Entropy of a classical channel

Alberta Mathematical Dialogue 2025

Takla Nateeboon

May 1, 2025

Department of Mathematics and Statistics, University of Calgary

This presentation is based on the preprint

Inevitable Negativity: Additivity Commands Negative Quantum Channel Entropy

Authors: Gilad Gour[1], Doyeong Kim[2], Takla Nateeboon[2], Guy Shemesh[1], and Goni Yoeli[1]

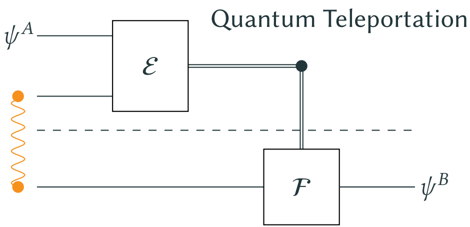
arXiv:2406.13823

1. Department of Mathematics, Technion - Israel Institute of Technology, Haifa, Israel
2. Department of Mathematics and Statistics and Institute for Quantum Science and Technology, University of Calgary, Calgary, AB, Canada

Entropy and quantum information theory

Entropy is a measure of many quantum resources

- Entanglements[1]
- Coherence[2]
- Purity[3]



Can we have an entropy for quantum channels?

← Pay 1 maximally entangled state and 2 classical bits to send a quantum bit.

[1] G. Vidal. "Entanglement monotones". In: Journal of Modern Optics 47.2-3 (2000)
[2] H. Zhu et al. "Operational one-to-one mapping between coherence and entanglement measures". In: Phys. Rev. A 96 (3 Sept. 2017)
[3] A. Streltsov et al. "Maximal coherence and the resource theory of purity". In: New Journal of Physics 20 (2018)

Can a classical channel have an entropy?

In this talk,

1. Entropies for classical state/ random variable.
2. Axiomatic definition of entropy
3. Extension of the axioms to classical channels.
4. Entropies of classical channels.

Shannon entropy and Rényi entropy

Suppose : X is discrete random variable.

It has possible value $1, 2, \dots, n$, $X(\omega) = x \in [n]$.

It has a probability mass distribution function $p(x)$.

Shannon entropy

$$H(\mathbf{p}) = -\sum_{x\in[n]} p_x \log p_x.$$

α-Rényi entropy ($\alpha \in \mathbb{R}_+$)

$$H_\alpha(\mathbf{p}) = \frac{1}{1-\alpha} \log\left(\sum_{x\in[n]} p_x^\alpha\right).$$

Denoted by $\mathbf{p}$ is an n-dimensional probability vector, $\mathbf{p} = (p(1), p(2), \dots, p(n))^T$.
Denoted by $[n]$ is a set of positive integers from 1 to n.

Entropy and uncertainty

Shannon entropy

$$H(\mathbf{p}) = -\sum_{x \in \mathcal{I}} p_x \log p_x.$$

α-Rényi entropy ($\alpha \in \mathbb{R}_+$)

$$H_\alpha(\mathbf{p}) = \frac{1}{1-\alpha} \log \left(\sum_{x \in [n]} p_x^\alpha \right).$$

The least uncertained distribution: If $\mathbf{p} = \mathbf{e}_1 = (1, 0, \ldots, 0)^T$, knowing the value of X with certainty,

$H(\mathbf{e}_1) = H_\alpha(\mathbf{e}_1) = 0.$ ← the *least* entropy can be.

The most uncertained distribution: If $\mathbf{p} = \mathbf{u}^{(n)} = \frac{1}{n}(1, 1, \ldots, 1)^T$, every outcome is equally likely,

$H(\mathbf{u}^{(n)}) = H_\alpha(\mathbf{u}^{(n)}) = \log(n).$ ← the *most* entropy can be.

Nice common properties: non-negative, additive, invariant with permutation and adding zero, quasi-concave.

Axiomatic definition of classical state entropy

Def. An entropy is a function H : ProbabilityVectors $\to \mathbb{R}_+$ such that

1. it is an antitone under majorization relation
2. it is additive under a (Kronecker) tensor products

Majorization ($\succ$) is a preorder on the set of probability vectors. It compares uncertainty of the distribution represents by the vector. E.g.

$$\mathbf{e}_1 = (1, 0, \dots, 0)^T \succ \mathbf{u}^{(n)} = \frac{1}{n}(1, 1, \dots, 1)^T.$$

Additivity under tensor product: two independent random variables $X \sim \mathbf{p}$, $Y \sim \mathbf{q}$ has a joint probability vector $\mathbf{p} \otimes \mathbf{q}$. Additivity means

$$H(\mathbf{p} \otimes \mathbf{q}) = H(\mathbf{p}) + H(\mathbf{q})$$

Majorization and uncertainty

k-game: within k guesses, correctly guess the value of a random variable X, with a known distribution.

