Quantum channels from subfactors

Pieter Naaijkens

Universidad Complutense de Madrid

21 March 2019

This work was funded by the ERC (grant agreement No 648913)

Three cultures

Type I_n: everything finite dimensional
(no infinite resources)

Type I_∞: separable Hilbert space
(e.g. quantum particle on line)

Type III: focus on algebra of observables
(particularly useful with infinite # d.o.f.)

Thanks to Reinhard Werner for this characterisation.

Quantum information

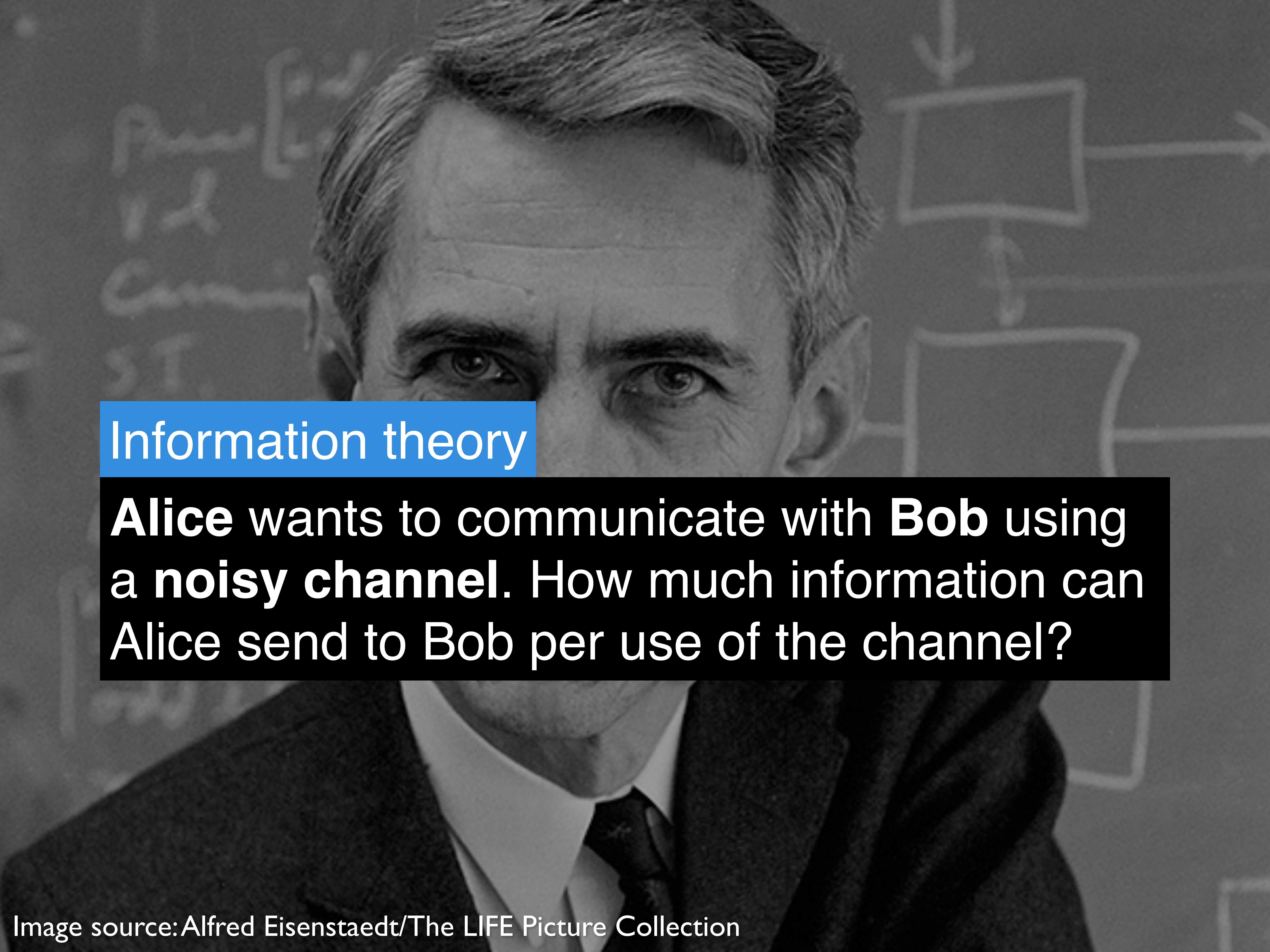
- use **quantum** systems to communicate
- main question: how much information can I transmit?
- will consider infinite systems here…
- … described by subfactors
- channel capacity is given by Jones index

Outline

Classical information theory

Subfactors and QI

Classical information theory



Information theory

Alice wants to communicate with **Bob** using a **noisy channel**. How much information can Alice send to Bob per use of the channel?

