

---

# Quantum Theory and Global Warming

Koenraad M.R. Audenaert



University of Wales, Bangor

---

February 29, 2004

---

Overture:

Quantum Information Theory

---

# QIT = QM + IT

- Quantum Information Processing (QIP) is the study of the information processing tasks that can be accomplished using quantum mechanical systems.
- Within the broad range of topics covered by QIP, one can single out the study of the fundamental theoretical questions, forming a counterpart to the field of information theory in classical information science.
- This subfield is called Quantum Information Theory (QIT).
- It deals with the fundamental notions of information and communication, information processing, and the resources required for information processing, all in the general setting of quantum mechanics.
- Specifically, the information carriers and the communication channels in QIT are quantum systems, governed by the laws of quantum mechanics.
- What makes QIT so different from classical information theory is that the behaviour of quantum systems is so widely different from classical systems.

---

# Quantum State Descriptions

- In its simplest form, a state description of a quantum system consists of a **vector** in a complex Hilbert space.
- Principle of superposition: any linear combination of physically allowed state vectors is also an allowed state vector.
- In general, we have to deal with statistical uncertainties, noise and incompleteness of state descriptions. To do that, quantum states have to be described not by vectors but by positive semidefinite (PSD) matrices, so-called **density matrices**.
- The eigenvalues of a density matrix form a probability distribution. Its eigenvectors are state vectors.
- A **pure** state is a rank-1 density matrix and is equally well described by a state vector. Non-pure states are called **mixed** states.

---

# Quantum Operations and Measurements

- Operations on quantum systems are described by *linear, completely-positive* (CP) maps acting on the states.
- Measurements form an intrinsic part of the theory and have to be described by CP maps as well.
- Note that, in classical physics, states have an objective existence and measurements are extrinsic operations that are not essential to the theory.
- In its simplest form, a measurement is specified by a set of orthogonal state vectors  $\psi_i$ , the measurement *alternatives*.
  - Given a particle with state  $\phi$ , you can't just ask Nature what this  $\phi$  is.
  - You can only ask which one of the alternatives it is. And if it is neither, Nature will *change* it to one of the alternatives, with some probability  $P_i = |\langle \phi | \psi_i \rangle|^2$ .
  - Outcome of measurement: the particular alternative Nature has chosen.

---

# Consequences

- The linearity of operations excludes the possibility of copying quantum states (the famous no-cloning theorem) but it simplifies the theory.
- Due to the superposition principle, there exists the purely quantum-mechanical phenomenon of **entanglement**:
  - State descriptions of *composite* quantum systems do not just consist of collections of state descriptions, one for every subsystem.
  - In fact, the subsystems in a composite system typically do not even have a state description of their own, and the composite system must be described as a “togetherness”.
- Entanglement is a quantum resource that gives quantum information processing its unique properties, and its unique power.

---

# Entanglement

- Composite systems (A,B) are described by state vectors of  $\mathcal{H}_A \otimes \mathcal{H}_B$ .
- This does not mean that every state vector is of the form  $\psi = \psi_A \otimes \psi_B$ .
- One can also have  $\psi = \psi_A \otimes \psi_B + \phi_A \otimes \phi_B$ ; this can never be written as a single Kronecker product (except in trivial cases).
- Product states  $\psi = \psi_A \otimes \psi_B$  form the exception; entangled states are the rule.
- Only when the state is a product state do the subsystems have a state on their own. In an entangled state, they have not.
- Example “par excellence”: the EPR state

$$\psi = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

---

# Strange Behaviour of the EPR State

- Send the A-particle of an EPR state to Aberdeen, and the B-particle to Bangor.
- In both towns measurements are performed on the local particles.
- No matter what the chosen measurement alternatives are, every outcome will occur with 50%.
- However, when A- and B-town use the same set of alternatives, they always obtain the same outcome!
- It is as if in an EPR state, Nature has fixed the correlations between the A- and B-outcomes without yet having chosen the outcomes themselves.