$\mathbf{p} \succ \mathbf{q}$ is equivalent to

1. (k-game) For any $k \in [n]$, giving k guesses of an outcome drawn from $\mathbf{p}$ is more or equally likely to be correct than that of an outcome drawn from $\mathbf{q}$.

Examples,

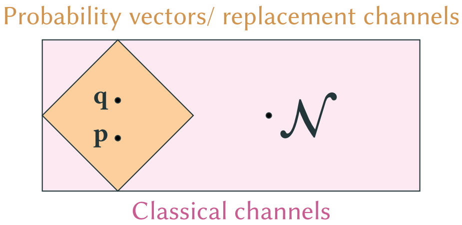
$$(1,0,0)^T \succ (\frac{2}{3}, \frac{1}{3}, 0)^T \succ (\frac{1}{2}, \frac{1}{2}, 0)^T \succ \frac{1}{3}(1,1,1)^T.$$

$(1,0,0)^T$ is called the maximal element as it *majorizes* everything.
$\frac{1}{3}(1,1,1)^T$ is called the minimal element as it *is majorized* by all vector in $\mathrm{Prob}(3)$.

Extending majorization to channels

This extended relation should reflect uncertainty inherent in classical channel,

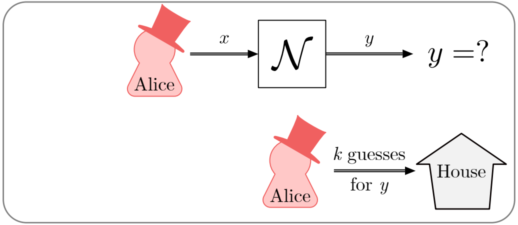
1. reduce to probability vector majorization on replacement channel,



2. have an identity channel as the maximal element,
3. have a maximally randomizing channel as the minimal

Extending game to classical channel

Goal: guess the value of the output of a channel within k guesses. The player can pick any x.

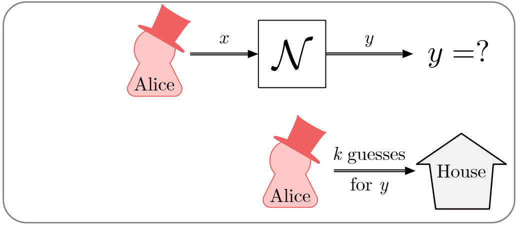


The player knows prior to giving input x

- transition matrix N associated with the channel $\mathcal{N}$ and
- k, the number of guesses.

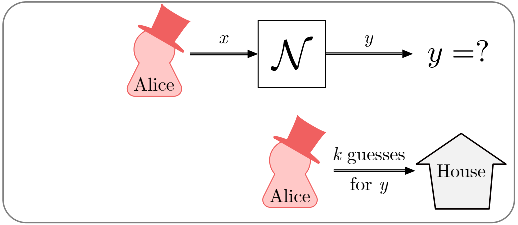
Majorization of classical channels

Goal: guess the value of the output of a channel within k guesses. The player can pick any x.



Given two classical channels $\mathcal{N}^{X\to Y}$ and $\mathcal{M}^{X\to Y}$. $\mathcal{N} \succ \mathcal{M}$ is equivalent to

1. For any k, it is more likely to win with channel $\mathcal{N}$ than the channel $\mathcal{M}$.



Given two classical channels $\mathcal{N}^{X \to Y}$ and $\mathcal{M}^{X \to Y}$. $\mathcal{N} \succ \mathcal{M}$ is equivalent to

1. For any k, it is more likely to win with channel $\mathcal{N}$ than the channel $\mathcal{M}$.

This extended relation should reflect uncertainty inherent in classical channel,

1. reduce to probability vector majorization on replacement channel,
2. have an identity channel as the maximal element, and
3. have a maximally randomizing channel as the minimal element.

Channel entropy

Definition. An entropy is a function H : ClassicalChannel $\to \mathbb{R}_+$ such that

1. it is an antitone under Channel majorization relation,

$$\mathcal{N} \succ \mathcal{M} \implies H(\mathcal{N}) \leq H(\mathcal{M}),$$

2. it is additive under a tensor product,

$$H(\mathcal{N} \otimes \mathcal{M}) = H(\mathcal{N}) + H(\mathcal{M}).$$

Existence?

