Upper bounds on the reliability of quantum information protocols

Naresh Sharma
Tata Institute of Fundamental Research
Mumbai, India

Based on arXiv:1205.1712 (with N. A. Warsi)

Beyond IID in information theory
Cambridge, UK
Jan 11, 2012

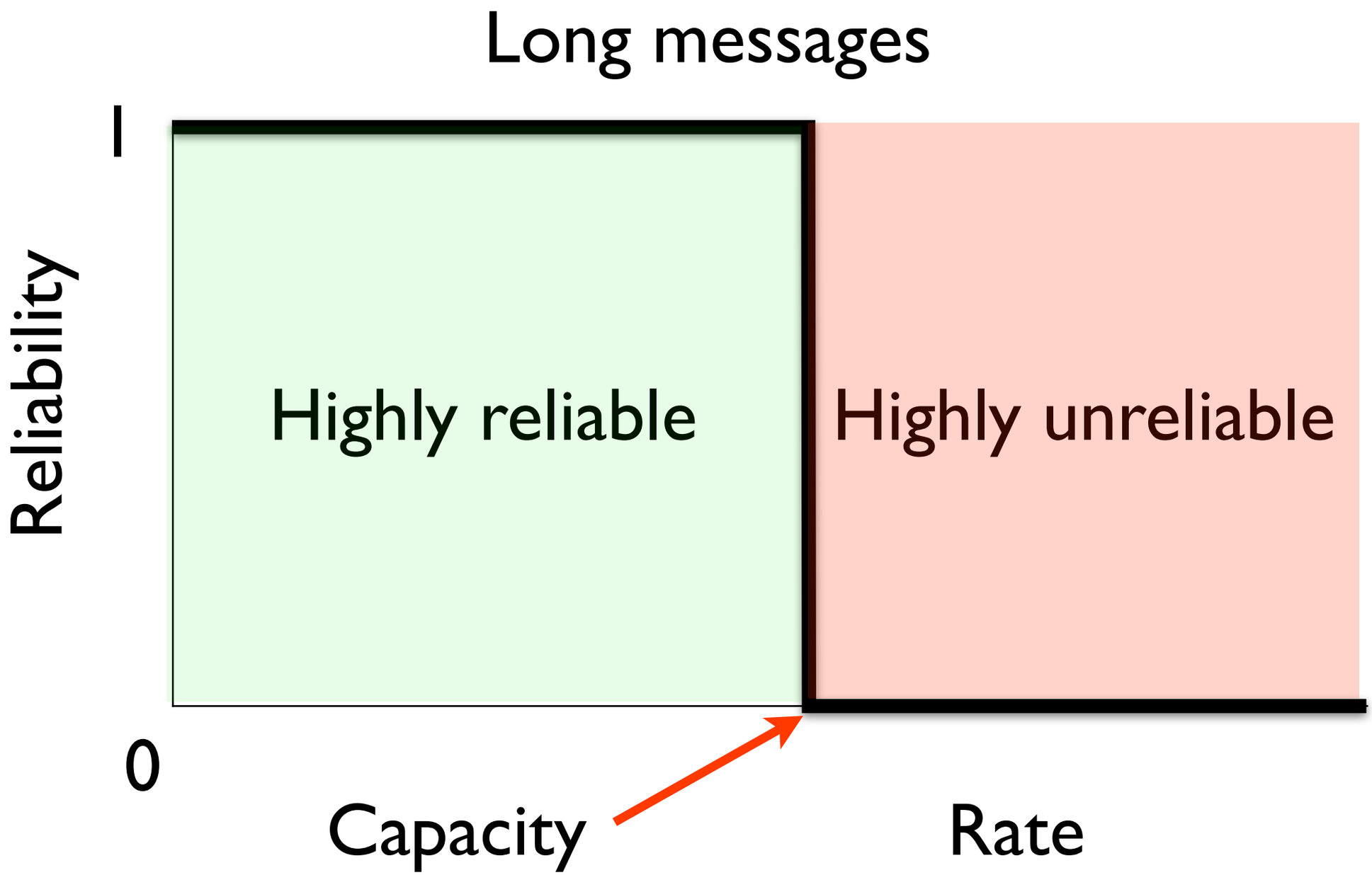
Introduction

- For a given channel, how much information could be transmitted reliably per channel use asymptotically?

- Shannon (1948) in his landmark paper identified a property of a communication channel called capacity.

