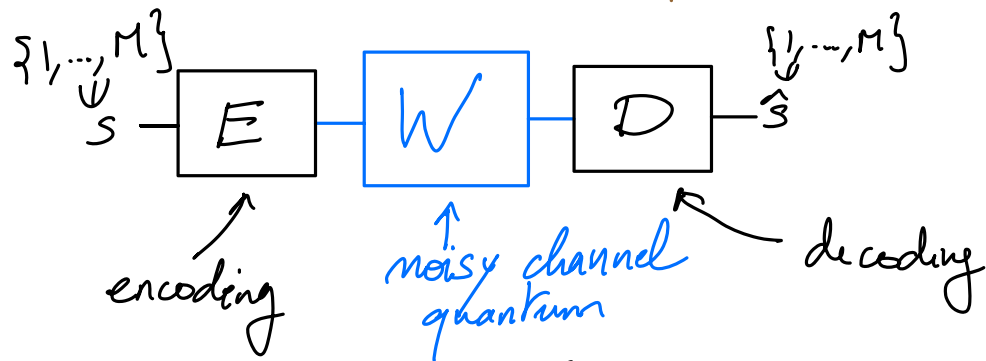


Note: answer questions from Whara: contractive, operational intr Choi, Kraus.



Objective: * $\mathbb{P}\{s \neq \hat{s}\}$ small
 * M large.

1. Classical - quantum channels.

Input of W is **classical**

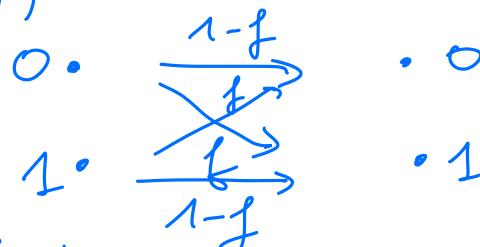
finite set
↓

Def: A classical - quantum channel W with input space X and output space B is a collection $\{W_\alpha\}_{\alpha \in X}$ of density operators W_α acting on B .
 B Hilbert space

Ex: • Classical channel: $\{W(y|x)\}_{x \in X, y \in Y}$

$W(y|x) =$ probability output y for input x .

For example: Binary symmetric channel flip probability f
 $X = \{0, 1\}$ $Y = \{0, 1\}$



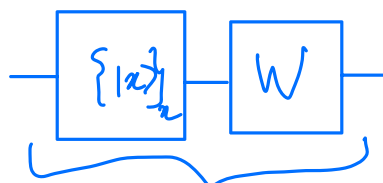
$$W(0|0) = W(1|1) = 1-f, \quad W(0|1) = W(1|0) = f.$$

Can see it as a classical-quantum channel with output \mathcal{B} a Hilbert space of dimension $|\mathcal{Y}|$

$$W_x = \sum_{y \in \mathcal{Y}} W(y|x) |y\rangle\langle y|$$

where $\{|y\rangle : y \in \mathcal{Y}\}$ is a fixed orthonormal basis.

- $W_0 = |0\rangle\langle 0|$ and $W_1 = |+\rangle\langle +|$ $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Can see W as a quantum channel that starts by measuring in a basis $\{|x\rangle\}_{x \in \mathcal{X}}$ followed by preparation

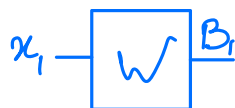


Quantum channel W satisfying $W(|x\rangle\langle x|) = W_x$ for $x \in \mathcal{X}$.

and $W(|x\rangle\langle x'|) = 0$ for $x \neq x'$

- Given W and $n \geq 1$ integer, can define $W^{\otimes n}$: input \mathcal{X}^n and output $\mathcal{B}^{\otimes n}$

$$(W^{\otimes n})_{x_1 \dots x_n} = W_{x_1} \otimes W_{x_2} \otimes \dots \otimes W_{x_n}$$



⋮



$[M] := \{1, \dots, M\}$.

Def: An M -code (E, D) for W is given by

- $E: [M] \rightarrow \mathcal{X}$ encoding function
- Decoding is a POVM $\{D_s\}_{s \in [M]}$ on \mathcal{B} .

Ex: For a classical channel, we may assume $\{D_s\}$ are diagonal $D_s = \text{diag}(D_s(y) : y \in \mathcal{Y})$

$D_s(y) =$ Probability of decoding to s when seeing y .

