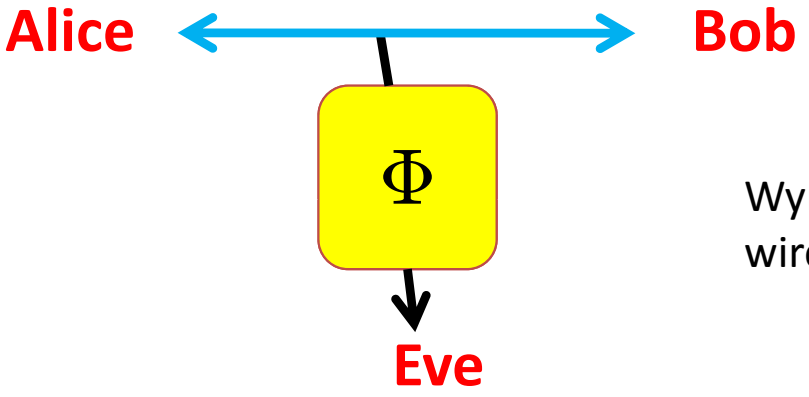
A strong converse for coding with entangled inputs

Robert König

joint work with Stephanie Wehner
arXiv:0903.2838

Caltech, 03/2010

(Our) motivation: uncertainty as a resource



Wyner's wiretap channel

- **How** can Alice and Bob exploit Eve's noise to obtain privacy?

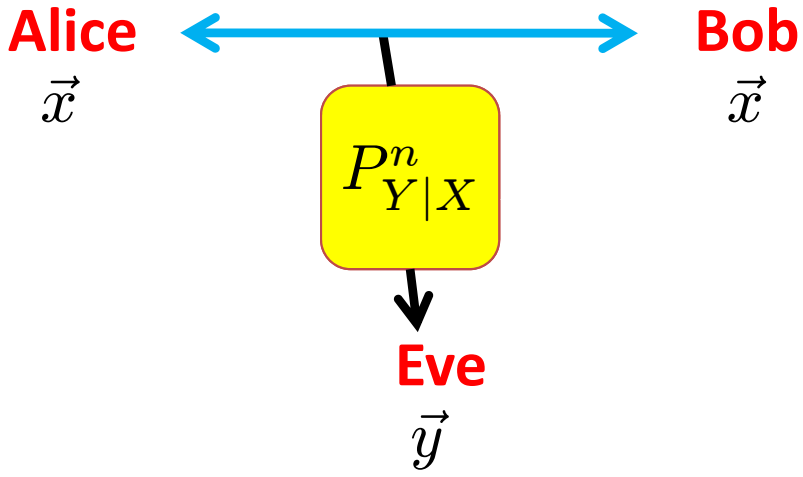
(non)-interactive two-party protocol

Topic of this talk:

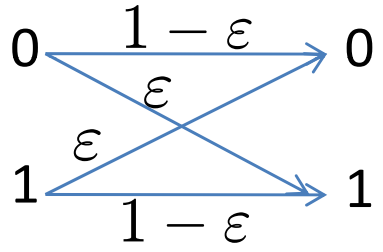
- **How much** privacy can they obtain?

$$\textit{Key rate} = \frac{\text{\# of generated secret bits}}{\text{\# of channel uses}}$$

Example: bit-flip channel with probability ε



$P_{Y|X}$



Key generation protocol:

1. setup: Alice flips n coins

$$\vec{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$$

and transmits them to Bob

2. extraction: Alice and Bob compute $z = \sum_i x_i \bmod 2$

- **How** can Alice and Bob exploit Eve's noise to obtain privacy?

(non)-interactive two-party protocol

- **How much** privacy can they obtain?

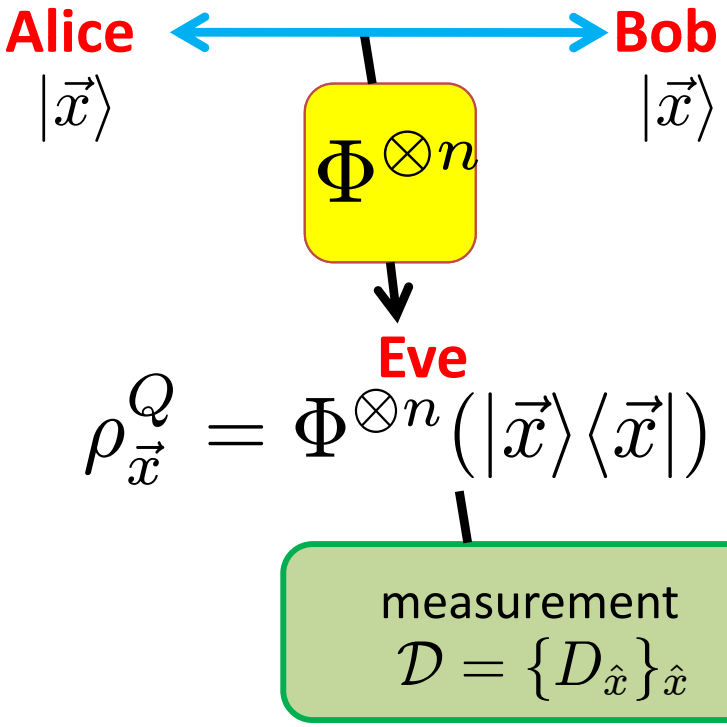
Key rate= $\dfrac{\text{\# of generated secret bits}}{\text{\# of channel uses}}$