- Channel capacity gives us the highest information transfer rate across the channel with arbitrarily high reliability asymptotically.

- For some channels, the following graph can be proved.



Converse

- Fidelity (F) of a communication protocol is a measure of closeness between the message sent and the reconstructed message at the receiver.
- $F \approx 1$ and $F \approx 0$ indicate highly reliable and unreliable transfer respectively.
- Converse theorem shows if the rate of the protocol is higher than the capacity, then F is bounded away from 1.

- There are two types of converse theorems:
  - Weak Converse: For rates above capacity, *F* is bounded away from 1
  - Strong Converse: For rates above capacity, *F* decays to 0 with the number of channel uses
- Not all channels have strong converses. See Dorlas and Morgan (2011) for an example

- Strong converse for the classical case
  - Wolfowitz (1950s)

$$F \leq \frac{A}{n} + \mathrm{e}^{-n(\mathcal{R}-C)},$$

$$A \text{ positive, finite}$$

  - Arimoto (1973)

$$F \leq \mathrm{e}^{-Kn},$$

$$K > 0 \text{ if } R > C$$

- It has been shown (though not in full generality) when classical information is sent across a quantum channel by
  - Winter (1999)
  - Ogawa and Nagaoka (1999)
  - König and Wehner (2009)

- Semi-strong converse for sending quantum information over quantum channels (degradable channels) - Morgan and Winter (2012)

Overview

- Prior results
- Provide alternate proof on the Ogawa and Nagaoka upper bound on the reliability
- Provide upper bounds (via the Gallager exponent) on the reliability of sending quantum information across quantum channels
- Applicability to the erasure channel

Prior results

- Most common (weak) converse is by using the Fano inequality
- One of the first results (if not the first) that connected monotonicity with converse is by Blahut (1976)

- Monotonicity => Fano (classical) OR
  Monotonicity => Converse
- His definition of 'refinement' - "*By a refinement, we mean the replacement of each point by several new points with the probability of the original point apportioned among the new points*"

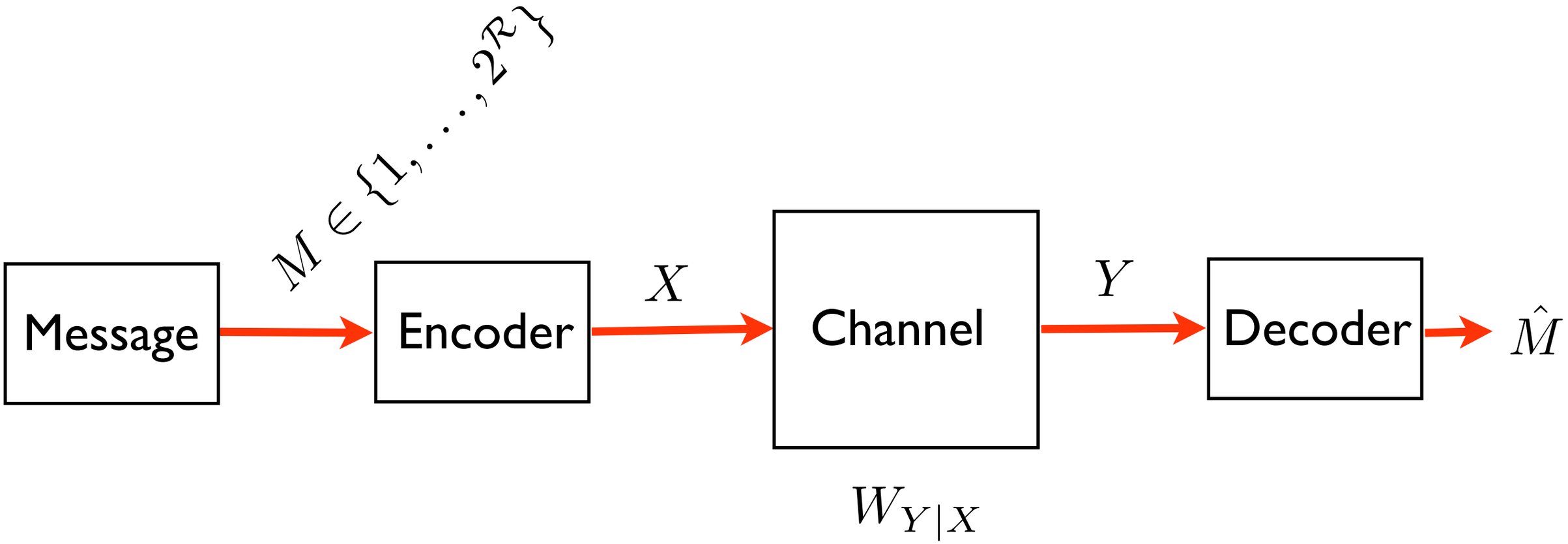
- Han and Verdú (1994) generalized classical Fano inequality using monotonicity
- Similar generalization for and alternate proof of the quantum Fano inequality (NS, 2008)
- Arimoto (1973) proved strong converse using the Gallager's exponent
- Csiszár (1995) related Rényi divergence with Gallager's exponent (using Sibson's identity)