POVM condition: $\sum_s D_s(y) = 1$.

Def: The error probability $p_{\text{err}}(E, D)$ of an M -code for W is defined by

$$p_{\text{err}}(E, D) = 1 - \frac{1}{M} \sum_{s \in [M]} \text{Tr}(D_s W_{E(s)})$$

probability of successful decoding.

If $p_{\text{err}}(E, D) \leq \epsilon$, we say that (E, D) is an (M, ϵ) -code

Remark: Used a uniform prior on $[M]$, another natural choice is

$$p_{\text{err}, \max}(E, D) = \max_{s \in [M]} 1 - \text{Tr}(D_s W_{E(s)})$$

p_{err} and $p_{\text{err}, \max}$ are related

Ex: • $\dim \mathcal{B} = |\mathcal{X}|$. $W_x = |x \times x|$.

$(|\mathcal{X}|, 0)$ code given by

$$E(s) = |s \times s|$$

(identifying \mathcal{X} with $[|\mathcal{X}|]$)

$$D_s = |s \times s|.$$

$$\frac{1}{|\mathcal{X}|} \sum_s \text{Tr}(|s \times s| \cdot |s \times s|) = 1.$$

• Let $e \in \mathcal{S}(\mathcal{B})$ and $W_x = e$ for all $x \in \mathcal{X}$.
(useless channel, output does not depend on input)

For any choice of (E, D) , we have

$$\sum_{s \in [M]} \text{Tr}(D_s e) = 1. \Rightarrow P_{\text{err}}(E, D) = 1 - \frac{1}{M}$$

Question: Fixed ϵ , largest M for which there exists an (M, ϵ) -code for W ?

$$M^{\text{opt}}(W, \epsilon) = \max \{M : \exists (M, \epsilon)\text{-code for } W\}.$$

Objective: Characterize $M^{\text{opt}}(W, \epsilon)$ in terms of "simple" properties of W .

Important special case: • $W^{\otimes n}$ with large n .
• ϵ small

$$\lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \underbrace{\frac{\log_2 M^{\text{opt}}(W^{\otimes n}, \epsilon)}{n}} = ?$$

number of bits transmitted per channel use

Intuition: $M^{\text{opr}}(W, \epsilon)$ should be given by a correlation measure between input and output of W .

Given a probability measure P_X on \mathcal{X} let

$$\rho_{XB} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x| \otimes W_x \quad \text{cq-state}$$

Recall we write $\rho_X = \text{Tr}_B \rho_{XB}$ and $\rho_B = \text{Tr}_X \rho_{XB}$.

To characterize $M^{\text{opr}}(W, \epsilon)$ need:

* upper bound (called converse)

* lower bound (called achievability)

Converse

Th: If there exists an (M, ϵ) code for W

then $\log M \leq \sup_{P_X} \underbrace{D_H^\epsilon(\rho_{XB} \| \rho_X \otimes \rho_B)}_{\text{correlation measure}}$

Rk: Channel W is arbitrary, "one-shot" entropy measure expected
For W iid, D_H^ϵ will become a relative entropy D .

Proof: Consider an (M, ϵ) code. (E, D) .

Let $C = \{x \in \mathcal{X} : \exists s \in [M] : E(s) = x\}$
and define $P_X(x) = 1/|C|$ for $x \in C$ and $P_X(x) = 0$ $x \notin C$

Then

$$\rho_{XB} = \frac{1}{|C|} \sum_{x \in C} |x\rangle\langle x| \otimes W_x.$$

and

$$F = \frac{|C|}{M} \sum_{x \in C} |x\rangle\langle x| \otimes \left(\sum_{s: E(s)=x} D_s \right)$$

As $\{D_s\}$ is a POVM, $0 \leq F \leq I$.

$$\begin{aligned} \text{Tr}(F \rho_{XB}) &= \frac{1}{M} \sum_{x \in C} \text{Tr} \left(\left(\sum_{s: E(s)=x} D_s \right) W_x \right) \\ &= \frac{1}{M} \sum_{s=1}^M \text{Tr} (D_s W_{E(s)}) \\ &\geq 1 - \epsilon. \end{aligned}$$

by the fact that (E, D) is an (M, ϵ) -code.