Image source: Alfred Eisenstaedt/The LIFE Picture Collection

Setup

Alice

$p(y|x)$

Bob

$\mathcal{X}$ input space

$\{p_x\}_{x\in\mathcal{X}}$

$\mathcal{Y}$ output space

$$p_y = \sum_{x\in\mathcal{X}} p(y|x)$$

How well can Bob recover the messages sent by Alice (small error allowed)?

Shannon entropy

Def: $$H(X) = -\sum_x p_x \log p_x$$

Measure for the **information content** of *X*

Coding: represent tuples in X^n by codewords

$$N \sim 2^{nH(X)}$$

(asymptotically, error goes to zero!)

Relative entropy

Compare two probability distributions *P*, *Q*:

$$H(P:Q) = \begin{cases} \sum p_x \log \frac{p_x}{q_x} & \{x : p_x > 0\} \subset \{x : q_x > 0\} \\ +\infty & \text{else} \end{cases}$$

Vanishes iff *P*=*Q*, otherwise positive

Mutual information

`information' due to noise

$$I(X:Y) = H(Y) - H(X|Y)$$

here the conditional entropy is defined:

$$H(Y|X) = \sum_x p_x H(Y|X=x)$$

some algebra gives: $P'_x = \{p(y|x)\}$ $\quad P' = \sum_x p_x P'_x$

$$I(X:Y) = \sum_x p_x H(P'_x : P')$$

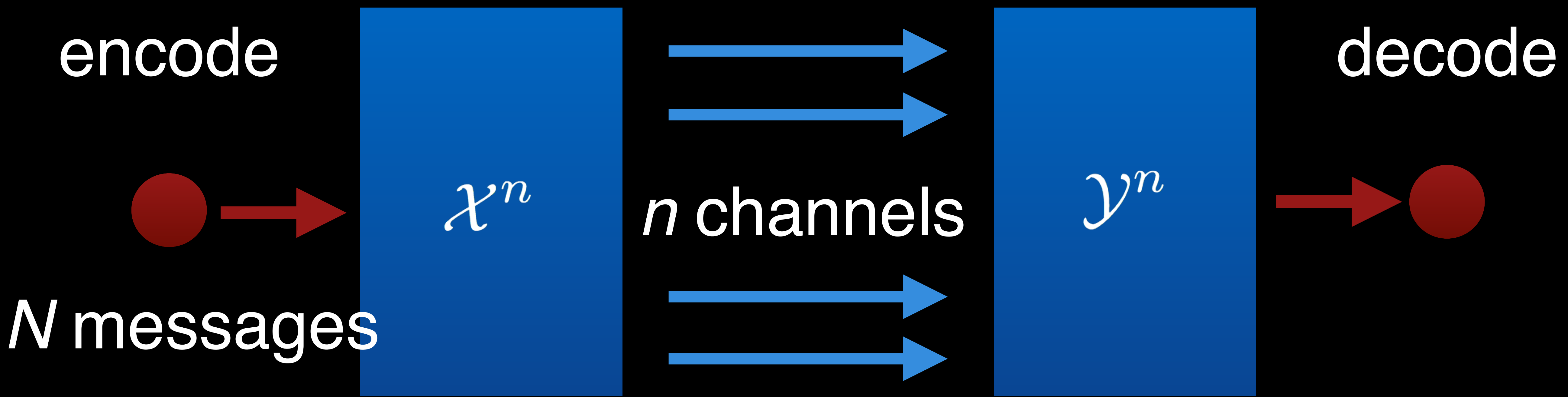
Channel capacities

What is the maximum amount of information we can send through the channel?