$\approx h(\varepsilon)$ asymptotically

even with the best "decoding" strategy d Eve's probability of correctly guessing z is

$$\max_{d:\{0,1\}^n \to \{0,1\}} \Pr_{\vec{x}}[d(\vec{y}) = z] \leq \frac{1}{2} + \frac{1}{2}(1-2\varepsilon)^n$$

Optimal key generation protocols and uncertainty



situation described by state/ensemble

$\{P_X(x), \rho^Q_x\}_x$

1. **setup:** Alice chooses $\vec{x} = (x_1, \ldots, x_n)$ and transmits it to Bob

2. **extraction:** Alice and Bob use optimal protocol

"guessing uncertainty" $\hat{x} \overset{???}{=} \vec{x}$

# of extractable key bits is equal to **Eve's uncertainty** $H^\varepsilon_\infty(X|Q)$ about X

measure: (smooth) *min-entropy*

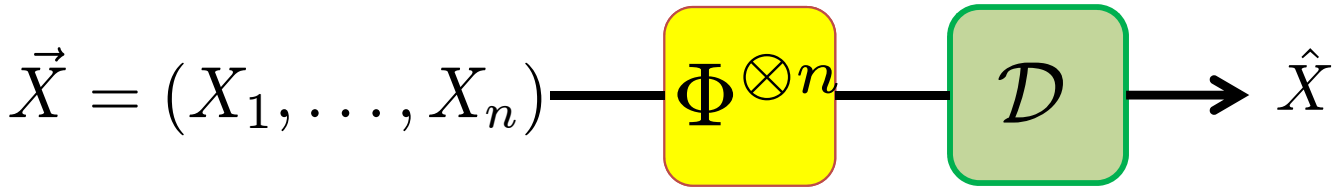
$$H_\infty(X|Q) = -\log \max_{\mathcal{D}} \Pr_x [\mathcal{D}(\rho^Q_x) = x]$$

optimal average guessing probability

$$\max_{\mathcal{D}=\{D_x\}_x \text{ POVM}} \sum_x P_X(x) \mathrm{tr}(D_x \rho^Q_x)$$

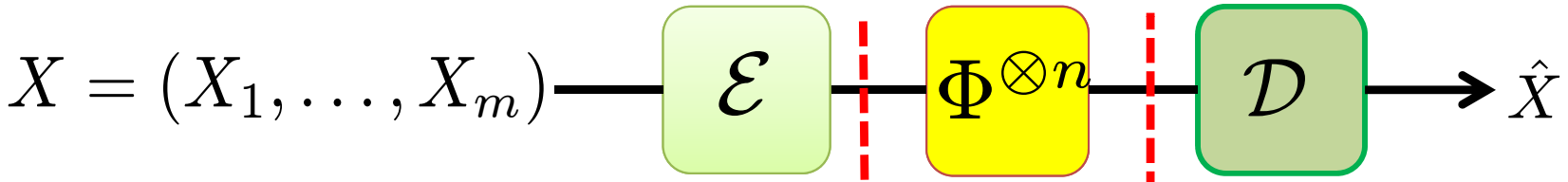
Relation to coding for $\Phi : \mathbf{B}(\mathcal{H}_{in}) \to \mathbf{B}(\mathcal{H}_{out})$

previous setting:



Relation to coding for $\Phi : \mathbf{B}(\mathcal{H}_{in}) \to \mathbf{B}(\mathcal{H}_{out})$

allow arbitrary encoding operation =**channel coding**



Ensemble:

$$P_X(x) = \frac{1}{2^m}$$

$$x \in \{0,1\}^m$$

codewords

$$\rho_x^{Q_{in}} = \mathcal{E}(|x\rangle) \quad \text{on } \mathcal{H}_{in}^{\otimes n}$$

noisy codewords

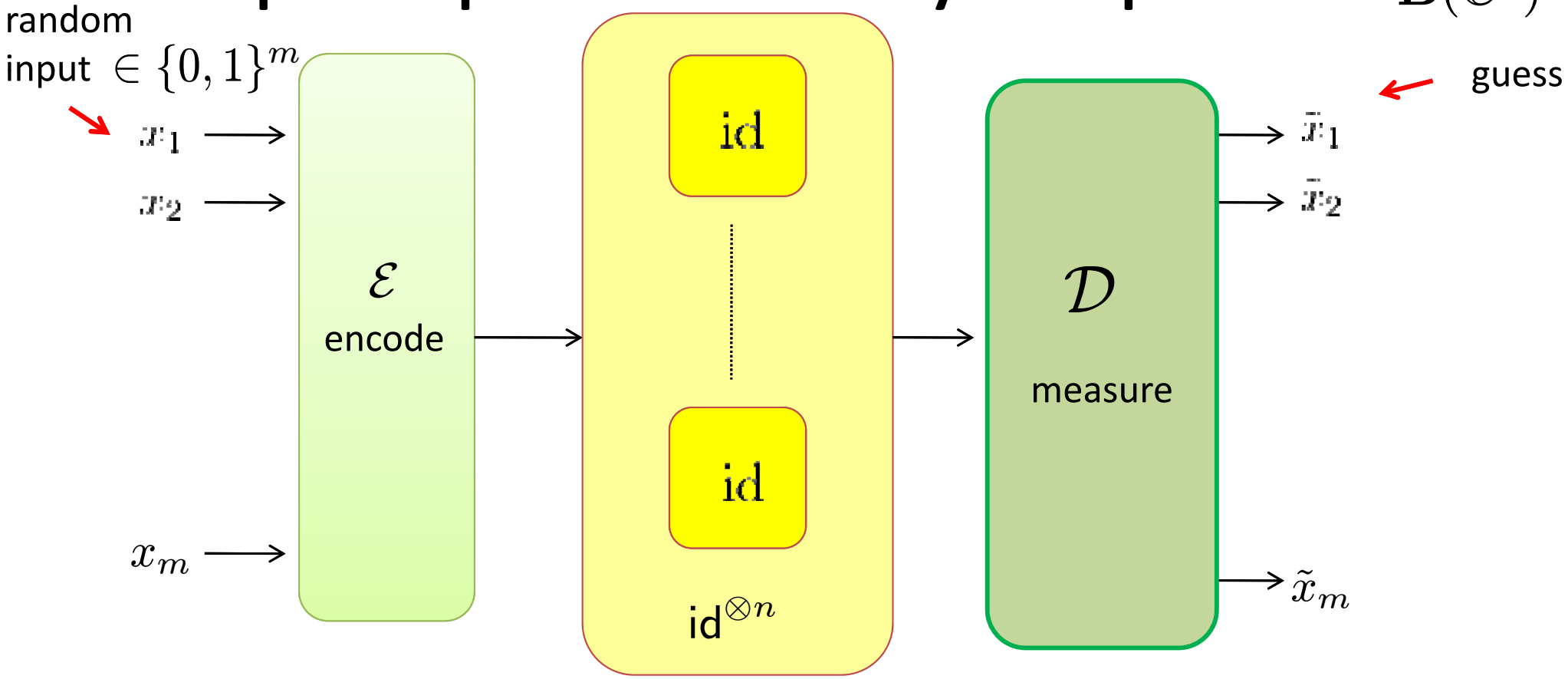
$$\rho_x^{Q_{out}} = \Phi^{\otimes n}(\rho_x^{Q_{in}}) \quad \text{on } \mathcal{H}_{out}^{\otimes n}$$

Problem: find **upper bound** on decoding probability

$$\max_{\mathcal{E},\mathcal{D}} \Pr_{x \in \{0,1\}^m} \left[(\mathcal{D} \circ \Phi^{\otimes n} \circ \mathcal{E})(x) = x \right]$$

as a function of m,n or the ***rate*** $R = \frac{m}{n}$

Example: qubit identity map $\Phi = \mathrm{id}_{\mathbf{B}(\mathbb{C}^2)}$



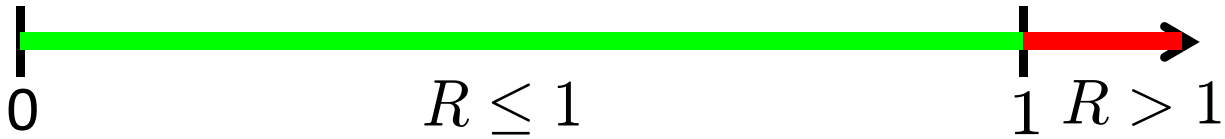
(Holevo '73)

