

The **Quest** for a Quantum Simultaneous Decoder

Mark M. Wilde

*School of Computer Science
McGill University*



In collaboration with

Omar Fawzi, Patrick Hayden, Ivan Savov, and Pranab Sen

arXiv:1102.2624

Difficult Problems in Quantum Information Theory, MIT, May 4, 2011

Motivation

Question: Why would you need this conjecture when **Andreas Winter** found the capacity of the quantum MAC channel as a *graduate student*?



quant-ph/9807019

Answer: The best known achievable rate region for the **classical interference channel** requires **simultaneous decoding** and we would like to “quantize” this technique. It would also solve many other *difficult problems in quantum information theory* :)

This conjecture will need to be proved in order to have a characterization of the capacity of the **quantum multiple access channel** in **one-shot information theory** (Time-sharing is NOT an option!)

Overview

- Review of **Typical Sequences**
- **Simultaneous Decoder** in Classical Info. Theory
- Classical Coding for Quantum Channels Overview
- Quantum **Multiple Access** Channel
- **Quantum Simultaneous Decoder** Conjecture
- Attempts at Proving the Conjecture

Review of Typical Sequences

A sequence x^n emitted from many **IID realizations** of a random variable $X \sim p_X(x)$ is *typical* if its **sample entropy** is close to its **true entropy**:

