Channels inclusion, falsification, and verification

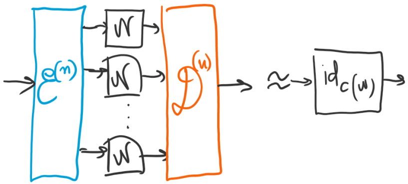
Francesco Buscemi[1]
in coll. with: S. Brandsen, M. Dall'Arno, Y.-C. Liang, D. Rosset, V. Vedral

QCQIP 2017, Chinese Academy of Sciences, Beijing, 14 November 2017

[1] Dept. of Mathematical Informatics, Nagoya University, buscemi@i.nagoya-u.ac.jp

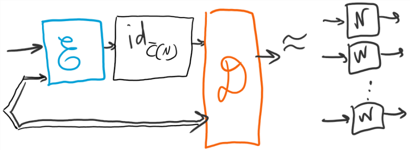
Direct and Reverse Shannon Theorems

Direct Shannon Coding



direct capacity $C(\mathcal{N})$

Reverse Shannon Coding



reverse capacity $\overline{C}(\mathcal{N})$

Bennett, Devetak, Harrow, Shor, Winter (circa 2007-2014)

For a classical channel $\mathcal{N}$, when shared randomness is free,
$C(\mathcal{N}) = \overline{C}(\mathcal{N})$.

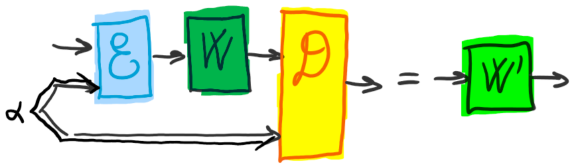
Shannon's noisy channel coding theorem is a statement about asymptotic simulability.

Shannon's "Channel Inclusion"

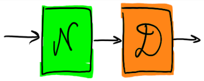
As a single-shot, zero-error analogue, Shannon, in *A Note on a Partial Ordering for Communication Channels* (1958), defines an exact form of simulability that he names "inclusion."

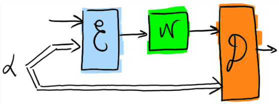
Definition (Inclusion Ordering)

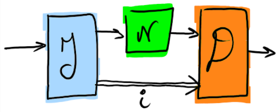
Given two classical channels $\mathrm{W} : \mathcal{X} \to \mathcal{Y}$ and $\mathrm{W}' : \mathcal{X}' \to \mathcal{Y}'$, we write $\mathrm{W} \supseteq \mathrm{W}'$ if there exist encodings $\{\mathcal{E}_\alpha\}_\alpha$, decodings $\{\mathcal{D}_\alpha\}_\alpha$, and a probability distribution μ_α such that $\mathrm{W}' = \sum_\alpha \mu_\alpha(\mathcal{D}_\alpha \circ \mathrm{W} \circ \mathcal{E}_\alpha)$.



"Simulability" Orderings







Degradability	**Shannon's Inclusion**	**Quantum Inclusion**
$\mathcal{N} \to \mathcal{N}'$	$\mathcal{N} \supseteq \mathcal{N}'$	$\mathcal{N} \supseteq_{\mathrm{q}} \mathcal{N}'$
$\exists \mathcal{D}$: CPTP such that $\mathcal{N}' = \mathcal{D} \circ \mathcal{N}$	$\exists \{\mathcal{E}_\alpha\}_\alpha, \{\mathcal{D}_\alpha\}_\alpha$: CPTP and μ_α : prob. dist. such that $\mathcal{N}' = \sum_\alpha \mu_\alpha (\mathcal{D}_\alpha \circ \mathcal{N} \circ \mathcal{E}_\alpha)$	$\exists \{\mathscr{I}^i\}_i$: CP instrument and $\{\mathcal{D}_i\}_i$: CPTP such that $\mathcal{N}' = \sum_i (\mathcal{D}_i \circ \mathcal{N} \circ \mathscr{I}^i)$

- for degradability, the two channels need to have the same input system; the two inclusion orderings allow to modify both input and output
- $\mathcal{N} \to \mathcal{N}' \implies \mathcal{N} \supseteq \mathcal{N}' \implies \mathcal{N} \supseteq_{\mathrm{q}} \mathcal{N}'$ (all strict implications)
- the "quantum inclusion" ordering $\supseteq_{\mathrm{q}}$ allows unlimited free classical forward communication: it is non-trivial only for quantum channels

Shannon's Coding Ordering

In the same paper, Shannon also introduces the following:

Definition (Coding Ordering)

Given two classical channels $\mathsf{W} : \mathcal{X} \to \mathcal{Y}$ and $\mathsf{W}' : \mathcal{X}' \to \mathcal{Y}'$, we write $\mathsf{W} \gg \mathsf{W}'$ if, for any (M, n) code for W' and any choice of prior distribution π_i on codewords, there exists an (M, n) code for W with average error probability $P_e = \sum_i \pi_i \lambda_i \leq P'_e = \sum_i \pi_i \lambda'_i$.