On the other hand,

$$\begin{aligned} \text{Tr}(F \rho_X \otimes \rho_B) &= \frac{|C|}{M} \text{Tr} \left(\sum_{x \in C} |x\rangle\langle x| \otimes \left(\sum_{s: E(s)=x} D_s \right) \right) \left(\rho_X \otimes \rho_B \right) \\ &= \frac{|C|}{M} \sum_{x \in C} \text{Tr} \left(|x\rangle\langle x| \otimes \sum_{s: E(s)=x} D_s \right) \left(\frac{|x\rangle\langle x|}{|C|} \otimes \rho_B \right) \\ &= \frac{1}{M} \text{Tr} \left(\sum_{x \in C} \sum_{s: E(s)=x} D_s \right) \rho_B \\ &= \frac{1}{M} \end{aligned}$$

So $D_H^\epsilon(\rho_{XB} \| \rho_X \otimes \rho_B) \geq \log M$ \square

Achievability

Th: For any $\epsilon \in (0, 1)$ and $\delta \in (0, \epsilon)$

↑ Tunable parameter for this bound.

and M satisfying:

$$\log M \leq \sup_{P_X} D_{\epsilon-\delta}^H(P_X \parallel P_X \otimes P_B) - \log(1/\delta)$$

then exists an (M, ϵ) -code.

Not the same ϵ but can choose it arbitrarily close to ϵ .

Think of this as a small error term

Rk: * Achievability statement matches converse up to error terms that are "small" in many settings of interest.

* Proof uses the **probabilistic method**: does not give an explicit (E, D) that is an (M, ϵ) code but rather we choose (E, D) **at random** and show that on average, it has an error probability $\leq \epsilon$.

Proof:

Assume ϵ is fixed (chosen later), we construct a decoder $\{D_s\}$

We use pretty good measurement:

$$D_s = \Lambda^{1/2} W_{E(s)} \Lambda^{-1/2}$$

$$\Lambda = \sum_{s' \in [M]} W_{E(s')}$$

notation $\rightarrow = \frac{W_{E(s)}}{\Lambda}$

Rk: Interpretation of this strategy in classical case
 On sample y , output s with prob $\frac{W_{E(s)}(y)}{\sum_s W_{E(s)}(y)}$

Maximum likelihood would be:

On sample y , output s maximizing $W_{E(s)}(y)$

$$\begin{aligned} \text{Perr}(E, D) &= \frac{1}{M} \sum_{s \in \mathcal{M}} \text{Tr} \left(\sum_{s' \neq s} D_{s'} W_{E(s')} \right) \\ &= \frac{1}{M} \sum_{s \in \mathcal{M}} \text{Tr} \left(\frac{\left(\sum_{s' \neq s} W_{E(s')} \right) W_{E(s)}}{W_{E(s)} + \left(\sum_{s' \neq s} W_{E(s')} \right)} \right) \end{aligned}$$

Note that for $a, b \geq 0$ scalars: $\frac{ab}{a+b} \leq \min(a, b)$.

Noncommutative minimum:

For $A, B \geq 0$,

$$A \wedge B := \frac{1}{2} (A + B - |A - B|)$$

$$\begin{aligned} \text{Properties: (i) } \text{Tr}(A \wedge B) &= \max_{M=M^*} \left\{ \text{Tr}(M) : M \leq A, M \leq B \right\} \\ &= \min_{0 \leq \Lambda \leq I} \left\{ \text{Tr}(A(1-\Lambda)) + \text{Tr}(B\Lambda) \right\} \end{aligned}$$

$$\text{(ii) } \text{Tr} \left(A (A+B)^{-1/2} B (A+B)^{-1/2} \right) \leq \text{Tr}(A \wedge B).$$

(iii) $(A, B) \mapsto \text{Tr}(A \wedge B)$ jointly concave

See arXiv:2208.02132 for proofs and more properties.

$$P_{\text{err}}(E, D) \leq \frac{1}{M} \sum_{s \in [M]} \text{Tr} \left(W_{E(s)} \wedge \sum_{s' \neq s} W_{E(s')} \right)$$

Now how to choose E ?

choose $E(s)$ **random** with distribution P_X maximizing \star independently for every $s \in [M]$.