$$T_\delta^{X^n} \equiv \{x^n : |\overline{H}(x^n) - H(X)| \leq \delta\}$$

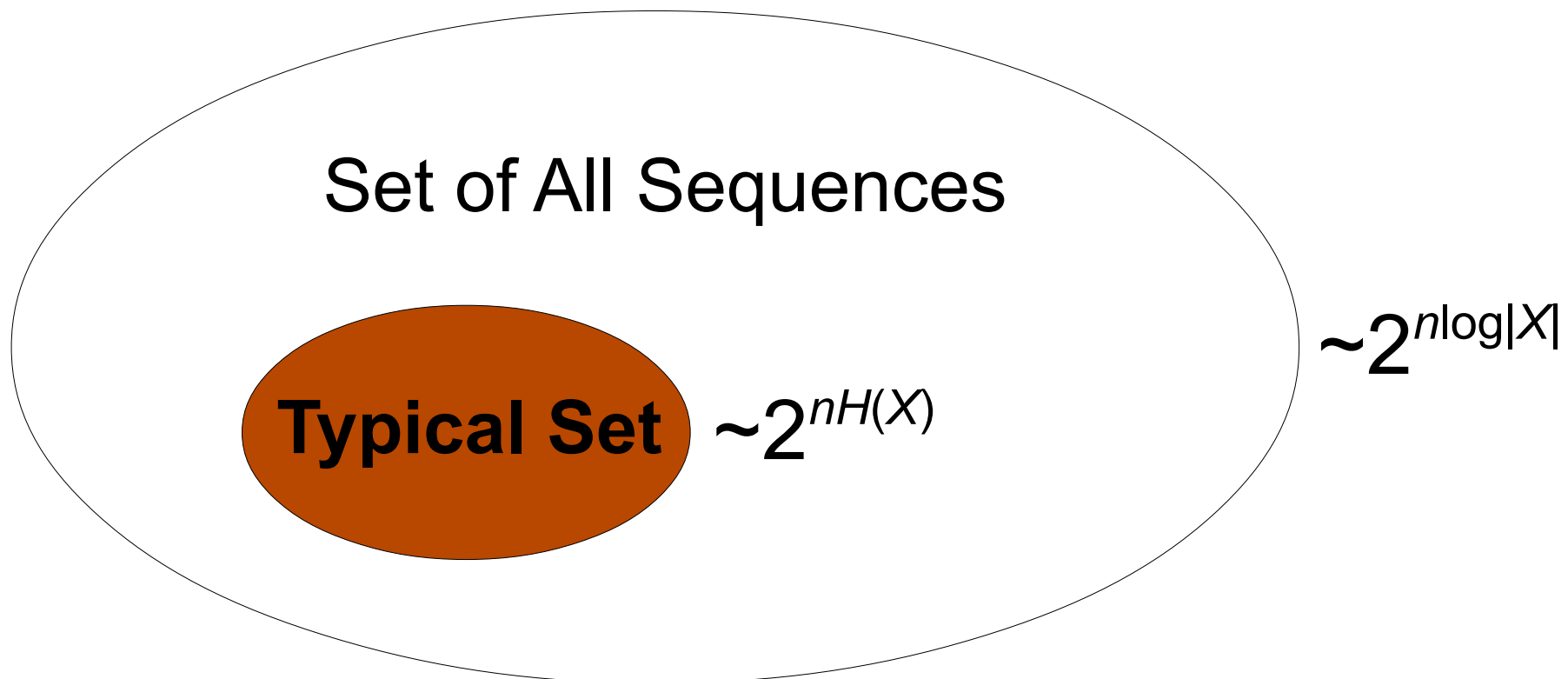
where

$$\overline{H}(x^n) \equiv -\frac{1}{n} \log(p_{X^n}(x^n))$$

$$H(X) \equiv -\sum_x p_X(x) \log(p_X(x))$$

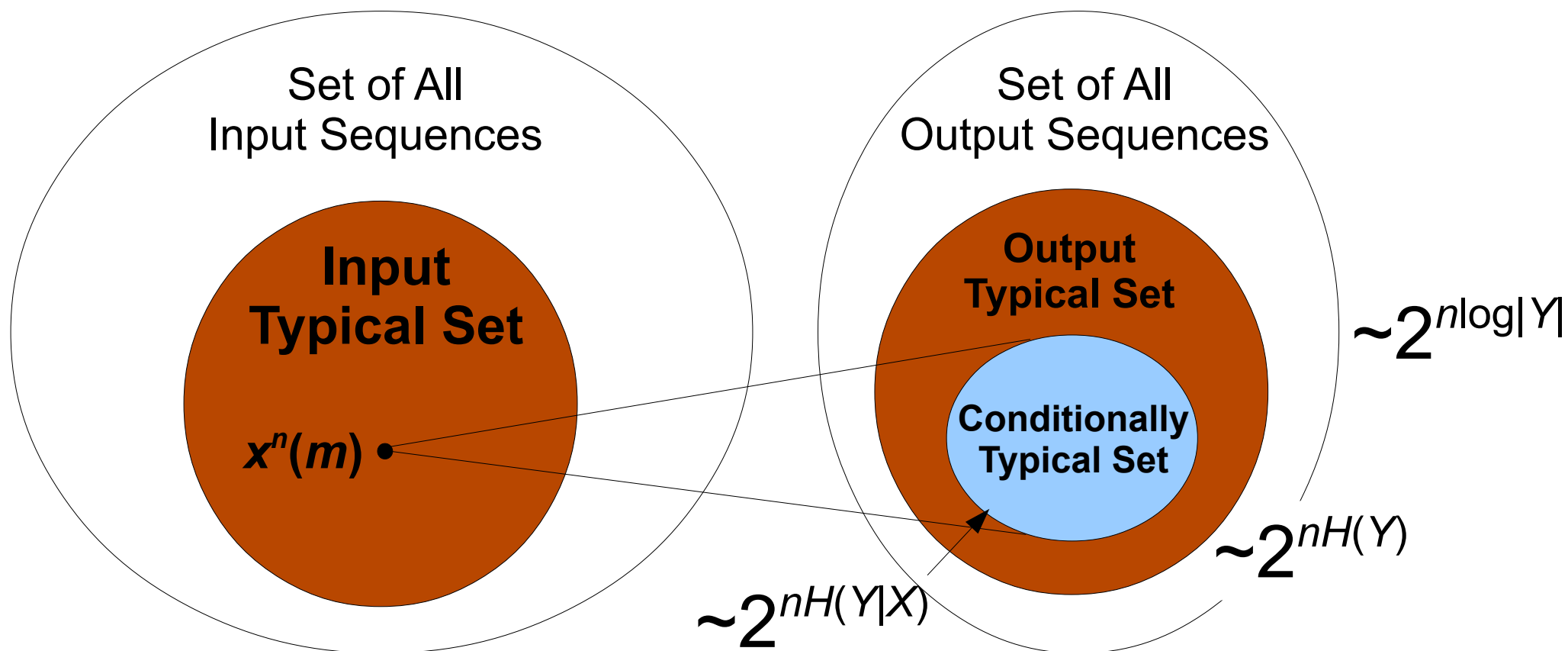
Key Property of Typical Sequences

The typical set *asymptotically* has **all of the probability**, while being ***exponentially smaller*** than the set of all sequences:



