Operational Insights from Quantum Shannon Theory

Holger Boche

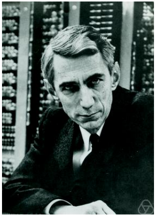
(joint work with G. Janßen)

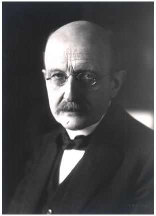
Lehrstuhl für Theoretische Informationstechnik
Technische Universität München

May 3rd, 2016

Claude Elwood Shannon 100th Birthday Celebration
Heinz Nixdorf Museum, Paderborn

Two Major Theories of the 20th Century

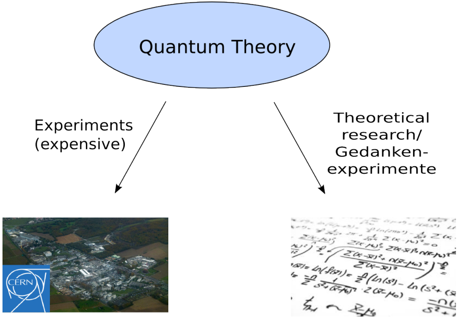




- The names **Claude Elwood Shannon** and **Max Planck** stand for two of the most fascinating theories of the 20th century.
- Quantum Shannon Theory is a combination of Shannon's theory of communication with the structure of quantum theory, and has developed into a mature theory in the last two decades.
- Research activities in Quantum Shannon Theory add fruitful insights to Classical Information Theory and Quantum Theory

A fruitful Connection

- The development of quantum theory raised several puzzling philsophical questions.
- Quantum Shannon theory besides its practical relevance is also a playground for thought experiments - Gedankenexperimente.
- In some cases, Shannon theoretical treatment of quantum communication tasks provides deep insights to aspects of the theory.



Classical and Quantum IT - Dictionary of Correspondences

Classical Theory	Quantum Theory
Alphabet $\mathcal{X}$	Hilbert space $\mathcal{H}$
Probability distribution $p \in \mathfrak{P}(\mathcal{X})$	Quantum state / Density matrix, $\rho \in \mathcal{L}(\mathcal{H}),\ \rho$ p.s.d, $\mathrm{tr}\rho = 1$
Shannon entropy $H(X)$	von Neumann entropy $S(\rho) := -\mathrm{tr}(\rho \log \rho)$
Conditional Shannon entropy $H(X\|Y) := H(XY) - H(Y)$	Conditional von Neumann entropy $S(A\|B) := S(\rho_{AB}) - S(\rho_B)$
Classical channel stochastic map $W : \mathcal{X} \to \mathfrak{P}(\mathcal{Y})$	Quantum channel completely positive & trace preserving map $\mathcal{N} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{K})$, c.p.t.p, $\mathrm{tr}(\mathcal{N}(x)) = \mathrm{tr}(x) \quad \forall x$

Example: Negativity of Conditional von Neumann Entropies

- **Observation in Quantum Theory**: For some bipartite states ρ_{AB}

$$S(A|B) < 0$$

  holds, while $H(X|Y) \geq 0$ for all pairs (X, Y) of classical random variables.

- **Question**: What is the meaning of negativity of $S(A|B)$?

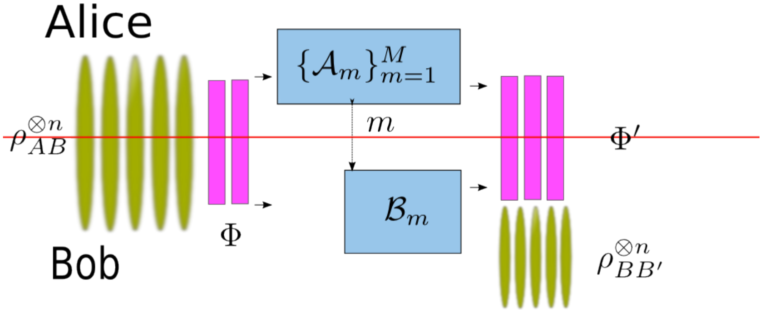
- Hordecki, Horodecki [**Phys. Lett. A 194** (1994)]:

$$S(A|B) > 0 \Rightarrow \rho_{AB} \text{ classically correlated.}$$

- A meaningful answer to the above question was given in the framework of quantum Shannon theory

Quantum State Merging - Task

- Quantum state merging introduced by Horodecki, Oppenheim and Winter [**Nature 436** (2005)], gives insight to the question of negativity of $S(A|B)$.
- **Task:** Recover the statistics of a bipartite memoryless quantum source with state ρ_{AB} completely on systems of party B.
- **Resources:** Local Operations and $A \to B$ Classical Communication (LOCC) together with help of maximally entangled qubit pairs.



Question: What is the optimal rate of maximally entangled qubit pairs for perfect merging of the quantum state ρ?

Local Operations and Classical Communication: $A \to B$ One-Way LOCC

We consider bipartite systems with communication parties A and B, which process systems on Hilbert spaces e.g. $\mathcal{H}_A \otimes \mathcal{H}_B$.