$$\begin{aligned} \mathbb{E} \left\{ P_{\text{err}}(E, D) \right\} &\leq \mathbb{E}_{\substack{E(1) \sim P_X \\ E(s') \sim P_X}} \text{Tr} \left(W_{E(1)} \wedge \sum_{s' \neq 1} W_{E(s')} \right) \\ &\leq \mathbb{E}_{E(1) \sim P_X} \left\{ \text{Tr} \left(W_{E(1)} \wedge \mathbb{E}_{E(s') \sim P_X} \left(\sum_{s' \neq 1} W_{E(s')} \right) \right) \right\} \\ &= \mathbb{E}_{x \sim P_X} \text{Tr} \left(W_x \wedge (M-1) \rho_B \right) \\ &= \text{Tr} \left(\rho_{XB} \wedge (M-1) \rho_{X \otimes B} \right). \end{aligned}$$

↑
randomness
in E

Now want to relate this to hypothesis testing.

$$= \inf_{0 \leq \Lambda \leq I} \text{Tr} \left((I - \Lambda) \rho_{XB} \right) + (M-1) \text{Tr} \left(\Lambda \rho_{X \otimes B} \right)$$

By definition, there exists $0 \leq F \leq I$ s.t.

$$\text{Tr}(F \rho_{XB}) \geq 1 - \epsilon + \delta \quad \& \quad \text{Tr}(F \rho_{X \otimes B}) \leq 2^{-D_{\text{H}}^{\epsilon-\delta}(\rho_{XB} \| \rho_{X \otimes B})}$$

As a result

$$\mathbb{E} \left\{ \text{perr}(E, D) \right\} \leq \varepsilon - \delta + (M-1) 2^{-D_H} (\varepsilon - \delta) \left(\frac{\|x\|}{\|x\|_b} \right)$$

Many condition on M in $(*)$

$$\mathbb{E} \left\{ \text{perr}(E, D) \right\} \leq \varepsilon$$

\Rightarrow There exists (E, D) s.t. $\text{perr}(E, D) \leq \varepsilon$ ■

This characterization of $\log M^{\text{opr}}(W, \epsilon)$ is very general.

Important special case where we can evaluate the expression more explicitly: Memoryless channel $W^{\otimes n}$.

Def: Let W be a cq channel.

The classical capacity $C(W)$ of W is defined by

$$C(W) := \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{\log M^{\text{opr}}(W^{\otimes n}, \epsilon)}{n}$$

↑ optimal rate for transmitting information.

Corollary: For any cq channel W

$$\sup_{P_X} I(X; B) \leq C(W) \leq \sup_n \frac{1}{n} \sup_{P_{X_1 \dots X_n}} I(X_1 \dots X_n; B_1 \dots B_n)$$

$$\text{where } \sup_{P_{X_1 \dots X_n}} = \sum_{x_1 \dots x_n} P(x_1 \dots x_n) W_{x_1} \otimes W_{x_2} \otimes \dots \otimes W_{x_n}$$

Notation: $X^n := X_1 \dots X_n$ $B^n = B_1 \dots B_n$

Proof:

Apply one-shot theorem with $W^{\otimes n}$

$$\sup_{P_{X^n}} D_H^{\epsilon/2}(P_{X^n B^n} \| P_{X^n} \otimes P_{B^n}) - \log\left(\frac{2}{\epsilon}\right) - 1 \leq \log M^{\text{opr}}(W^{\otimes n}, \epsilon) \leq \sup_{P_{X^n}} D_H^{\epsilon}(P_{X^n B^n} \| P_{X^n} \otimes P_{B^n})$$

Multiply by $\frac{1}{n}$ and take limits $n \rightarrow \infty$; $C(W) = \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} \sup_{P_{X^n}} D_H^{\epsilon}(P_{X^n B^n} \| P_{X^n} \otimes P_{B^n})$

We should evaluate $\lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} \sup_{P_{X^n}} D_H^\epsilon(P_{X^n B^n} \| P_{X^n} \otimes P_B) =: \alpha$

• $\alpha \geq \sup_{P_X} I(X; B)_{P_X}$ Let P_X achieve the sup.