---

# Spooky Action at a Distance?

- When the Scots try to fool the Welsh by choosing a different set of alternatives, this *immediately* shows up in the correlations.
- Einstein called this a “Spooky Action at a Distance”, and it was one of the reasons why he thought quantum mechanics was just a load of pants.
- Can one use entanglement to transmit messages faster than light, and thus violate special relativity?
- Nope: it only shows up in the correlations, not in the local (marginal) distributions.
- You need the outcomes from both A and B to see that, hence you need classical communication in addition.

---

# Uses for Entanglement?

- Unfortunately, “lodestone resonators” based on entanglement remain fiction.
- But it’s useful for other things:
- Quantum Cryptography
- Teleportation of quantum states
- Quantum Computing

---

# Topics in QIT

- Some questions that are being considered in QIT are similar in nature to those from classical information theory, with quantumness giving them a distinct flavour:
  - generalisations of Shannon's coding theorems
  - quantum data compression
  - the capacity of quantum channels for classical information.
- Other questions have no classical counterpart:
  - study of state estimation
  - state discrimination
  - the capacity of quantum channels for quantum information
  - quantum error-correcting codes
  - entanglement theory

---

Theme I:

Additivity Problems in QIT

---

# Algebraic Quantum Information Theory

- Quantum Information Theory (QIT) is a two-legged science:
  - Information Theory
  - Quantum Mechanics
- “My” kind of QIT = Algebraic QIT = QIT with a third leg: tools
  - Matrix Theory: matrix inequalities, eigenvalues, singular values,...
  - Convexity Theory: convex optimisation, duality theory, convex hulls,...
- Focus on problems where these tools are essential.

---

# The Trouble with QIT

- QIT is about bipartite and even multipartite states.
- These are essentially higher-order tensors: one pair of indices (row, column) for every subsystem.
- Life would be easy if higher-order generalisations of eigenvalue and singular value decompositions existed.
- They do not, so we get a lot of difficult problems in QIT.
- We need all the help we can get, hence my focus on the mathematical tools.
- In this talk, we will have a look at the so-called **additivity problems** in QIT.

---

# Entanglement Measures

- How to quantify entanglement of a state?
- Pure states: only one reasonable measure
  - $E(|\psi\rangle\langle\psi|) = S(\text{Tr}_A |\psi\rangle\langle\psi|)$ . Here  $S$  is the von Neumann entropy, and  $\text{Tr}_A$  is the *partial trace*, the mathematical equivalent of ignoring a subsystem.
- Mixed states: whole zoo of measures, use what you need
  - Entanglement Cost  $E_C$
  - Entanglement of Distillation  $E_D$
  - Entanglement of Formation (EoF,  $E_F$ )
  - Relative Entropy of Entanglement  $E_R$
  - Squashed Entanglement  $E_{sq}$

---

# Entanglement Cost

- Calculating the entanglement cost  $E_C$  is one of the Big Open Problems of QIT.
- $E_C$  defined in an operational way, nearly impossible to calculate
- Hayden, Horodecki and Terhal:  $E_C$  is equal to the *regularisation* of  $E_F$ :

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

- $E_C$  would be equal to  $E_F$  if  $E_F$  were **additive**.

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

- This is Additivity Problem #1.
- One only needs to prove **superadditivity**,  $E_F(\rho_1 \otimes \rho_2) \geq E_F(\rho_1) + E_F(\rho_2)$ ?, because **subadditivity**,  $E_F(\rho_1 \otimes \rho_2) \leq E_F(\rho_1) + E_F(\rho_2)$ , is trivial to prove.

---

# Strong Superadditivity of EoF

- Vollbrecht and Werner conjectured a stronger property implying superadditivity:

**Strong Superadditivity:**

$$E_F(\rho) \geq E_F(\text{Tr}_1 \rho) + E_F(\text{Tr}_2 \rho) ?$$

where  $\rho$  is a state over a duplicated Hilbert space

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 = (\mathcal{H}_{1A} \otimes \mathcal{H}_{1B}) \otimes (\mathcal{H}_{2A} \otimes \mathcal{H}_{2B}).$$

- This is Additivity Problem #2
- And now for something completely different...

