \sup_{E_b} \sup_{|\phi_b\rangle} \sum_i \sum_b p_i \langle \psi_i | E_b | \psi_i \rangle |\langle \psi_i | \phi_b \rangle|^2.$$

and is a measure of the maximal probability that Eve's actions will remain undetected.

- **Theorem:** AF is multiplicative. Proof relies on
  - Eve's actions implementing an entanglement breaking channel
  - multiplicativity of  $\nu_\infty$  for entanglement breaking maps
- See Audenaert, Fuchs, King and Winter, [quant-ph/0308120](#).

---

# Multiplicativity of the MOP

- (quant-ph/0003002) Multiplicativity of  $\nu_q$  conjectured by Amosov, Holevo and Werner for trace preserving channels.
- Proven by King in the cases that one of the channels is:
  - (quant-ph/0103086) a qubit channel, when  $q = 2$
  - (quant-ph/0103156) a unital qubit channel
  - (quant-ph/0212057) an entanglement breaking map
- (quant-ph/0203003) Refuted for qutrit channels when  $q > 4.79$  by Holevo and Werner.
- Might still hold for  $1 \leq q \leq q_0$  and/or for qubit channels.

---

## Part 2: King's Conjecture

---

# King's Conjecture

- In [quant-ph/0103086](#), King presented the following conjecture for any state  $\rho$  on a  $d \times 2$  Hilbert space and any qubit channel  $\Phi$ :

$$\|(\mathbf{I} \otimes \Phi)(\rho)\|_q \leq \nu_q(\Phi)(\|\rho_{11}\|_q + \|\rho_{22}\|_q).$$

Here,  $\rho$  is to be written as a  $2 \times 2$  block matrix:  $\rho = \begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix}$ .

- Multiplicativity of MOP would follow immediately. Put  $\rho = (\Omega \otimes \mathbf{I})(\sigma)$ , then

$$\begin{aligned} \sum_i \|\rho_{ii}\|_q &= \sum_i \|\Omega(\sigma_{ii})\|_q \\ &= \sum_i \text{Tr}(\sigma_{ii}) \|\Omega(\sigma_{ii}/\text{Tr}(\sigma_{ii}))\|_q \\ &\leq \sum_i \text{Tr}(\sigma_{ii}) \nu_q(\Omega) = \text{Tr}(\sigma) \nu_q(\Omega). \end{aligned}$$

---

# Generalised King's Conjecture

- We might consider the more general (hence incorrect in general) conjecture for states on a  $d_1 \times d_2$  Hilbert space and for completely positive maps  $\Phi$ :

$$\|(\mathbf{I} \otimes \Phi)(\rho)\|_q \leq \nu_q(\Phi) \sum_i \|\rho_{ii}\|_q.$$

- It can be proven in the following cases:

- $\Phi = \mathbf{I}$ : reduces to the known inequality  $\|\rho\|_q \leq \sum_i \|\rho_{ii}\|_q$  (1)

(Horn and Johnson, *Topics in Matrix Analysis*, Section 3.5, Problem 22).

- $\rho$  is **pure**: in that case,  $\sum_i \|\rho_{ii}\|_q$  is just  $\text{Tr}(\rho)$ , and by (1) we have

$$\|(\mathbf{I} \otimes \Phi)(\rho)\|_q \leq \sum_{j=1}^{d_1} \|\Phi(\rho^{jj})\|_q \leq \nu_q(\Phi) \text{Tr}(\rho).$$

- $\rho$  is **separable**: following King's treatment of entanglement breaking channels we find the stronger result  $\|(\mathbf{I} \otimes \Phi)(\rho)\|_q \leq \nu_q(\Phi) \|\text{Tr}_2 \rho\|_q$ .

---

# King's Conjecture Rephrased

- King's Conjecture can be rephrased as follows:

$$\|(\mathbf{I} \otimes \Phi)(\rho)\|_q \leq \nu_q(\Phi) \sum_i \|\rho_{ii}\|_q$$

$$\max_{\Phi} \frac{\|(\mathbf{I} \otimes \Phi)(\rho)\|_q}{\nu_q(\Phi)} \leq \sum_i \|\rho_{ii}\|_q$$

$$\max_{\Phi'} \{ \|(\mathbf{I} \otimes \Phi')(\rho)\|_q : \nu_q(\Phi') \leq 1 \} \leq \sum_i \|\rho_{ii}\|_q$$

- Both sides are now functions of  $\rho$  only.
- Denote the LHS by  $\gamma_q(\rho)$ .