Choose $P_{X^n} = P_X \otimes P_X \dots \otimes P_X$ (X_1, \dots, X_n independent distribution P_X).

$$\alpha \geq \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{D_H^\epsilon(P_{XB}^{\otimes n} \| P_X^{\otimes n} \otimes P_B^{\otimes n})}{n}$$

Stein lemma:

$$= D(P_{XB} \| P_X \otimes P_B)$$

$$= I(X; B)_{P_X}$$

• $\alpha \leq \sup_m \sup_{P_{X^n}} \frac{1}{n} I(X^n; B^n)_{P_{X^n B^n}}$

In the converse part of Stein's lemma, we showed

$$D_H^\epsilon(P \| \sigma) \leq \frac{D(P \| \sigma) + 1}{1 - \epsilon}$$

$$\alpha \leq \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} \sup_{P_{X^n}} \frac{D(P_{X^n B^n} \| P_{X^n} \otimes P_{B^n}) + 1}{1 - \epsilon}$$

$$= \lim_{n \rightarrow \infty} \frac{1}{n} \sup_{P_{X^n}} I(X^n; B^n)_{P_{X^n B^n}}$$

$$= \sup_m \frac{1}{n} \sup_{P_{X^n}} I(X^n; B^n)_{P_{X^n B^n}}$$

$f(n) := \sup_{P_{X^n}} I(X^n; B^n)$
is superadditive (ex)
 $f(n+m) \geq f(n) + f(m)$.
+ Fekete lemma.

Rk: Actually easy to see $C(W) = \sup_m \sup_{P_{X^n}} \frac{1}{n} I(X^n; B^n)_{P_{X^n B^n}}$.

How to compute $\sup_{P_{X^n}} \frac{1}{n} \sup_{P_{B^n}} I(X^n: B^n)$?

For cq channels $\rightarrow = \sup_{P_X} I(X: B)$, ie $f(n)$ additive

Lemma: For any n

$$\frac{1}{n} \sup_{P_{X^n}} I(X^n: B^n) = \sup_{P_X} I(X: B)$$

Proof: $\cdot \geq$ simple (always true, not only cq channels)

$\cdot \leq$ Let P_{X^n} be arbitrary $P_{X^n B^n} = \sum_{x^n} P_{X^n}(x^n) |x^n\rangle\langle x^n| \otimes W_{x^n}$

$$I(X^n: B^n) = H(B^n) - H(B^n | X^n)$$

$$* H(B^n) \leq \sum_{i=1}^n H(B_i) \quad (\text{subadditivity})$$

$$* H(B^n | X^n) = \sum_{x_1, \dots, x_n} P_{X^n}(x_1, \dots, x_n) H(B^n)_{W_{x_1} \otimes W_{x_2} \otimes \dots \otimes W_{x_n}}$$

Property of von Neumann entropy:

conditional entropy = average of entropy of conditional state.

$$= \sum_{x_1, \dots, x_n} P_{X^n}(x_1, \dots, x_n) (H(B)_{W_{x_1}} + H(B)_{W_{x_2}} + \dots + H(B)_{W_{x_n}})$$

entropy of a product state is sum of entropies.

$$= \sum_{i=1}^n \sum_{x_i} P_{X_i}(x_i) H(B)_{W_{x_i}}$$

$$= \sum_{i=1}^n H(B_i | X_i)$$

$$\begin{aligned}
 \text{So } I(X^n: B^n) &\leq \sum_{i=1}^n H(B_i) - H(B_i|X_i) \\
 &= \sum_{i=1}^n I(X_i: B_i) \\
 &\leq n \cdot \sup_{P_X} I(X: B) \quad \square
 \end{aligned}$$

Th (Shannon theorem for cq channel)

The capacity of a cq channel is given by

$$\begin{aligned}
 C(W) &= \sup_{P_X} I(X: B) \Big|_{P_{XB}} \\
 P_{XB} &= \sum_x P_X(x) |x\rangle\langle x| \otimes W_x
 \end{aligned}$$

Rk.: If $W_x = W$ for all $x \Rightarrow C(W) = 0$
 Surprisingly, converse also true

$$C(W) = 0 \Leftrightarrow W_x = W \quad \forall x$$

This is surprising, just using "repetition" will not work.

2. General quantum channels.

Now $\mathcal{W}: L(A) \rightarrow L(B)$ quantum channel.

Very similar definitions:

Def: An M -code (E, D) for \mathcal{W} is given by

- $E: [M] \rightarrow S(A)$ encoding function
- Decoding is a POVM $\{D_s\}_{s \in [M]}$ on B .

Def: The error probability $p_{\text{err}}(E, D)$ of an M -code for \mathcal{W} is defined by

$$p_{\text{err}}(E, D) = 1 - \frac{1}{M} \sum_{s \in [M]} \text{Tr}(D_s \mathcal{W}(E(s)))$$

probability of successful decoding.