The protocols which are used in this contribution are of the following type:

$$\mathcal{T}(x) := \sum_{k=1}^{D} \mathcal{A}_k \otimes \mathcal{B}_k(x) \qquad (x \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B))$$

where

- $\{\mathcal{A}_k\}_{k=1}^{D}$ is a Quantum instrument, i.e.
  - $\mathcal{A}_k$ is completely positive and trace-nonincreasing for each $1 \leq k \leq D$
  - $\sum_{k=1}^{D} \mathcal{A}_k$ is a quantum channel
- $\mathcal{B}_k$ is a quantum channel for each $1 \leq k \leq D$.
- D is the number of different classical messages communicated $A \to B$ within application of the protocol.

Quantum State Merging - Definitions

- A **quantum state merging protocol** is a map

$$\mathcal{M} : \mathcal{L}(\mathcal{H}_{AB} \otimes \mathcal{K}_{AB}) \rightarrow \mathcal{L}(\mathcal{H}_{BB'} \otimes \mathcal{K}'_{AB}),$$

  of the one-way LOCC type.

  $\mathcal{H}_{AB} \simeq \mathcal{H}_{BB'}$: Hilbert spaces of the source state.

  $\mathcal{K}_{AB}$, $\mathcal{K}'_{AB}$: Hilbert spaces of the input/output entanglement resources.

- **Performance** of a quantum state merging protocol $\mathcal{M}$ applied on a state ρ_{AB} is quantified by the merging fidelity

$$F_m(\rho_{AB}, \mathcal{M}, \Phi, \Phi') := F(\mathcal{M} \otimes \mathrm{id}_E(\Phi \otimes \Psi_{ABE}), \Phi' \otimes \Psi_{BB'E})$$

  where F is the generalized transition probability (quantum Fidelity).

  Ψ : "Purification" of ρ_{AB}.

  Φ, Φ' : Input/output maximally entangled resource states.

Quantum State Merging - Achievable Rates, Merging Cost

Definition

A number $R \in \mathbb{R}$ is an achievable entanglement rate for quantum state merging of ρ_{AB}, if there is a sequence $\{\mathcal{M}_n\}_{n=1}^{\infty}$ if one-way LOCC channels, such that

1. $\liminf_{n\to\infty} F_m(\rho_{AB}^{\otimes n}, \mathcal{M}_n, \Phi_n, \Phi'_n) = 1$
2. $\limsup_{n\to\infty} \frac{1}{n}(\log(sr(\Phi_n) - \log(sr(\Phi'_n))) \leq R$,

where $sr(\Phi)$ is the "Schmidt rank" of the maximally entangled resource state Φ.

Definition

The $A \to B$ merging cost $C_{m,\to}(\rho_{AB})$ of ρ_{AB} is defined

$$C_{m,\to}(\rho_{AB}) := \inf\{R : \ R \text{ achievable entanglement rate for merging of } \rho_{AB}\}.$$

Quantum State Merging - Result

The optimal asymptotical average cost of entangled qubit pairs for quantum state merging was determined by Horodecki, Oppenheim, and Winter [**Comm. Math. Phys. 269** (2007)]

Theorem

Let ρ_{AB} be a density matrix on $\mathcal{H}_A \otimes \mathcal{H}_B$. It holds

$$C_{m,\rightarrow}(\rho_{AB}) = S(A|B, \rho_{AB}).$$

Interpretation - Quantum partial information

- The quantum state merging theorem allows an **operational interpretation** of the conditional von Neumann entropy.

- $S(A|B)$ quantifies the information B has about the whole state.

- Negative values of $S(A|B)$ have a clear meaning: If negative rates are achieved in quantum state merging, entanglemrnt resources can be generated by state merging protocols.

- Some states have negative "partial information".

State Merging in Quantum Shannon Theory

- Quantum state merging is a communication primitive in quantum Shannon theory.
- Protocols for quantum state merging can be used to establish protocols for e.g. entanglement distillation, entanglement transmission, distributed compression, and coding of quantum multiple-access channels.
- Are a basis for secret-key distillation protocols.
- Further developments: Design of protocols for the mentioned tasks in non-ideal communication systems e.g.
  - Compound memoryless quantum sources and channels
  - Arbitrarily varying sources/channels

Shannon's ideas have essential impact on communication
and
quantum theory of the 21th century

References

1. M. Horodecki, J. Oppenheim, A. Winter: "Partial quantum information",
Nature 436, 673–676 (2005).

2. M. Horodecki, J. Oppenheim, A. Winter: "Quantum State Merging and Negative Information",
Comm. Math. Phys. 269, 107–136 (2007).

3. I. Bjelaković, H. Boche, G. Janßen: "Universal quantum state merging",
J. Math. Phys. 54, 032204 (2013).

4. H. Boche, G. Janßen: "Resource Cost Results for One-Way Entanglement Distillation and State Merging of Compound and Arbitrarily Varying Quantum Sources",
J. Math. Phys. 55, 1-27 (2014).

5. H.Boche, G. Janßen: "Distillation of secret key from a class of compound memoryless quantum sources",
Preprint: arXiv:1604.05530