---

# Classical Capacity of Quantum Channels

- Noisy communication channels modelled as completely positive trace-preserving (CPTP) maps between operator algebras.
- One of the most fundamental questions in QIT: determination of *classical capacity of a quantum channel* i.e. the capacity of quantum channels to transmit classical information.
- Much more difficult than its purely classical counterpart due to the existence of *entanglement*.
- Optimal quantum channel *decoder* uses *entangled measurements* over the channel output states; i.e. the measurement alternatives are entangled states

---

# Additivity of Holevo Capacity

- Is entanglement also necessary to obtain an optimal *encoder*?
- Widely believed not to be the case, i.e. no benefit is expected in having entanglement between the (single-letter) states sent over the channel.
- To prove this, it is necessary to show that the single-letter classical capacity (a.k.a. the Holevo capacity  $\chi$ ) of a quantum channel is additive.
- The Holevo capacity of a channel  $\Phi$  is:

$$\chi(\Phi) = \sup_{\{(\pi_i, \rho_i)\}} S\left(\sum \pi_i \Phi(\rho_i)\right) - \sum \pi_i S(\Phi(\rho_i)).$$

- Is this additive?  $\chi(\Phi_1 \otimes \Phi_2) = \chi(\Phi_1) + \chi(\Phi_2)$ ?
- This is Additivity Problem #3.

---

# Maximal Output Purity of Channels

- Holevo capacity is a complicated quantity. A simpler channel property, called the minimal output entropy (MOE), has been introduced.
- In general, if a pure state is sent through a channel it will become noisy, i.e. a mixed state.
- Consider the state that is least affected and measure its noisiness...
- ... by the Schatten  $q$ -norm  $\|X\|_q = (\text{Tr } X^q)^{1/q}$ , giving the *maximal output  $q$ -purity* (MOP),  $\nu_q$ , of the channel:

$$\nu_q(\Omega) = \max_{\psi} \{ \|\Omega(|\psi\rangle\langle\psi|)\|_q : \|\psi\| = 1 \}$$

- ... or by the entropy  $S$ , giving the *minimal output entropy* (MOE),  $\nu_S$ :

$$\nu_S(\Omega) = \min_{\psi} \{ S(\Omega(|\psi\rangle\langle\psi|)) : \|\psi\| = 1 \}.$$

---

# Additivity Problem #4

- Is MOE additive:  $\nu_S(\Phi_1 \otimes \Phi_2) = \nu_S(\Phi_1) + \nu_S(\Phi_2)$ ?
- Could shed some light on the additivity problem for the Holevo capacity.
- Additivity of MOE would follow from multiplicativity of MOP for “small”  $q$  (Amosov, Holevo and Werner):  $\nu_q(\Phi \otimes \Omega) = \nu_q(\Phi)\nu_q(\Omega)$ .
- Multiplicativity of MOP proven by Chris King for entanglement breaking channels, unital qubit maps and depolarising channels.
- Refuted for values of  $q > 4.79$  (Holevo and Werner)
- Nevertheless, it could still hold for  $q \downarrow 1$  (Hope springs eternal...)
- If we could prove it for  $q = 2$  this would already be uplifting...

---

Theme II:

Optimisation Theory

---

# Local and Global Optimisation

- There are lots of techniques for finding the maxima of a general function
- Most methods can get stuck in local maxima
- Global optimisation is about finding the biggest local maximum
- No method exists that guaranteedly finds that
- So we are very happy when we have a problem for which there is only one local optimum
- Convex problems are in that league.