If $p_{\text{err}}(E, D) \leq \epsilon$, we say that (E, D) is an (M, ϵ) -code

Looking back at the proofs for cq channels, we see that it suffices to optimize over choices of $\{\sigma_A^x\}_{x \in X} \subseteq S(A)$ and consider the corresponding cq channel $\mathcal{W}_x = \mathcal{W}(\sigma_A^x)$

We then define (as before) for $\{P_X(x), \sigma_A^x\}_{x \in X}$

$$\rho_{XB} = \sum_{x \in X} P_X(x) |x\rangle\langle x| \otimes \mathcal{W}(\sigma_A^x)$$

↑ This is called an ensemble

Th: Any (M, ϵ) -code for \mathcal{W} satisfies

$$\log M \leq \sup_{\sigma_A^x} \sup_{P_X} D_H^\epsilon (P_{XB} \| P_X \otimes P_B)$$

and there exists an (M, ϵ) -code for \mathcal{W}

$$\log M \geq \sup_{\sigma_A^x} \sup_{P_X} D_H^{\epsilon-\delta} (P_{XB} \| P_X \otimes P_B) - \log(1/\delta)$$

Basically the same proof. (good exercise to redo it yourself)

Rk: we take supremum over arbitrarily large X but in many cases can bound it.

Important special case: $\mathcal{W}^{\otimes n}$.

Def: The classical capacity $C(\mathcal{W})$ of a quantum channel \mathcal{W} is defined as: some def as for cq channels

$$C(\mathcal{W}) := \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{\log M^{\text{opt}}(\mathcal{W}^{\otimes n}, \epsilon)}{n}$$

Same as before: using Stein lemma $\frac{1}{n} D_H^\epsilon \rightarrow D$.

Notation: $\chi(\mathcal{W}) := \sup_{\{\sigma_A^x, P_X(x)\}} \underbrace{D(P_{XB} \| P_X \otimes P_B)}_{I(X:B)_{P_{XB}}}$

where $P_{XB} = \sum_x P_X(x) |x\rangle\langle x| \otimes \mathcal{W}(\sigma_A^x)$

Rk: * $\chi(W)$ is called the Holevo information of W . See [Wilde, Ch 13] or [Watrous, Ch 8] for properties.

* The Holevo information of an ensemble $\{P_X(x), \sigma_A^x\}$ also commonly denoted $\underbrace{I(X:A)}_{\chi(X:A)}$ for $\rho_{XA} = \sum_x P_X(x) |x\rangle\langle x| \otimes \sigma_A^x$
 $\chi(\{P_X(x), \sigma_A^x\})$

With this notation, for a cq channel W : $C(W) = \sup_{P_X} \chi(\{P_X(x), W_x\})$

The (Holevo-Schumacher-Westmoreland, HSW)

Let W be a quantum channel
$$C(W) = \lim_{n \rightarrow \infty} \frac{1}{n} \chi(W^{\otimes n}) = \sup_n \frac{1}{n} \chi(W^{\otimes n})$$

Proof is the same as what we did in cq case.

Question: Is χ additive under tensor product?

i.e. $\chi(W^{\otimes n}) \stackrel{?}{=} n \chi(W)$

Note that $\chi(W^{\otimes n}) \geq n \chi(W)$ is simple, follows from the fact that $D(\rho \otimes \rho \| \sigma \otimes \sigma) = 2D(\rho \| \sigma)$.

Answer: . NO in general, i.e., there exists channels W s.t. $\chi(W^{\otimes 2}) > 2 \chi(W)$.

This means that optimal choices of states $\sigma_{A_1 A_2}^x$ will be entangled

Construction in [Hastings, 2009] by choosing W "random" and a very involved analysis. [See book Alice & Bob meet Banach]

- But there are families of channels for which additivity can be proved.

Research question:

parameter $\delta \in [0, 1]$

Consider the amplitude damping channel A_δ

$$\begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} \xrightarrow{A_\delta} \begin{pmatrix} \rho_{00} + \delta \rho_{11} & \sqrt{1-\delta} \rho_{01} \\ \sqrt{1-\delta} \rho_{10} & (1-\delta) \rho_{11} \end{pmatrix}$$

$C(A_\delta)$ unknown.

[Simplistic model for decay of 2-level atom due to spontaneous emission of photon]