Note: here λ_i denotes the conditional probability of error, given that index i was sent.

Fact

$\mathsf{W} \supseteq \mathsf{W}' \implies \mathsf{W} \gg \mathsf{W}' \implies C(\mathsf{W}) \geq C(\mathsf{W}')$

The above definition and theorem can be directly extended to quantum channels and their classical capacity.

Other "Coding" Orderings

From: J. Körner and K. Marton, *The Comparison of Two Noisy Channels*. Topics in Information Theory, pp.411-423 (1975)

Definition (Capability and Noisiness Orderings)

Given two classical channels $\mathsf{W} : \mathcal{X} \to \mathcal{Y}$ and $\mathsf{W}' : \mathcal{X} \to \mathcal{Z}$, we say that

1. W is more capable than W′ if, for any input random variable X, $H(X|Y) \leq H(X|Z)$
2. W is less noisy than W′ if, for any pair of jointly distributed random variables (U, X), $H(U|Y) \leq H(U|Z)$

Theorem (Körner and Marton, 1975)

It holds that

$$\textit{degradable} \implies \textit{less noisy} \implies \textit{more capable},$$

and all implications are strict.

Reverse Data-Processing Theorems

- two kinds of orderings: **simulability orderings** (degradability, Shannon inclusion, quantum inclusion) and **coding orderings** (Shannon coding ordering, noisiness and capability orderings)
- simulability orderings $\Longrightarrow$ coding orderings: data-processing theorems
- coding orderings $\Longrightarrow$ simulability orderings: reverse data-processing theorems

Why Reverse Data-Processing Theorems Are Relevant

- role in statistics: majorization, comparison of statistical models (Blackwell's sufficiency and Le Cam's deficiency), asymptotic statistical decision theory
- role in physics, esp. quantum theory: channels describe physical evolutions; hence, reverse-data processing theorems allow the reformulation of statistical physics in information-theoretic terms
- applications so far: quantum non-equilibrium thermodynamics; quantum resource theories; quantum entanglement and non-locality; stochastic processes and open quantum systems dynamics

Channels Inclusion(s), Falsification, and Verification

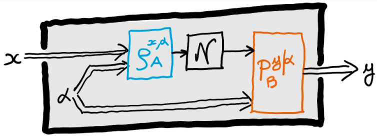
(Two Possible) Quantum Inclusion Orderings

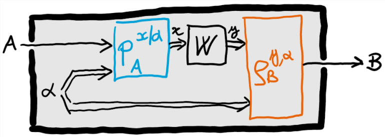
Definition (Q-to-C Inclusion)

For a given CPTP map $\mathcal{N} : \mathsf{L}(\mathcal{H}_A) \to \mathsf{L}(\mathcal{H}_B)$, we denote by $S_{\mathcal{X}\to\mathcal{Y}}(\mathcal{N})$ the set of all classical channels $\mathsf{W} : \mathcal{X} \to \mathcal{Y}$ such that $\mathsf{W}(y|x) = \sum_\alpha \mu_\alpha \operatorname{Tr}[\mathcal{N}(\rho_A^{x,\alpha})\ P_B^{y|\alpha}]$, where $\{\rho_A^{x,\alpha}\}_{x,\alpha}$ are normalized states and $\{P_B^{y|\alpha}\}_\alpha$ POVMs.

Definition (C-to-Q Inclusion)

For a given classical channel $\mathsf{W} : \mathcal{X} \to \mathcal{Y}$, we denote by $S_{A\to B}(\mathsf{W})$ the set of all CPTP maps $\mathcal{N} : \mathsf{L}(\mathcal{H}_A) \to \mathsf{L}(\mathcal{H}_B)$ such that $\mathcal{N}(\bullet_A) = \sum_{\alpha,x} \mu_\alpha \rho_B^{y,\alpha}\ \mathsf{W}(y|x) \operatorname{Tr}[\bullet_A\ P_A^{x|\alpha}]$, where $\{\rho_B^{y,\alpha}\}_{y,\alpha}$ are normalized states and $\{P_A^{x|\alpha}\}_\alpha$ POVMs.