Random Coding over Noisy Channels

- Choose codewords $\{x^n(m)\}_m$ **randomly** from typical set for X^n
- Send codeword $x^n(m)$ over **IID** channel $p_{Y|X}(y|x)$
- Receiver exploits **jointly typical decoding**



Error Analysis

A **jointly typical decoder** declares message m was sent if it is the unique message such that

$$(x^n(m), y^n) \in T_\delta^{X^n Y^n}$$

Shannon's idea was to analyze the **expectation of the average error probability**

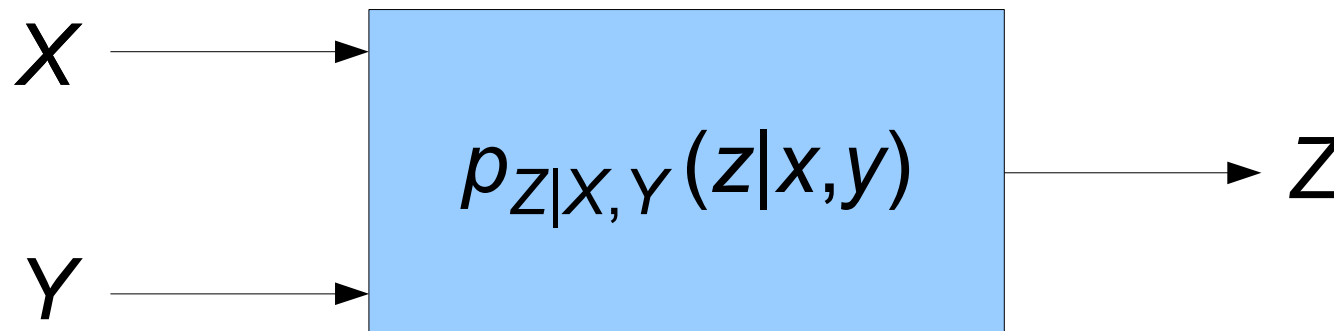
From **symmetry** of code construction, it suffices to analyze error probability for **first message**

Two kinds of error can occur:

- 1) Sequences $x^n(1)$ and y^n are not jointly typical.
Bound this by ε from LLN
- 2) Some other codeword $x^n(m')$ is jointly typical with y^n .
Gives packing bound: $|\mathcal{M}| 2^{-nI(X;Y)}$

Multiple Access Channel (MAC)

Two senders and one receiver:



- Choose codewords $\{x^n(l)\}_l$ and $\{y^n(m)\}_m$ **randomly** from typical set for X^n and Y^n , respectively
- Send codewords $x^n(l)$ and $y^n(m)$ over **IID** channel $p_{Z|X,Y}(z|x,y)$
- Receiver exploits **simultaneous decoding**

Error Analysis for MAC

A **simultaneous decoder** declares that messages l and m were sent if they are the unique messages such that

$$(x^n(l), y^n(m), z^n) \in T_\delta^{X^n Y^n Z^n}$$

Four kinds of error can occur:

- 1) Sequences $x^n(1)$, $y^n(1)$, and z^n are not jointly typical.
Bound this by ε from LLN
- 2) $x^n(1)$ typical but some other codeword $y^n(m')$ is jointly typical with z^n : $|\mathcal{M}| 2^{-nI(Y;ZX)}$
- 3) $y^n(1)$ typical but some other codeword $x^n(l')$ is jointly typical with z^n : $|\mathcal{L}| 2^{-nI(X;ZY)}$
- 4) Some other codewords $x^n(l')$ and $y^n(m')$ are jointly typical with z^n : $|\mathcal{L}| |\mathcal{M}| 2^{-nI(XY;Z)}$