---

# Convex Sets and Functions

- A set  $S$  is **convex** if and only if  $\forall p, q \in S : \overline{pq} \in S$ , where  $\overline{pq}$  is the line segment joining  $p$  and  $q$
- Whatever one can say about sets, one can say about functions
- The **Graph** of a function  $y = f(x)$  is the set of points  $\{(x, y) : y = f(x)\}$
- The **Epigraph** of a function  $y = f(x)$  is the set of points

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

- A function  $f$  is convex if and only if  $\text{Epi}(f)$  is a convex set
- A function  $f$  is convex if and only if

$$\forall \{(a_i, x_i)\} : f\left(\sum_i a_i x_i\right) \leq \sum_i a_i f(x_i)$$

---

# Duality Theory

- A dual view of convexity:  
a convex set  $S$  equals the intersection of all halfplanes containing  $S$
- Likewise,  $f$  is convex if and only if  
 $f$  equals the pointwise supremum of all affine functions majorised by  $f$

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

- For every  $a$ , one can calculate  $\hat{b}(a)$ , the largest  $b$  satisfying the condition

$$\forall y : a^T y + b \leq f(y).$$

- The affine functions  $a^T x + \hat{b}(a)$  are the **tangents** to  $f$  with given slope  $a$ .

---

# Duality in Optimisation

- Let's consider the following constrained optimisation:
- Minimise a convex function  $f(x)$  over the interval  $x \leq x_u$ .

$$\hat{f} = \min_x \{f(x) : x \leq x_u\}.$$

- This is a convex problem.
- We can easily prove

$$\min_x \{f(x) : x \leq x_u\} \geq \max_a \{ax_u + \hat{b}(a) : a \leq 0\}.$$

(In fact, equality holds!)

- The maximisation over  $a$  is also a convex problem, called the **dual** problem.
- The minimisation over  $x$  is called the **primal** problem.

---

# Certificates of Convergence

- By picking specific  $x \leq x_u$  (so-called **feasible**  $x$ ), you get *upper bounds* on  $\hat{f}$ .
- By picking specific tangents  $a \leq 0$  (feasible  $a$ ), you get *lower bounds* on  $\hat{f}$ .
- Thus if you solve the primal problem together with the dual one, you can bracket the solution within an upper and a lower bound.
- The difference between the bounds is an upper bound on how far you are from the real solution.
- You, therefore, get a **certificate of convergence**.
- This works for general convex optimisation problems.
- No other optimisation problem has this feature.

---

# Duality and Convex Hulls

- The **Convex Hull**  $\text{Conv}(S)$  of a set  $S$  is the *union* of all  $\overline{pq}$  with  $p, q \in S$ .
- Dually, the convex hull of  $S$  is the *intersection* of all halfplanes containing  $S$ .
- The convex hull  $\hat{f}$  of a function  $f$  is defined by

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

- ... and it can be calculated by taking all convex combinations:

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

- ... or as the pointwise supremum of all (global) tangents to  $f$ :

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

- The latter formula states that  $\hat{f}$  is the **double conjugation**  $f^{**}$  of  $f$ .

---

# Conjugate function

- Define the **conjugate function**  $f^*$ :

$$f^*(a) = \max_x a^T x - f(x)$$

- If  $f$  is continuous this is the **Legendre transform** of  $f$ .
- The conjugate and convex hull determine each other completely!

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

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

---

Allegro:

# Convex Optimisation and Additivity

---

# 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  $\{(p_i, \psi_i)\}_{i=1}^N$

- $N$  state vectors  $\psi_i$  and statistical weights  $p_i$

- $p_i \geq 0$  and  $\sum_i p_i = 1$

- The entanglement of formation (EoF) of a bipartite state  $\rho$  is

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

- This is the **convex hull** of the pure state entanglement function  $E$ .

$$E(|\psi\rangle\langle\psi|) = S(\text{Tr}_A |\psi\rangle\langle\psi|)$$

- The EoF is thus the conjugate of the conjugate of  $E$ .