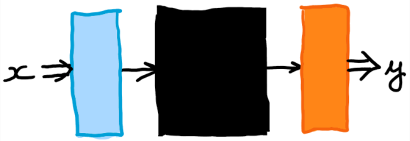
Falsification

To provide experimental evidence for $\exists \mathsf{W}$ such that $\mathsf{W} \notin S(\mathcal{N})$

Verification

To provide experimental evidence for $\nexists\, \mathsf{W}$ such that $\mathcal{N} \in S(\mathsf{W})$

Channel Falsification: The Task



- A memory is thought of as a black-box with one input (classical or quantum) and one output (classical or quantum)
- Some hypothesis is made about the black-box, that is, a description of it in terms of a channel $\mathcal{N}$

While it is impossible to verify the hypothesis $\mathcal{N}$ in a device-independent way, it is possible to *falsify* it: if a correlation $p(y|x) \notin S_{\mathcal{X}\to\mathcal{Y}}(\mathcal{N})$ is observed, the hypothesis $\mathcal{N}$ is falsified in a device-independent way.

Example: Dimension Falsification

Problem: how to give a lower bound on the dimension of a memory by observing input/output classical correlations?

Question

Are d-dimensional classical identity id_d^c and d-dimensional quantum identity id_d^q distinguishable in this basic setting?

Equivalently stated, is there a correlation $p(y|x)$ able to falsify id_d^c but not id_d^q?

Theorem (P.E. Frenkel and M. Weiner, CMP, 2015)

No: the identity $S_{\mathcal{X}\to\mathcal{Y}}(\mathrm{id}_d^c) = S_{\mathcal{X}\to\mathcal{Y}}(\mathrm{id}_d^q)$ holds for all choices of alphabets $\mathcal{X}$ and $\mathcal{Y}$.

Remark. Strongest generalization of Holevo theorem for static quantum memories.

Other Results

More generally, what can one say about the structure of $S_{\mathcal{X}\to\mathcal{Y}}(\mathcal{N})$, for an arbitrary channel $\mathcal{N}$?

- qubit c-q channels: closed analytical form, when $\mathcal{Y} = \{0, 1\}$ [Dall'Arno, 2017]
- qubit q-c channels (POVMs): closed analytical form in general [Dall'Arno, Brandsen, FB, Vedral, 2017]
- general channels: closed form for a large class of qubit channels (including amplitude damping) and d-dimensional universally covariant channels, when $\mathcal{Y} = \{0, 1\}$ [Dall'Arno, Brandsen, FB, 2017]

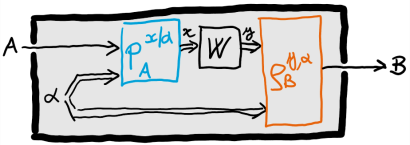
Little Corollary About Shannon's Orderings

Given a quantum channel $\mathcal{N} : A \to B$ and a classical testing channel $\mathsf{W} : \mathcal{X} \to \mathcal{Y} \equiv \{0, 1\}$,

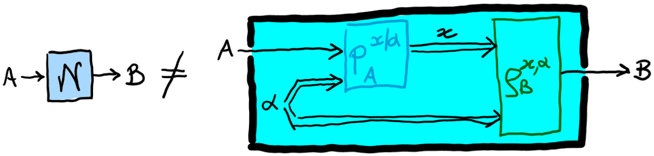
$$\mathcal{N} \supseteq \mathsf{W} \iff \mathcal{N} \gg \mathsf{W} .$$

Quantum Channel Verification: The Task

The "complementary" problem to falsification is that of *quantum channel verification*: how to verify that $\nexists$ W such that $\mathcal{N} \in S(\mathrm{W})$?



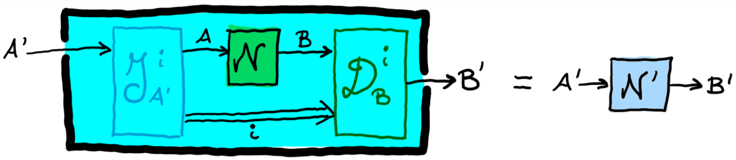
Since in the above scheme W can be any classical channel, i.e., one-way cc is free, channel verification here amounts to verify that the given channel $\mathcal{N} : \mathsf{L}(\mathcal{H}_A) \to \mathsf{L}(\mathcal{H}_B)$ is not entanglement-breaking.