Classical Comm. Over Quantum Channels

For simplicity, let's study a channel with **classical input** and **quantum output**:

$$x \rightarrow \rho_x$$

If we use **random coding** according to $p_X(x)$ at input, then **expected density operator** at output is

$$\rho \equiv \sum_x p_X(x) \rho_x$$

Can still use **random coding** to select codebook $\{x^n(m)\}_m$, but need to design a **decoding POVM**

Holevo-Schumacher-Westmoreland Decoding POVM

Consider spectral decomposition: $\rho = \sum_z \lambda_z |z\rangle\langle z|$

Use **typical projector** for expected state:

$$\Pi_{\rho, \delta}^n \equiv \sum_{z^n \in T_\delta^{Z^n}} |z^n\rangle\langle z^n|$$

And **conditionally typical projectors** for codeword states:

$$\Pi_{\rho_{x^n}, \delta} \equiv \bigotimes_x \Pi_{\rho_x, \delta}$$

To form the elements of the **HSW decoding POVM**

$$\Lambda_m \equiv \left(\sum_{m'} \Pi_\rho \Pi_{\rho_{x^n(m')}} \Pi_\rho \right)^{-1/2} \Pi_\rho \Pi_{\rho_{x^n(m)}} \Pi_\rho \left(\sum_{m'} \Pi_\rho \Pi_{\rho_{x^n(m')}} \Pi_\rho \right)^{-1/2}$$

Error Analysis

Analyze **expectation of avg. error probability** for first message (exploit Shannon's idea):

$$\mathbb{E}_{X^n} \left[\text{Tr} \left\{ (I - \Lambda_1) \rho_{x^n(1)} \right\} \right]$$

Exploit **Hayashi-Nagaoka operator inequality** to bound the error from above by two terms:

1) Probability that codeword is not typical:

$$\text{Tr} \left\{ (I - \Pi_{\rho_{x^n(1)}, \delta}) \rho_{x^n(1)} \right\} \leq \epsilon$$

2) Probability that some other codeword is typical:

$$\mathbb{E}_{X^n} \left[\sum_{m' \neq 1} \text{Tr} \left\{ \Pi_{\rho_{x^n(m')}} \Pi_{\rho} \rho_{x^n(1)} \Pi_{\rho} \right\} \right] \leq |\mathcal{M}| 2^{-nI(X;B)}$$

Quantum Multiple Access Channel

Two **spatially separated** senders and one receiver.

Two **classical inputs** and one **quantum output**:

$$x, y \rightarrow \rho_{x,y}$$

- Choose codewords $\{x^n(l)\}_l$ and $\{y^n(m)\}_m$ **randomly** from typical set for X^n and Y^n , respectively
- Send codewords $x^n(l)$ and $y^n(m)$ over **IID** quantum MAC
- Receiver *would like* to exploit **simultaneous decoding**

Decoding POVM for Quantum MAC

How to construct it when $\rho_{x,y}$ **do not commute**?

To start, let us first suppose they *do* commute

Define the **density operators**:

$$\rho_x \equiv \sum_y p_Y(y) \rho_{x,y}$$

$$\rho_y \equiv \sum_x p_X(x) \rho_{x,y}$$

$$\rho \equiv \sum_{x,y} p_X(x) p_Y(y) \rho_{x,y}$$

And their **typical projectors**:

$$\Pi_{\rho_x^n, \delta}$$

$$\Pi_{\rho_y^n, \delta}$$

$$\Pi_{\rho, \delta}^n$$

Decoding POVM for Quantum MAC

(ctd.)

Define decoding POVM *in the commuting case* to be:

$$\Lambda_{l,m} \equiv \left(\sum_{l',m'} \Pi'_{l',m'} \right)^{-1/2} \Pi'_{l,m} \left(\sum_{l',m'} \Pi'_{l',m'} \right)^{-1/2}$$

where

$$\Pi'_{l,m} \equiv \Pi_{\rho}^n \Pi_{\rho_{x^{n(l)}}} \Pi_{\rho_{y^{n(m)}}} \Pi_{\rho_{x^{n(l)}, y^{n(m)}}}$$

Note: The above operator is **positive** if all $\rho_{x,y}$ commute.