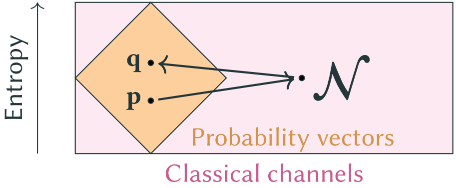
Optimal extensions of an antitone

Maximal extension: entropy of the least noisy probability vector that is still more noisy than the channel.

$$\overline{\mathbb{H}}(Y|X)_{\mathcal{N}} = \inf_{\substack{\mathbf{q}\in\mathrm{Prob}(m)\\ m\in\mathbb{N}}} \left\{\mathbb{H}(\mathbf{q}) \,:\, \mathcal{N} \succ \mathbf{q}\right\}$$

Minimal extension: entropy of the most noisy probability vector that is still less noisy than the channel.

$$\underline{\mathbb{H}}(Y|X)_{\mathcal{N}} = \sup_{\substack{\mathbf{p}\in\mathrm{Prob}(m)\\ m\in\mathbb{N}}} \left\{\mathbb{H}(\mathbf{p}) \,:\, \mathbf{p} \succ \mathcal{N}\right\}$$



Additivity of the antitone

Suppose $\mathcal{N}$ is a classical channel, $\mathbb{H}$ is a quasi-concave classical entropy, then the maximal extension of the entropy is the *min-entropy output*,

$$\overline{\mathbb{H}}(\mathcal{N}) = \min_{y\in[m]} \mathbb{H}(\mathbf{p}_y) \tag{1}$$

where $\mathbf{p}_y \stackrel{\text{def}}{=} \mathcal{N}(\mathbf{e}_y)$ and $\overline{\mathbb{H}}$ is a classical channel entropy.

α-Rényi entropies

$$H_\alpha(\mathbf{p}) = \frac{1}{1-\alpha} \log\left(\sum_{y\in[n]} p_y^\alpha\right).$$

Denoted by $\mathrm{supp}(\mathbf{p})x = \left\{ y \,:\, p_y \neq 0 \right\}$ is a set of outcomes y with non-zero probability.

$$\text{Max-entropy} \rightarrow H_0(\mathbf{p}) = \log|\mathrm{supp}(\mathbf{p})|,$$

$$\text{Shannon entropy} \rightarrow H_1(\mathbf{p}) = -\sum_{y\in[n]} p_y \log(p_y),$$

$$\text{Min-entropy} \rightarrow H_\infty(\mathbf{p}) = -\log\left(\max_{y\in[n]} p_y\right).$$

Uniqueness of the extensions

Max-entropy: $H_0(\mathbf{p}) = \log |\mathrm{supp}(\mathbf{p})|$, **Min-entropy**: $H_\infty(\mathbf{p}) = -\log\left(\max_{y\in[n]} p_y\right)$

Theorem: The extensions of max-entropy and min-entropy to be a monotone on the domain of classical channels are unique, min-entropy output.

Shannon entropy: $H_1(\mathbf{p}) = -\sum_{y\in[n]} p_y \log\left(p_y\right)$,

Theorem: Shannon entropy extends to a unique classical channel entropy, min-entropy output.

Remark: This theorem does not imply that monotone extension of Shannon entropy is unique.

Nonexample: entropy of the Choi state

Suppose that $\mathcal{N} \in \mathrm{CPTP}(X \to Y)$. We define $\mathfrak{J}_{\mathcal{N}} \in \mathfrak{L}(XY)$ to be its Choi matrix and $\hat{\mathfrak{J}}_{\mathcal{N}}$ to be the normalized Choi matrix. A function f of $\mathcal{N}$ is defined by

$$f(\mathcal{N}) = H\left(\hat{\mathfrak{J}}_{\mathcal{N}}\right) - \log(|X|)$$

where H is a von Neumann entropy. The function f is purposed to be an entropy function[1,2].

This function is not a Channel entropy.

$\mathbf{e}_1 \sim (\mathbf{e}_1, \mathbf{p})$ for any $\mathbf{p}$ being probability vector.
Their images by f are not necessary the same.

[1] J. Czartowski, D. Braun, and K. Życzkowski. "Trade-off relations for operation entropy of complementary quantum channels". International Journal of Quantum Information 17.05 (2019).
[2] Y. Chu et al. "An entropy function of a quantum channel".Quantum Information Processing 22.1 (2022)

Conclusion

We can define entropy of a classical channel axiomatically and concretely.

Axiomatically:

1. Axiomatic definition of classical state entropy and majorization.
2. Extension of majorization to classical channels.
3. Axiomatic definition of classical channel entropy follows from extended majorization.

Concretely:

1. Antitone of the extended majorization can be extended from a state entropy.
2. Additivity is not guaranteed. An α-Rényi entropy extends to a channel entropy.