Remark: from now on, we consider that α is included in x.

Quantum Inclusion

We are naturally led to consider a resource theory of quantum memories, in which resources are quantum channels and free operations are pre/post-processings assisted by one-way classical communication.



Definition

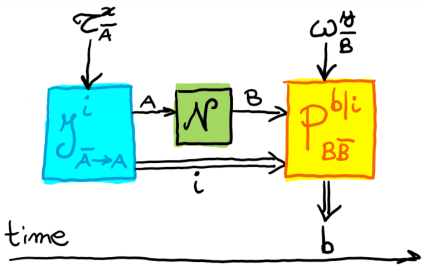
Given two CPTP maps $\mathcal{N} : A \to B$ and $\mathcal{N}' : A' \to B'$, we write $\mathcal{N} \supseteq_{\mathrm{q}} \mathcal{N}'$ whenever there exists a CP instrument $\{\mathscr{I}^i_{A' \to A}\}$ and a family of CPTP maps $\{\mathcal{D}^i_{B \to B'}\}$ such that

$$\mathcal{N}' = \sum_i \mathcal{D}^i \circ \mathcal{N} \circ \mathscr{I}^i$$

Question: what is the *operational* counterpart of the quantum inclusion ordering?

Semiquantum Signaling Games

A semiquantum signaling game is a tuple $\mathbb{G} = [\mathcal{X}, \mathcal{Y}, \mathcal{B}, \{\tau^x_{\bar{A}}\}, \{\omega^y_{\bar{B}}\}, \wp(x,y,b)]$:



- the referee picks an $x \in \mathcal{X}$ and gives $\tau^x_{\bar{A}}$ to Alice
- Alice does something on it and is able to store as much classical information as she likes
- the referee then picks a $y \in \mathcal{Y}$ and gives her $\omega^y_{\bar{B}}$
- the round ends with Alice outputting a classical outcome $b \in \mathcal{B}$
- Alice's computed outcome earns or costs her an amount decided by $\wp(x,y,b) \in \mathbb{R}$

Expected Channel Utility

Given the channel $\mathcal{N} : A \to B$ as a resource for Alice, its expected utility in game $\mathbb{G}$ is given by

$$\wp^*_{\mathbb{G}}(\mathcal{N}) = \max \sum_{x,y,i,b} \wp(x,y,b) \operatorname{Tr}\left\{ P^{b|i}_{B\bar{B}} \left[(\mathcal{N}_A \circ \mathscr{I}^i_{\bar{A}})(\tau^x_{\bar{A}}) \otimes \omega^y_{\bar{B}} \right] \right\} ,$$

where the max is taken over instrument $\{\mathscr{I}^i_{\bar{A}\to A}\}$ and POVMs $\{P^{b|i}_{B\bar{B}}\}_i$.

MDI Quantum Memory Verification

Theorem

For any given pair of CPTP maps $\mathcal{N} : A \to B$ and $\mathcal{N}' : A' \to B'$, $\mathcal{N} \supseteq_{\mathrm{q}} \mathcal{N}'$ if and only if $\wp^*_{\mathbb{G}}(\mathcal{N}) \geq \wp^*_{\mathbb{G}}(\mathcal{N}')$, for all semiquantum signaling games $\mathbb{G}$.

Corollary

1. All EB channels achieve the same expected payoff $\wp^{\mathrm{EB}}_{\mathbb{G}}$ in all games $\mathbb{G}$.
2. A channel $\mathcal{N}$ is not EB if and only if there exists a semiquantum signaling game $\mathbb{G}$ such that $\wp^*_{\mathbb{G}}(\mathcal{N}) > \wp^{\mathrm{EB}}_{\mathbb{G}}$.

- that is, as long as the quantum memory (channel) $\mathcal{N}$ is not EB, there exists a semiquantum signaling game capable of verifying that
- assumption: the referee trusts the preparation of states τ^x and ω^y, but that is anyway required in the time-like scenario: no fully device-independent quantum channel verification [Pusey, 2015]
- extra feature: it is possible to *quantify* the minimal dimension (Schmidt rank) of the quantum memory
- practicality, tolerance against loss, etc

Role of “reverse data-processing theorems” in statistical physics