- Statements about EoF might translate to statements about  $E^*$ .
-

---

# Additivity of EoF

## Theorem 1 (Audenaert and Braunstein)

With  $E^*$  defined by

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

*strong superadditivity of the EoF:*

$$E_F(\rho) \geq E_F(\text{Tr}_1 \rho) + E_F(\text{Tr}_2 \rho),$$

*is equivalent to (some kind of) subadditivity of  $E^*$ :*

$$E^*(H_1 \otimes \mathbf{I} + \mathbf{I} \otimes H_2) \leq E^*(H_1) + E^*(H_2).$$

---

# Relation to MOP

- The above Theorem reduces the additivity problem for the EoF, defined as a minimisation over *ensembles*, to an equivalent problem for the conjugate function, defined as a maximisation over *pure states*.
- Using the Lie-Trotter relation, entropic quantities can be converted to power-law quantities.
- Using some involved mathematics, Audenaert and Braunstein also proved:  
**Theorem 2** *If  $\nu_q$  is multiplicative for  $q \downarrow 1$  and for all completely positive maps, then the entanglement of formation is strongly superadditive.*
- So two additivity problems are closely related!

---

# Equivalence of All Additivity Problems

- One month later...
- Peter Shor proved equivalence of all four additivity problems!
  - additivity of EoF,
  - strong superadditivity of EoF,
  - additivity of classical capacity of a quantum channel,
  - additivity of the MOE:  $\nu_S(\Phi \otimes \Omega) = \nu_S(\Phi) + \nu_S(\Omega)$ .
- The stakes for proving multiplicativity of MOP have raised.
- So what's next?

---

Theme III:

The Quantum de Finetti Theorem

---

# Unknown Probabilities

- Probability Estimation is a procedure to estimate an unknown probability from the results of repeated trials in identical circumstances.
- In Bayesian view of probability theory, a probability is a “measure of credible belief, reflecting one’s state of knowledge”.
- In this view, “unknown probability” is an oxymoron.
- Bruno de Finetti (early 1930’s) tried to eliminate this offending concept.
- He focused on the equivalence of repeated trials:
  - indistinguishability of the different trials w.r.t. predictions
  - a probability assignment for multiple trials should be symmetric under permutation of the trials

---

# Exchangeable Probabilities

- Principle of Equivalence of Repeated Trials:
  - If an experimenter judges a collection of  $N$  trials to have a probability  $P^{(N)}$ , he will judge any permutation of the trials to have that same probability.
  - This will be true for every  $N$
  - Consistency condition:  $P^{(N)}$  must be derivable from  $P^{(N+1)}$
- Sequence of probabilities  $(P^{(N)})_N$  obeying this condition are called **exchangeable**.

---

# de Finetti's Theorem

- A sequence of probabilities  $(P^{(N)})_N$  is exchangeable if and only if

$$P^{(N)} = \int d\mu(P) P^{\times N},$$

where  $d\mu(P)$  is a positive measure over (single-trial) probabilities.

- “Probability distribution over probabilities” replaces “unknown probability”
- Experimenter can act as if...
  - there is an objective (single-trial) probability assignment,  $P$ ,
  - yielding  $P^{\times N}$  for  $N$  repeated trials,
  - his uncertainty about  $P$  is expressed by  $\int d\mu(P)$ .

---

# Exchangeable Quantum States

- In Quantum Theory, the analogon of a probability is the *quantum state*
- In quantum tomography, one tries to measure an unknown quantum state using repeated trials on identically prepared particles.
- In the information-based interpretation of quantum mechanics, a state represents the state of knowledge of an observer.
- Again, in that interpretation, “unknown quantum state” is an oxymoron.
- Sequence of **exchangeable quantum states**  $(\rho^{(N)})_N$ :
  - State  $\rho^{(N)}$  defined over  $N$ -fold copy of Hilbert space  $\mathcal{H}^{\otimes N}$ ;
  - Every  $\rho^{(N)}$  is symmetric under permutation of copies of  $\mathcal{H}$
  - Consistency:  $\rho^{(N)} = \text{Tr}_1 \rho^{(N+1)}$

---

# The Quantum de Finetti Theorem

- Theorem (Hudson and Moody 1976; Størmer 1969):

A sequence of states  $(\rho^{(N)})_N$  is exchangeable if and only if

$$\rho^{(N)} = \int d\mu(\rho) \rho^{\otimes N},$$

where  $d\mu(\rho)$  is a positive measure over the state space of  $\mathcal{H}$ .