Does not necessarily have to be otherwise.

MAC Error Analysis

Analyze **exp. of avg. error probability** for first message pair:

$$\mathbb{E}_{X^n, Y^n} \left[\text{Tr} \left\{ (I - \Lambda_{1,1}) \rho_{x^n(1), y^n(1)} \right\} \right]$$

Exploit **Hayashi-Nagaoka operator inequality** to bound the error from above by **four terms**:

1) Probability that codeword is not typical:

$$\text{Tr} \left\{ (I - \Pi_{\rho_{x^n(1), y^n(1)}, \delta}) \rho_{x^n(1), y^n(1)} \right\} \leq \epsilon$$

MAC Error Analysis (ctd.)

2) Probability that one message detected correctly but the other incorrectly:

$$\mathbb{E}_{X^n, Y^n} \left[\sum_{m' \neq 1} \text{Tr} \left\{ \Pi_{\rho_{x^n(1), y^n(m')}} \Pi_{\rho_{x^n(1)}} \rho_{x^n(1), y^n(1)} \Pi_{\rho_{x^n(1)}} \right\} \right] \leq |\mathcal{M}| 2^{-nI(Y; BX)}$$

3) Symmetric case:

$$\mathbb{E}_{X^n, Y^n} \left[\sum_{l' \neq 1} \text{Tr} \left\{ \Pi_{\rho_{x^n(l'), y^n(1)}} \Pi_{\rho_{y^n(1)}} \rho_{x^n(1), y^n(1)} \Pi_{\rho_{y^n(1)}} \right\} \right] \leq |\mathcal{L}| 2^{-nI(X; BY)}$$

4) Probability that both detected incorrectly:

$$\mathbb{E}_{X^n, Y^n} \left[\sum_{l', m' \neq 1} \text{Tr} \left\{ \Pi_{\rho_{x^n(l'), y^n(m')}} \Pi_{\rho} \rho_{x^n(1), y^n(1)} \Pi_{\rho} \right\} \right] \leq |\mathcal{L}| |\mathcal{M}| 2^{-nI(XY; B)}$$

Quantum Simultaneous Decoding Conjecture

There exists a **doubly-indexed decoding POVM**

$$\{\Lambda_{l,m}\}$$

such that the following **error probability** is small:

$$\mathbb{E}_{X^n, Y^n} \left[\text{Tr} \left\{ (I - \Lambda_{1,1}) \rho_{x^n(1), y^n(1)} \right\} \right]$$