Def: the *Shannon capacity* of the channel is defined as:

$$C_{Shan} = \max_X I(X:Y)$$

Operational approach



Maximum error for *all* possible encodings:

$$p_e(n, N)$$

Coding theorem

Def: *R* is called an *achievable rate* if

$$\lim_{n\to\infty} p_e(n, 2^{nR}) = 0$$

The supremum of all *R* is called the **capacity** *C*.

$$C = C_{Shan}$$

Quantum information

Quantum information

- work mainly in the **Heisenberg picture**
- observables modelled by **von Neumann algebra**
- consider **normal states** on $\mathfrak{M}$
- channels are normal unital CP maps $\mathcal{E} : \mathfrak{M} \to \mathfrak{N}$
- Araki **relative entropy** $S(\omega, \phi)$

Araki relative entropy

Let ω, ϕ be faithful normal states:

Def:
$$S_{\varphi,\omega} : x\xi_\varphi \mapsto x^*\xi_\omega$$
$$\Delta(\varphi,\omega) = S_{\varphi,\omega}\overline{S}^*_{\varphi,\omega}$$

Def:
$$S(\varphi,\omega) := -\langle \xi_\phi, \log\Delta(\varphi,\omega), \xi_\phi\rangle$$
$$= i \lim_{t\to 0^+} t^{-1}(\varphi([D\omega : D\varphi]_t) - 1)$$

$$S(\rho,\sigma) = \mathrm{Tr}(\rho\log\rho - \rho\log\sigma)$$

Distinguishing states

Alice prepares a mixed state ρ:

$$\rho = \sum_{i=1}^{n} p_i \rho_i$$

…and sends it to Bob

Can Bob recover $\{p_i\}$?

Holevo χ quantity

In general not exactly:

$$\chi(\{p_i\},\{\rho_i\}) := S(\rho) - \sum_i p_i S(\rho_i)$$

$$= \sum_i p_i S(\rho_i, \rho)$$

Generalisation of **Shannon information**

Infinite systems

Suppose $\mathfrak{M}$ is an infinite factor, say Type III, and φ a faithful normal state

$$\sup_{(\varphi_i)} \sum p_x S(\varphi_x, \varphi) = \infty$$

Better to compare algebras!

Comparing algebras

Want to compare $\widehat{\mathcal{R}}$ and $\mathcal{R}$, with $\mathcal{R} \subset \widehat{\mathcal{R}}$ subfactor

$$H_\phi(\widehat{\mathcal{R}}|\mathcal{R}) = \sup_{(\phi_i)} \left(\sum_i [S(p_i\phi_i, \phi) - S(p_i\phi_i \restriction \mathcal{R}, \phi \restriction \mathcal{R})] \right)$$

$$= \sup_{(\phi_i)} \underbrace{(\chi(\{p_i\}, \{\phi_i\}) - \chi(\{p_i\}, \{\phi_i \restriction \mathcal{R}\}))}_{\Delta_\chi}$$

Shirokov & Holevo, arXiv:1608.02203

A quantum channel

For finite index inclusion $\mathcal{R} \subset \widehat{\mathcal{R}}$, say *irreducible,*

$$\mathcal{E} : \widehat{\mathcal{R}} \to \mathcal{R}, \qquad \mathcal{E}(X^* X) \geq \frac{1}{[\widehat{\mathcal{R}} : \mathcal{R}]} X^* X$$