- Concept of “unknown state” replaced by “probability distribution over states”
- Tomographer can act as if...
  - there is an “observer-in-the-box” preparing systems in the same state  $\rho$ ,
  - yielding  $\rho^{\otimes N}$  for  $N$  repeated trials,
  - his own uncertainty about  $\rho$  is expressed by  $\int d\mu(\rho)$ .

---

Allegretto:

There, and Back Again

---

# The Plan

- Optimisation theory can help us in solving questions in quantum theory.
- It has done so before.
- It can't help us very much with the MOP:
- Not a convex problem: *maximisation* of a convex function over a convex set
- All we get from convexity theory is that the maximum will be obtained in an extreme point
- Now here is where Quantum de Finetti comes in!
- So, in return, quantum theory can offer solutions to questions in optimisation theory!

---

# Maximal Output Purity (again!)

- Consider the maximal output purity  $\nu_q$  for integer  $q$ ; then

$$\nu_q^q(\Phi) = \max_{\rho \in \mathcal{S}(\mathcal{H})} \text{Tr}[(\Phi(\rho))^q],$$

- Note that  $\text{Tr}[(\Phi(\rho))^q] = \text{Tr}[\Phi(\rho)\Phi(\rho) \dots \Phi(\rho)]$ , with  $q$  factors.
- We can write  $\text{Tr}[(\Phi(\rho))^q] = \text{Tr}[A\rho^{\otimes q}]$ , with

$$A_{(i),(j)} = \text{Tr}[\Phi_{i_1, j_1} \dots \Phi_{i_q, j_q}],$$

where  $\Phi$  is the Choi matrix of the map  $\Phi$ .

---

# Symmetry

- Consider permutations of  $n$  copies of  $\mathcal{H}$ .
- If, for every permutation  $\pi \in S_n$ , a matrix  $A$  over  $\mathcal{H}^{\otimes n}$  obeys

$$A_{(i_1, \dots, i_q), (j_1, \dots, j_q)} = A_{(i_{\pi(1)}, \dots, i_{\pi(q)}), (j_{\pi(1)}, \dots, j_{\pi(q)})},$$

then the matrix  $A$  is *symmetric*.

- Let  $P_\pi$  be a permutation matrix, permuting indices according to  $\pi$ , i.e.  $(P_\pi x)_{(i)} = x_{\pi(i)}$ .
- Thus  $A$  is symmetric if and only if  $\forall \pi \in S_n, P_\pi^\dagger A P_\pi = A$ .
- The linear map  $P_n$  that projects all operators to the symmetric subspace is

$$P_n(A) = \frac{1}{n!} \sum_{\pi \in S_n} P_\pi^\dagger A P_\pi.$$

We call  $P_n(A)$  the *symmetric part* of  $A$ .

---

---

# Another Main Theorem

Using the QdF theorem we can prove:

**Theorem 3** *For any  $q, n \in \mathbb{N}$ , and for any operator  $A$  over  $\mathcal{H}^{\otimes q}$  with Hermitian symmetric part, the sequence  $(\mu_n(A))_n$ , with*

$$\mu_n(A) := \lambda_{\max}(\mathbf{P}_{q+n}(A \otimes \mathbf{I}^{\otimes n})),$$

*is non-increasing and converges to*

$$\lim_{n \rightarrow \infty} \mu_n(A) = \max_{\rho} \text{Tr}[A\rho^{\otimes q}].$$

---

# Proof of Theorem (I)

- We want to maximise  $\text{Tr}[A\rho^{\otimes q}]$  over all states  $\rho$ .
- First turn this into the more general optimisation problem

$$\max_{d\mu(\rho) \geq 0} \left\{ \text{Tr} \left[ A \int \rho^{\otimes q} d\mu(\rho) \right] : \int d\mu(\rho) = 1 \right\}$$

(going to convex combinations does not change the maximum).