- Blahut: Monotonicity of divergence => Fano
- Polyanskiy and Verdú (2010): Monotonicity of Rényi divergence + Csiszár's observation => strong converse for the classical channel capacity theorem
  - Has a non-commutative extension - the subject of this talk
  - Wolfowitz's converse from *f*-relative entropy by choosing *f* to be the hockey-stick function -

$$f(x) = (x - \gamma)^+$$

  - Also provide an elegant proof of the additivity of the Gallager's exponent

Classical information over classical channels



$\mathcal{R}$ – Rate of the protocol in bits per channel use

$\Pr\{M = \hat{M}\}$ – Fidelity of the protocol

- Weak converse using Fano:

$$\Pr\{M = \hat{M}\} \leq \frac{C}{\mathcal{R}} + \frac{1}{n\mathcal{R}}$$

- Wolfowitz's Strong Converse:

$$\Pr\{M = \hat{M}\} \leq \frac{4\mathcal{A}}{n(\mathcal{R} - C)^2} + 2^{-n(\mathcal{R}-C)}$$

- Arimoto's Strong Converse:

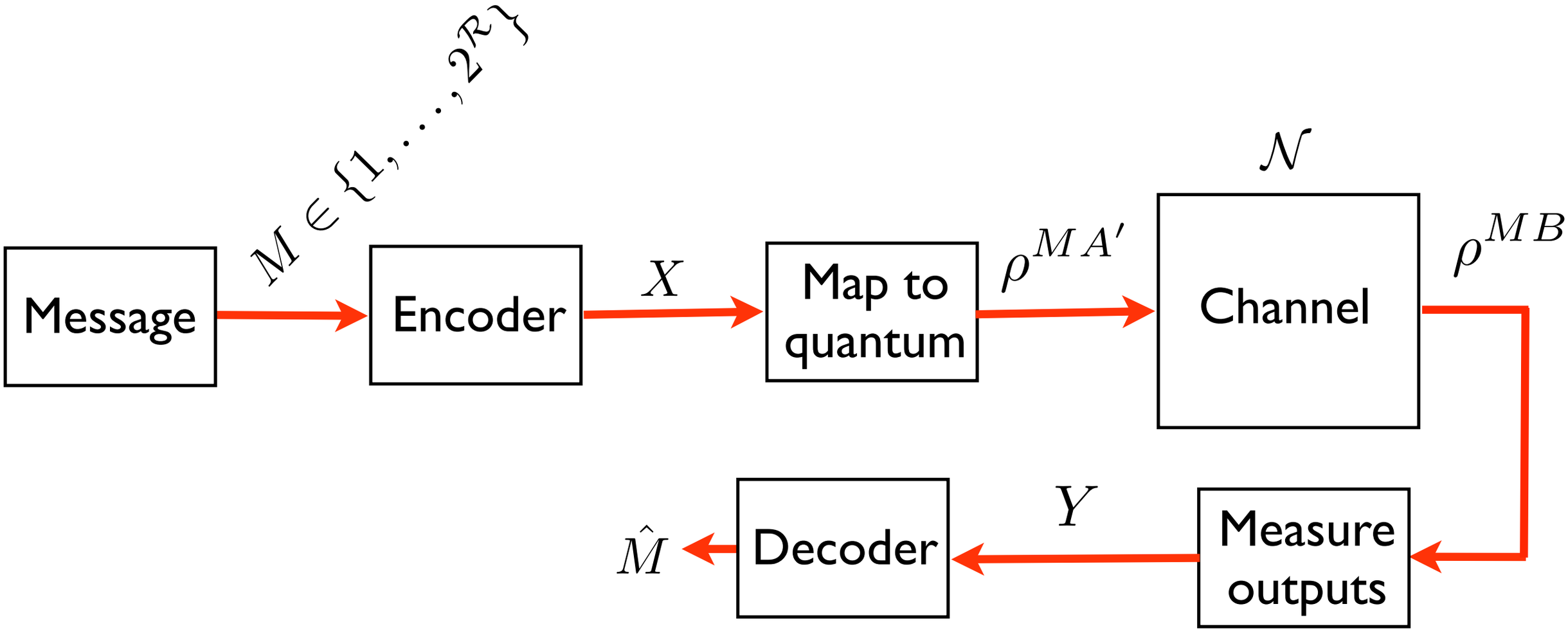
$$\Pr\{M = \hat{M}\} \leq 2^{n\left[s\mathcal{R} - E_0(s, W_{Y|X})_P\right]}, \quad s \in [-1, 0)$$