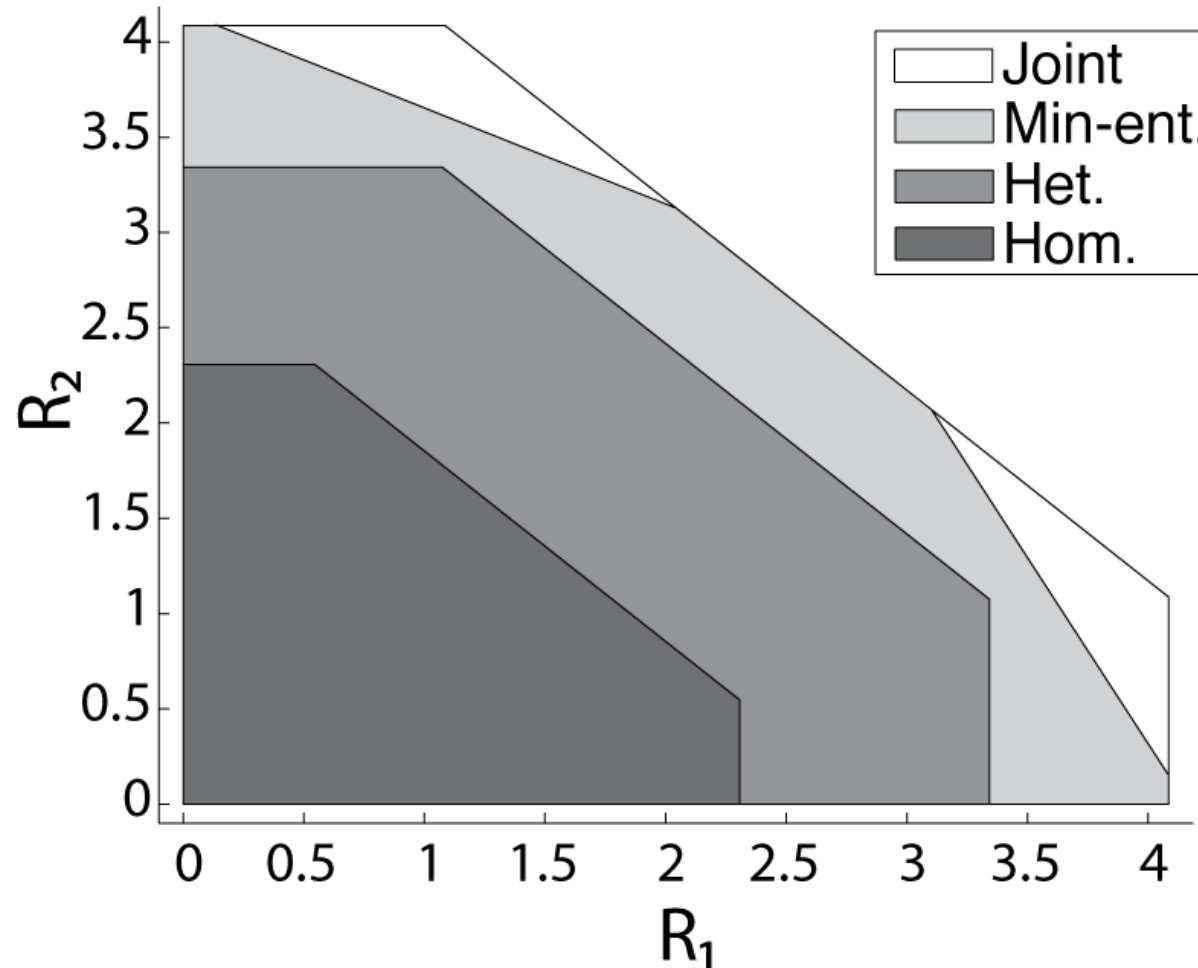
regardless of whether $\rho_{x,y}$ s commute

Tried to prove this in *many* ways (see arXiv:1102.2624)

- 1) simple way with **Gentle Operator Lemma** accumulates errors
- 2) **smooth min-entropies** (à la Renner)
- 3) **Feinstein approach** (à la Lloyd *et al.*)

Notable Success in Bosonic Comm.