- The QdF Theorem says that a state is the  $q$ -th element from an exchangeable sequence if and only if it is of the form  $\int \rho^{\otimes q} d\mu(\rho)$ .
- Hence, we can replace the above maximisation by a maximisation of  $\text{Tr}[A\rho^{(q)}]$  over all  $\rho^{(q)}$  that are  $q$ -th element in some exchangeable sequence.

---

## Proof of Theorem (II)

From the definition of exchangeable sequence, we infer that  $\rho^{(q)}$  must be the partial trace of a symmetric state  $\rho^{(\infty)}$  over  $\mathcal{H}^{\otimes \infty}$ , where all but  $q$  copies of  $\mathcal{H}$  have been traced out.

$$\begin{aligned} \max_{\rho} \text{Tr}[A\rho^{\otimes q}] &= \max_{\rho^{(q)}} \text{Tr}[A\rho^{(q)}] \\ &= \lim_{n \rightarrow \infty} \max_{\rho} \{ \text{Tr}[A \text{Tr}_n \rho] : \rho \text{ symmetric over } \mathcal{H}^{\otimes (q+n)} \} \\ &= \lim_{n \rightarrow \infty} \max_{\rho} \{ \text{Tr}[(A \otimes \mathbf{I}^{\otimes n}) \rho] : \rho \text{ symmetric over } \mathcal{H}^{\otimes (q+n)} \} \\ &= \lim_{n \rightarrow \infty} \max_{\rho} \text{Tr}[(A \otimes \mathbf{I}^{\otimes n}) \mathbf{P}_{q+n}(\rho)] \\ &= \lim_{n \rightarrow \infty} \max_{\rho} \text{Tr}[\mathbf{P}_{q+n}(A \otimes \mathbf{I}^{\otimes n}) \rho] \\ &= \lim_{n \rightarrow \infty} \lambda_{\max}(\mathbf{P}_{q+n}(A \otimes \mathbf{I}^{\otimes n})). \end{aligned}$$

---

## Proof of Theorem (III)

- We still have to show that  $\mu_n(A)$  is non-increasing with  $n$ .
- To do so, we use the convexity of  $\lambda_{\max}$ :

$$\begin{aligned}\mu_{n+1}(A) &= \lambda_{\max}(\mathbf{P}_{q+n+1}(A \otimes \mathbf{I}^{\otimes(n+1)})) \\ &= \lambda_{\max}(\mathbf{P}_{q+n+1}(\mathbf{P}_{q+n}(A \otimes \mathbf{I}^{\otimes n}) \otimes \mathbf{I})) \\ &\leq \frac{1}{(q+n+1)!} \sum_{\pi \in S_{q+n+1}} \lambda_{\max}(P_{\pi}^{\dagger}(\mathbf{P}_{q+n}(A \otimes \mathbf{I}^{\otimes n}) \otimes \mathbf{I})P_{\pi}) \\ &= \lambda_{\max}(\mathbf{P}_{q+n}(A \otimes \mathbf{I}^{\otimes n}) \otimes \mathbf{I}) \\ &= \lambda_{\max}(\mathbf{P}_{q+n}(A \otimes \mathbf{I}^{\otimes n})) \\ &= \mu_n(A).\end{aligned}$$

- This finishes the Proof.

---

# Coda

- Algorithmic issues: with some more symmetry theory, we get a modestly efficient algorithm that calculates **guaranteed** upper bounds and has no problems at all with local maxima!
- See [quant-ph/0402076](#) for more details than you'd care for
- There might be more in store here; e.g. Duality for non-convex problems?
- Theoretical Issues: reduces a difficult optimisation problem to an eigenvalue problem
- This might be just the simplification needed for tackling additivity
- (Watch out for forthcoming stuff on ArXiv)