$$E_0(s, W_{Y|X})_P := -\log \sum_y \left\{ \sum_x P_X(x) \left[W_{Y|X}(y|x)\right]^{\frac{1}{1+s}} \right\}^{1+s}$$

- $-sR + E_0(s, W_{Y|X})_P$ is called the Gallager's exponent who first proposed it in a different context

- Key property: $\left.\frac{\partial E_0(s, W_{Y|X})_P}{\partial s}\right|_{s=0} = I(X;Y)$

Classical information over quantum channels



$\mathcal{R}$ – Rate of the protocol in bits per channel use

$\Pr\{M = \hat{M}\}$ – Fidelity of the protocol

- Ogawa and Nagaoka gave an Arimoto-like strong converse (for product inputs)

- We provide an alternate proof

- Key quantity to deal with:

$$\mathcal{K}^{(c)}(A;B)_\rho := \inf_{\sigma^B \in \mathcal{S}(\mathcal{H}_B)} \mathcal{D}(\rho^{AB} || \rho^A \otimes \sigma^B)$$

- Satisfies certain monotonicity inequalities

- Satisfies a Holevo-like bound

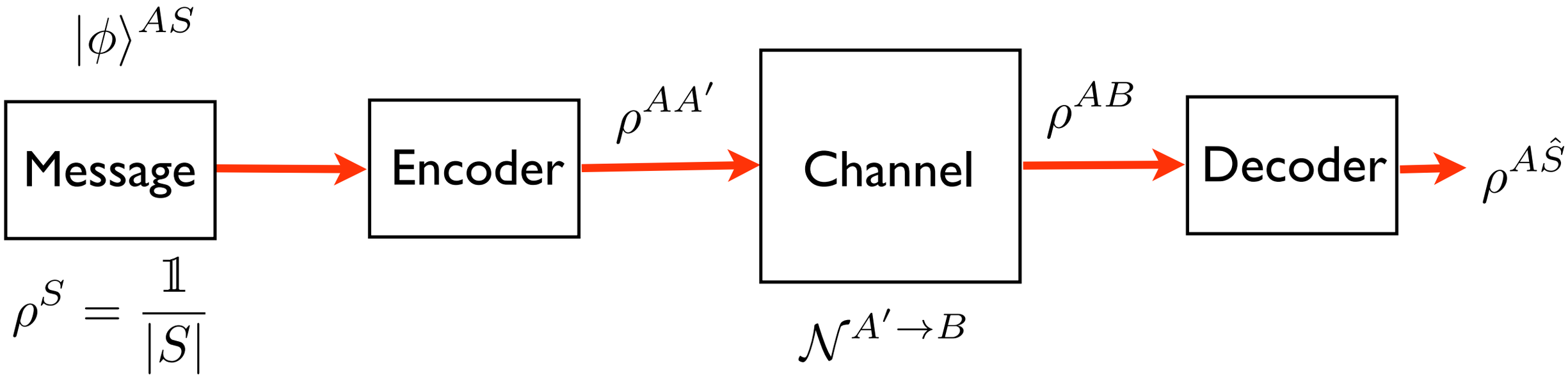
$$\mathcal{K}^{(c)}(X;Y) \leq \mathcal{K}^{(c)}(M;B)_\rho$$

- Define a non-commutative hockey-stick divergence

$$\mathcal{D}(\rho||\sigma) = \mathrm{Tr}(\rho - \gamma\sigma)^+, \quad \gamma > 1$$

- Satisfies the required properties (monotonicity etc.)