Strong interference – high power



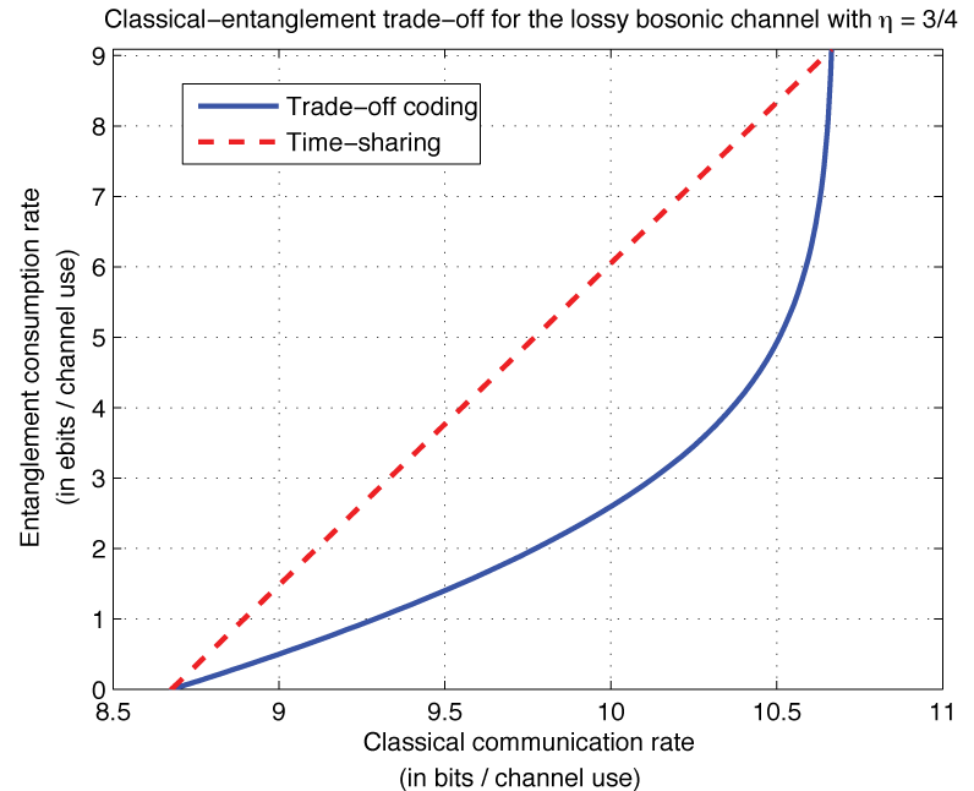
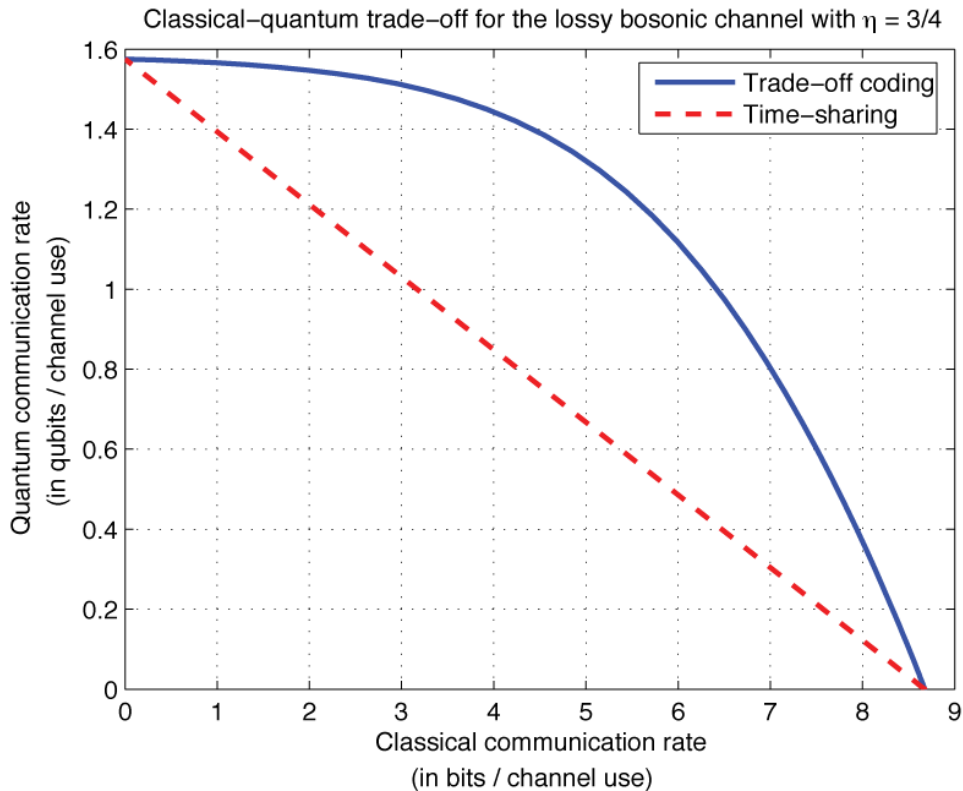
A min-entropy decoder can outperform classical strategies in the context of comm. over a **bosonic interference channel**

Conclusion

Solving this conjecture would allow us to import many results from **network information theory** for use in **quantum information theory**

For a **related conjecture** in multiparty state transfer, see the *PhD thesis* of *Nicolas Dutil* or **arXiv:1011.1974**

Advertisement of New Results



Trade-off coding for a **lossy bosonic channel** gives a remarkable gain over **time-sharing**