quantum channel, describes the **restriction** of operations

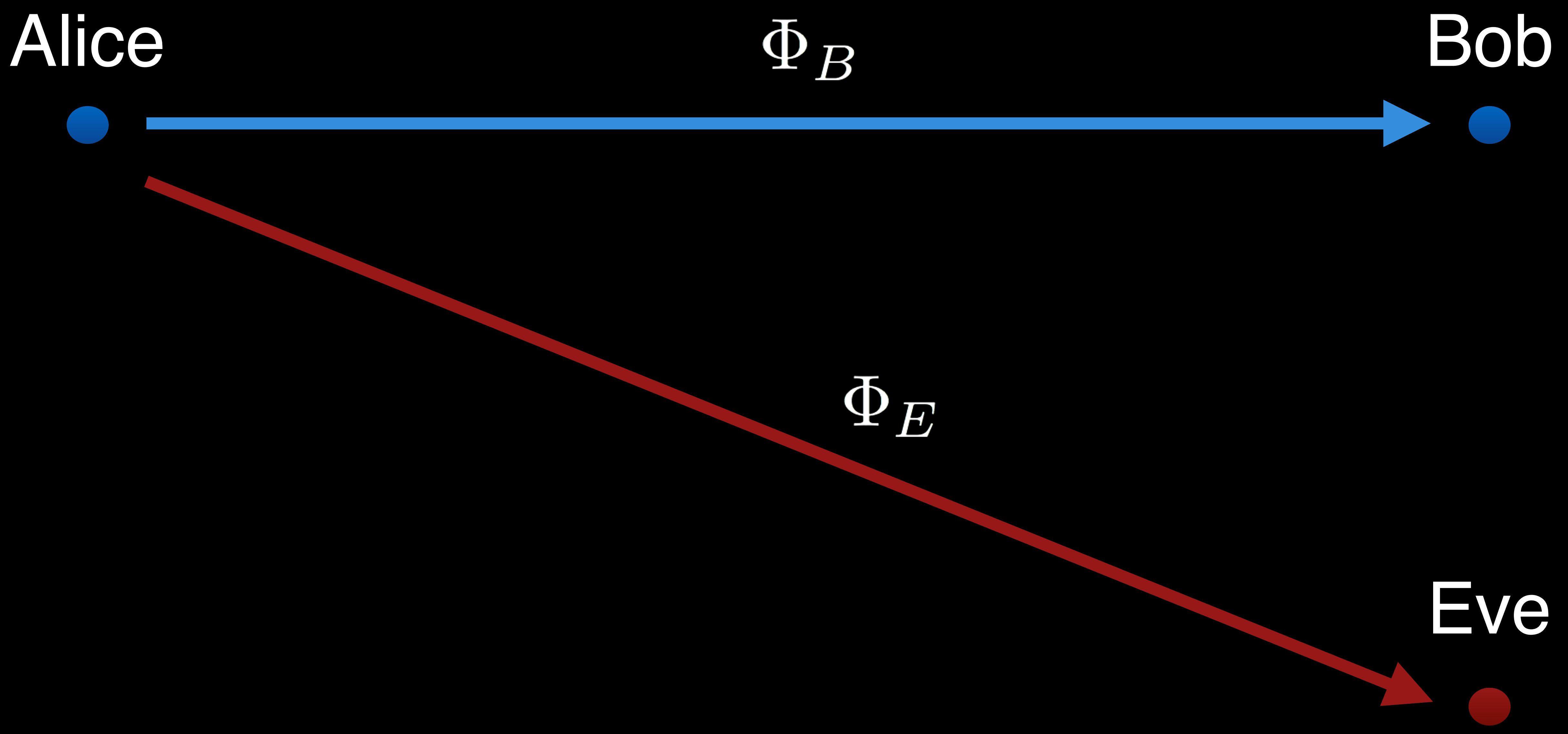
Jones index and entropy

$$\log[\widehat{\mathcal{R}} : \mathcal{R}] = \sup_{\phi:\phi\circ\mathcal{E}=\phi} H_\phi(\widehat{\mathcal{R}}|\mathcal{R})$$

Hiai, J. Operator Theory, ’90; J. Math. Soc. Japan, ‘91

gives an **information-theoretic** interpretation to the Jones index

Quantum wiretapping



Theorem (Devetak, Cai/Winter/Young)

The rate of a wiretapping channel is given by

$$\lim_{n\to\infty} \frac{1}{n} \max_{\{p_x,\rho_x\}} \left(\chi(\{p_x\}, \Phi_B^{\otimes n}(\rho_x)\}) - \chi(\{p_x\}, \Phi_E^{\otimes n}(\rho_x)\})\right)$$

A conjecture

The Jones index $[\mathfrak{M} : \mathfrak{N}]$ of a subfactor gives the classical capacity of the wiretapping channel that restricts from $\mathfrak{M}$ to $\mathfrak{N}$.

L. Fiedler, PN, T.J. Osborne, New J. Phys **19**:023039 (2017)
PN, Contemp. Math. **717**, pp. 257-279 (2018), arXiv:1704.05562

Some remarks

- use entropy formula by Hiai
- together with properties of the index

$$[\widehat{\mathcal{R}}^{\otimes n} : \mathcal{R}^{\otimes n}] = [\widehat{\mathcal{R}} : \mathcal{R}]^n$$

- averaging drops out: **single letter formula**
- coding theorem is missing