
Quantum Information Theory: An Invitation

Koenraad M.R. Audenaert

University of Wales
Llanfairpwllgwyngyllgogerychwyrndrobwlllantysiliogogoch

December 14, 2003

Part 1: Quantum Information Theory

Quantum Mechanics I: States

- Quantum Mechanics (QM) is the physical theory of the microworld of particles.
- In Quantum Mechanics, everything is *linear* and *positive*!
- Properties of quantum systems (e.g. particles) are described by *states*.
- States are positive semidefinite matrices (PSD) with trace 1. Reason: their eigenvalues must form a probability distribution.
 - Rank 1 states are called *pure* states. Their eigenvector is the *state vector*, known from undergraduate quantum mechanics.
 - Rank > 1 states are called *mixed* states, because they correspond to statistical mixtures of pure states.

Quantum Mechanics II: Operations

- Actions on states are described by *operations*.
- Operations are represented by matrices. Reason: QM is linear.
- Moreover, these matrices are also PSD. Reason: states must be mapped on states, hence operations must be positivity-preserving.
- The matrix representing an operation is sometimes called the Choi matrix.

Quantum Information Theory

- Quantum Information Processing (QIP) is about exploiting QM features in all facets of information processing (data communication, computing).
- The information carriers are the states, the channels are the operations.
- Quantum Information Theory (QIT) is the underlying theory, a halfbreed of Information Theory and Quantum Mechanics (“Shannon meets von Neumann”).
- QIT typically considers multiple particles, potentially widely separated.
- The most amazing thing in QM is that, in general, the particles in a group do not have a state of their own, only the group has. This is called *entanglement*.
- In QIP we try to exploit entanglement as a novel resource.

Entanglement

- The state of a group of *independent* particles is the tensor product of the individual particles' states. $\rho = \rho_1 \otimes \rho_2 \otimes \dots \otimes \rho_n$. This is called a *product state*.
- Statistical mixtures of product states are called *separable states*:

$$\rho = \sum_k p_k \rho'_k \otimes \rho''_k.$$

- All other states are entangled states. Most states in Nature are entangled.
- In QIT, we try to find ways to characterise when and how much a state is entangled.
- The first problem is called the separability problem (cfr. Previous talk by Hugo Woerdeman), the second problem is the study of entanglement measures.

Some Notations

- States ρ, σ , are trace 1 positive operators over a Hilbert space \mathcal{H} . We consider finite-dimensional spaces only (qubits, qutrits, ...).
- States of two-particle systems are called bipartite states, defined over a tensor product space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$.
- Bipartite states are represented by block matrices $\in M_{d_A}(M_{d_B}(\mathbb{C}))$. They have two pairs of indices: $\rho_{k,l}^{i,j}$.
- Operations are operators over the tensor product space $\mathcal{H}_{in} \otimes \mathcal{H}_{out}$. Their Choi matrices also have two pairs of indices. For an operation $\Omega : \rho \mapsto \rho' = \Omega(\rho)$:

$$\rho'_{i,j} = \sum_{k,l} \text{Choi}(\Omega)_{k,l}^{i,j} \rho_{k,l}.$$

Why am I telling you this?

- The basic mathematical entities in QIT are positive block matrices.
- One might guess that Matrix Analysis could be one of the main tools.
- Indeed, in QIT much use has been found for:
 - eigenvalue and singular value decompositions
 - eigenvalue and singular value inequalities
 - matrix norms
 - majorisation
 - matrix inequalities
- For some open problems: please, send more Matrix Analysis!

Part 2: An Open Problem

Maximal Output Purity of Channels

- In general, if an operation acts on a pure state, the output will be a mixed state.
- The *maximal output purity* (MOP), ν_q , of an operation or channel quantifies how close to purity one can get by choosing the input state. As a measure of purity, the Schatten q -norm is used:

$$\nu_q(\Omega) = \max_{\psi} \{ \|\Omega(\psi\psi^*)\|_q : \|\psi\| = 1 \}.$$

- There is also an entropic version: the *minimal output entropy* (MOE), ν_S , where the von Neumann entropy $S(\rho) = -\text{Tr}[\rho \log(\rho)]$ is used as a measure of purity.

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

Additivity Problems

- Proving additivity of the classical capacity of a quantum channel is still an open problem in QIT after three decades (Holevo).
- Shor proved that this problem is equivalent to additivity of MOE: $\nu_S(\Phi \otimes \Omega) = \nu_S(\Phi) + \nu_S(\Omega)$.
- Additivity of MOE would follow from multiplicativity of MOP for small q (Amosov, Holevo and Werner): $\nu_q(\Phi \otimes \Omega) = \nu_q(\Phi)\nu_q(\Omega)$.
- It is trivial to show $\nu_q(\Phi \otimes \Omega) \geq \nu_q(\Phi)\nu_q(\Omega)$. Indeed, this follows by restricting the maximisation over state vectors ψ for $\nu_q(\Phi \otimes \Omega)$ to ψ of the form $\psi = \psi' \otimes \psi''$.
- The opposite inequality would follow from a conjectured inequality by King.
- Matrix Analysis might be the key to solving this problem...