Quantum information over quantum channels



$\mathcal{R} = \frac{\log_2 |S|}{n}$ is the rate of the protocol

$F = \langle \phi |^{AS} \rho^{A\hat{S}} |\phi\rangle^{AS}$ – Fidelity of the protocol

- Key quantity to deal with:

$$\mathcal{K}^{(q)}(A;B)_\rho := \inf_{\sigma^B \in \mathcal{S}(\mathcal{H}_B)} \mathcal{D}(\rho^{AB} || \mathbb{1} \otimes \sigma^B)$$

- Need a quantum version of Sibson's identity

$$D_\lambda(\rho^{AB} || \mathbb{1} \otimes \sigma^B) = D_\lambda(\sigma^* || \sigma^B) + \frac{\lambda}{\lambda - 1} \log \mathrm{Tr} \left[\mathrm{Tr}_A \left(\rho^{AB} \right)^\lambda \right]^{\frac{1}{\lambda}},$$

$$\sigma^* = \frac{\left[\mathrm{Tr}_A \left(\rho^{AB} \right)^\lambda \right]^{\frac{1}{\lambda}}}{\mathrm{Tr} \left[\mathrm{Tr}_A \left(\rho^{AB} \right)^\lambda \right]^{\frac{1}{\lambda}}}.$$

- Quantum Gallager's exponent

$$F \leq 2^{s\mathcal{R} - E_0(s, \mathcal{N}^{A'\to B})_\rho}, \qquad s \in [-1/2, 0)$$

$$E_0(s, \mathcal{N}^{A'\to B})_\rho := -\log \operatorname{Tr} \left\{ \operatorname{Tr}_A \left[\mathcal{N}^{A'\to B}(\rho^{AA'}) \right]^{1/(1+s)} \right\}^{1+s}$$

- Key property:

$$\left. \frac{\partial E_0(s, \mathcal{N}^{A'\to B})_\rho}{\partial s} \right|_{s=0} = I(A\rangle B)_\sigma$$

$$= H(B)_\sigma - H(AB)_\sigma$$

- Why should this work (if it works)?

Since E_0 obeys $E_0(0) = 0$, $\left.\frac{\partial E_0(s)}{\partial s}\right|_{s=0} = I$, for a negative s near 0, $-E_0(s) \approx -sI \leq -sC$
and the above bound could be weakened to give
$F \lessapprox \mathrm{e}^{s(\mathcal{R}-C)}$

Hence, if $\mathcal{R} > C$, then F is always exponentially bounded away from 1

For n channel uses and some (elusive) additivity conditions, if they hold, one could write the above bound as $F \lessapprox \mathrm{e}^{sn(\mathcal{R}-C)}$

- What are the additivity conditions?

$$E_0^*(s,\mathcal{N}) := \min_{\rho^{AA'}} E_0(s,\mathcal{N})_\rho$$

$$E_0^*\left(s,\mathcal{N}^{\otimes n+m}\right) = E_0^*\left(s,\mathcal{N}^{\otimes n}\right) + E_0^*\left(s,\mathcal{N}^{\otimes m}\right)?$$

Strong converse for erasure channel for some inputs

- Erasure channel:

$$\mathcal{N}_p^{A'\to B}(\rho^{AA'}) = (1-p)\sigma^{AB} + p\rho^A \otimes |e\rangle\langle e|^B$$

$$\sigma^{AB} = \mathcal{G}^{A'\to B}(\rho^{AA'})$$

$\mathcal{G}$ increases the dimension

but leaves the state intact

- Quantum capacity:

$$Q = (1-2p)^+ \log |A'|$$

- Strong converse holds for maximally entangled channel inputs

$$F \leq \exp\left\{n\left[s\mathcal{R} - E_0(s)\right]\right\}$$

$$E_0(s) := -\ln\left[(1-p)|A'|^{-s} + p|A'|^{s}\right]$$

$$Q = \lim_{s\uparrow 0} \frac{E_0(s)}{s}$$

- Strong converse from the hockey-stick divergence

$$F \leq 2^{-\frac{n}{2}[\mathcal{R}-Q]} + 2^{-\frac{n}{2p}\left[\frac{(2p-1)^+}{2} + \frac{\mathcal{R}}{4\log|A'|}\right]^2}.$$

Open issues

- Approach is quite general - holds for any relative entropies that satisfy monotonicity and some other properties
- Can we find a divergence that gives the strong converse and for which additivity is easier to prove?
- If single letter formula for the capacity is available, does it necessarily imply a strong converse?
- Extension to network scenarios?