---

# Properties of $\gamma_q$

- With the definition  $\gamma_q(\rho) := \max_{\Phi} \{ \|(\mathbf{I} \otimes \Phi)(\rho)\|_q : \nu_q(\Phi) \leq 1 \}$   
King's conjecture is

$$\gamma_q(\rho) \stackrel{?}{\leq} \sum_i \|\rho_{ii}\|_q$$

- $\gamma_q$  is convex:  
As  $\|(\mathbf{I} \otimes \Phi)(\rho)\|_q$  is a convex function of  $\rho$ ,  
 $\gamma_q$  is the pointwise maximum of convex functions and thus convex itself.
- The known cases for correctness of the conjecture yield explicit values:
  - Pure states:  $\gamma_q(\rho) = \text{Tr}(\rho)$ .
  - Separable states:  $\gamma_q(\rho) = \|\text{Tr}_2(\rho)\|_q$ .

---

## An upper bound on $\gamma_q$

- So  $\gamma_q$  is convex and has known values on specific states.
- There are lots of such functions, but the largest one can be found via the convex closure construction, yielding an upper bound on  $\gamma_q$ :
  - Define  $g_q(\rho)$  to be equal to  $\gamma_q(\rho)$  for the known cases and  $+\infty$  elsewhere.
  - The convex closure of  $g_q$  is an upper bound on  $\gamma_q$ .

- One can easily show:

$$\text{Conv}(g_q)(\rho) = \min_X \{ \text{Tr } \rho + \| \text{Tr}_2(X) \|_q - \text{Tr } X : 0 \leq X \leq \rho, X \text{ separable} \}$$

- Could we be so lucky that  $\text{Conv}(g_q)(\rho) \leq \sum_i \| \rho_{ii} \|_q$  ?
  - Alas: even for  $2 \times 2$  states, this inequality is violated (Died in Simulation).
  - Nevertheless, this failed attempt illustrates the available techniques quite nicely.
-

---

# Steps of the Calculation

- Let's consider  $d \times 2$  states only.
- Fix all  $\rho_{ii}$ ; this fixes the RHS of  $\text{Conv}(g_q)(\rho) \leq \sum_i \|\rho_{ii}\|_q$ .  
It is known that  $\rho_{12} = \rho_{11}^{1/2} C \rho_{22}^{1/2}$ , with  $C$  a contraction.
- Maximise the LHS over all such  $\rho$ . As the LHS is convex in  $\rho$ , it achieves its maximum in the extreme points of the allowed set, i.e. for  $C = U$ , a unitary.
- These extreme  $\rho$  have rank  $d$ . Hence, the allowed  $X$  in  $\text{Conv}(g_q)(\rho) = \min_X \{ \text{Tr } \rho + \|\text{Tr}_2(X)\|_q - \text{Tr } X : 0 \leq X \leq \rho, X \text{ separable} \}$  are also rank  $d$ . By a result of Kraus, Cirac, Karnas and Lewenstein, such  $X$  are separable iff they are PPT.
- Using further “matrix magic”, we find that the allowed  $X$  depend on  $d$  positive parameters only.
- The minimisation can be done easily using brute force numerical calculations.

---

# Outlook: Where to go from here?

- The difficulty of the problem demands a many-viewpoints approach
- Every viewpoint supplies some “pieces of the puzzle”
- One particularly interesting approach is to consider the norm properties of  $\gamma_q$
- The definition of  $\gamma_q$  can be extended to general operators via  $\gamma_q(X) = \gamma_q(|X|)$ .
- This turns  $\gamma_q$  into a **vector norm** on operators:
  - positive and homogenous: trivial to see
  - triangle inequality: follows from convexity of  $\gamma_q$ .
- In this formulation, King’s Conjecture is a comparison between norms on the *same space*

$$\gamma_q(\rho) \leq? \sum_i \|\rho_{ii}\|_q$$

---

# Possible benefits of the norm approach

- There is a lot of theory available on matrix norms
- One has to ask the right questions, and that is largely determined by the viewpoint.

- Is  $\gamma_q$  a genuine matrix norm, i.e. is it submultiplicative?

$$\gamma_q(XY) \leq? \gamma_q(X)\gamma_q(Y).$$

- If it is a matrix norm, is it an induced one?

- Questions like this would not have been raised in other approaches and may well hold the key
- One might even get the mathematicians interested...