King's Conjecture

- Let ρ be a bipartite state on $\mathcal{H}_1 \otimes \mathcal{H}_2$ and Ω be a CP map operating on \mathcal{H}_2 , then *King's Inequality* reads:

$$\|(\mathbf{I} \otimes \Omega)(\rho)\|_q \leq \nu_q(\Omega) \sum_{i=1}^{d_2} \|\rho_{ii}\|_q.$$

- From it, multiplicativity of MOP follows easily. Put $\rho = (\Phi \otimes \mathbf{I})(\sigma)$, then

$$\begin{aligned} \|(\Phi \otimes \Omega)(\sigma)\|_q &\leq \nu_q(\Omega) \sum_i \|((\Phi \otimes \mathbf{I})(\sigma))_{ii}\|_q \\ &= \nu_q(\Omega) \sum_i \|\Phi(\sigma_{ii})\|_q = \nu_q(\Omega) \sum_i \text{Tr}[\sigma_{ii}] \|\Phi(\sigma_{ii}/\text{Tr}[\sigma_{ii}])\|_q \\ &\leq \nu_q(\Omega) \sum_i \text{Tr}[\sigma_{ii}] \nu_q(\Phi) = \nu_q(\Omega) \nu_q(\Phi). \end{aligned}$$

Known Cases of King's Conjecture 1

- The *half-noisy channel*: $\Omega = \mathbf{I}$, i.e. $\Omega(\rho) = \rho$.
- Since $\nu_q(\Omega) = 1$, King's Inequality becomes:

$$\|\rho\|_q \leq \sum_i \|\rho_{ii}\|_q.$$

- Proof of validity: In Problem 22 of R.A. Horn and C.R. Johnson, *Topics in Matrix Analysis*, p. 217, the reader has to show that this inequality holds for any unitarily invariant norm.
- Application: In this case, we can show that

$$\nu_q(\Phi \otimes \mathbf{I}) = \nu_q(\Phi).$$

- This was first proven by Amosov, Holevo and Werner (in a different way).

Known Cases of King's Conjecture 2

- $\Omega(\rho) = A\rho A^*$, i.e. the Choi matrix of Ω is rank 1.
- We first calculate $\nu_q(\Omega)$:

$$\begin{aligned}\nu_q(\Omega) &= \max_{\psi} \{ \|A\psi\psi^*A^*\|_q : \|\psi\| = 1 \} \\ &= \max_{\psi} \{ \text{Tr}[A\psi\psi^*A^*] : \|\psi\| = 1 \} \\ &= \max_{\psi} \{ (\psi, A^*A\psi) : \|\psi\| = 1 \} = \|A\|_{\infty}^2.\end{aligned}$$

- Then, using the Lieb-Thirring inequality,

$$\begin{aligned}\|(\mathbf{I} \otimes \Omega)(\rho)\|_q &= (\text{Tr}[\mathbf{I} \otimes A \cdot \rho \cdot \mathbf{I} \otimes A^*]^q)^{1/q} \\ &\leq (\text{Tr}[(\mathbf{I} \otimes A^*A)^q \cdot \rho^q])^{1/q} \\ &\leq \|A\|_{\infty}^2 \|\rho\|_q = \nu_q(\Omega) \|\rho\|_q.\end{aligned}$$

- Since $\|\rho\|_q \leq \sum_i \|\rho_{ii}\|_q$, this is stronger than King's inequality.

Known Cases of King's Conjecture 3

- ρ is a pure state; i.e. it is rank 1.
- Using the Horn&Johnson inequality again:

$$\begin{aligned}\|(\mathbf{I} \otimes \Omega)(\rho)\|_q &\leq \sum_j \|((\mathbf{I} \otimes \Omega)(\rho))^{jj}\|_q \\ &= \sum_j \|\Omega(\rho^{jj})\|_q \\ &\leq \nu_q(\Omega) \sum_j \text{Tr}[\rho^{jj}] = \nu_q(\Omega) \text{Tr}[\rho].\end{aligned}$$

- For rank 1 states, $\sum_i \|\rho_{ii}\|_q = \sum_i \text{Tr}[\rho_{ii}] = \text{Tr}[\rho]$.

Known Cases of King's Conjecture 4

- ρ is *separable*, i.e. it is of the form $\rho = \sum_k p_k A_k \otimes B_k$.
- Proposition (essentially due to King): for separable ρ ,

$$\|\rho\|_q \leq \left\| \sum_k p_k A_k \right\|_q \max_k \|B_k\|_q.$$

- For separable ρ ,

$$\begin{aligned} \|(\mathbf{I} \otimes \Omega)(\rho)\|_q &= \left\| \sum_k p_k A_k \otimes \Omega(B_k) \right\|_q \\ &\leq \left\| \sum_k p_k A_k \right\|_q \max_k \|\Omega(B_k)\|_q \\ &\leq \left\| \sum_k p_k A_k \right\|_q \nu_q(\Omega) = \nu_q(\Omega) \|\mathrm{Tr}_2[\rho]\|_q. \end{aligned}$$

- Since $\mathrm{Tr}_2[\rho] = \sum_i \rho_{ii}$, we have $\|\mathrm{Tr}_2[\rho]\|_q \leq \sum_i \|\rho_{ii}\|_q$.

A Counterexample :-)

- Holevo and Werner found a counterexample to the multiplicativity of MOP...
- This immediately gives a counterexample to King's Conjecture. How annoying!
- When
 - \mathcal{H}_1 and \mathcal{H}_2 are both 3-dimensional,
 - $\Omega(\sigma) = \mathbf{I} \text{Tr}[\sigma] - \sigma^T$,
 - $\rho = (\Omega \otimes \mathbf{I})(\psi\psi^*)$, with $\psi = \sum_i e^i \otimes e^i$,
 - $q > 4.79$,

King's inequality is violated.

- However, it might still hold for smaller q . Maybe for $1 \leq q \leq 2$?
- If it holds for $1 \leq q \leq q_0$, some q_0 , we're saved.

Conclusion

- King's Conjecture is only one of a host of open problems in QIT.
- The entities central to QIT are also central to Matrix Analysis.
- MA has been used to solve problems in QIT in the past.
- Can MA provide answers towards solving the open problems?
- In turn, can these problems provide novel questions to MA?
- Consider this talk as an invitation!
- P.S.: suggestions for proving King's Inequality are kindly accepted after the talk.