encoding

$$|\vec{x}\rangle \mapsto |\vec{x}\rangle|0\rangle^{\otimes n-m}$$

allows **perfect decoding**

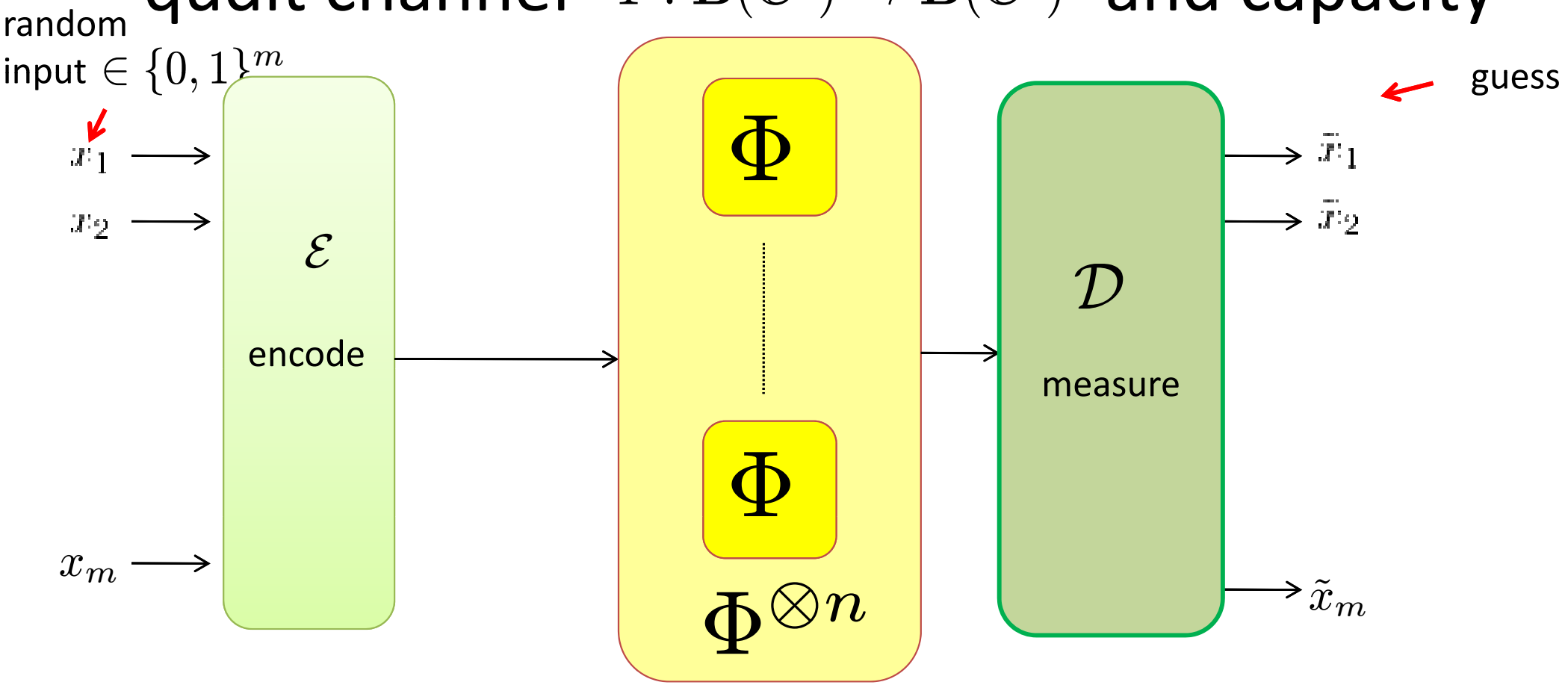
no encoding allows perfect decoding



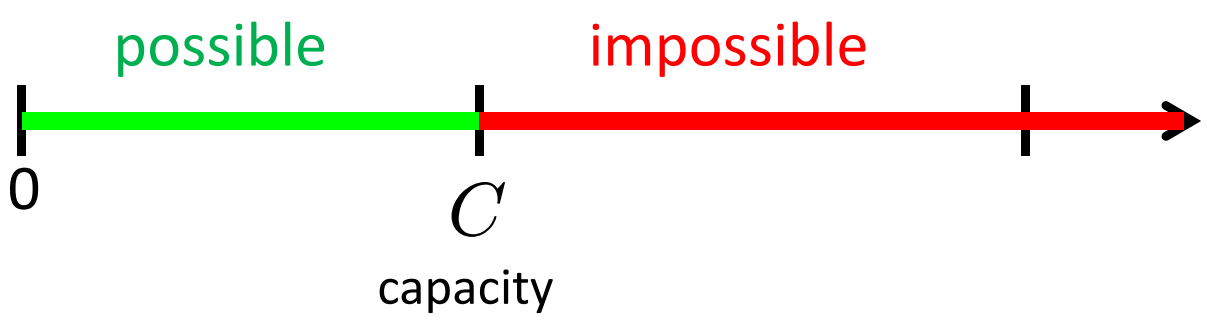
rate

$$R = \frac{m}{n}$$

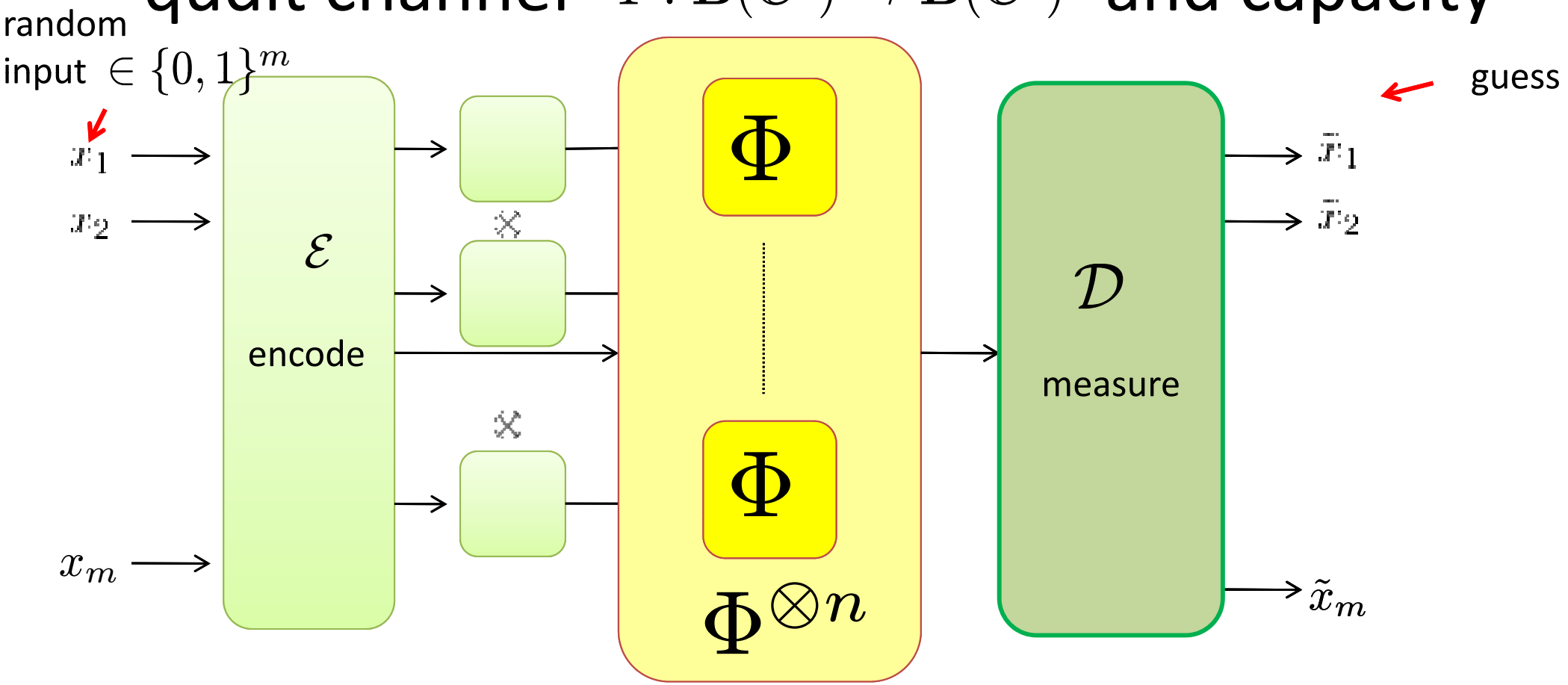
qudit channel $\Phi : \mathbf{B}(\mathbb{C}^d) \to \mathbf{B}(\mathbb{C}^d)$ and capacity



asymptotically:
error-free
decoding



qudit channel $\Phi : \mathbf{B}(\mathbb{C}^d) \to \mathbf{B}(\mathbb{C}^d)$ and capacity



asymptotically:
error-free
decoding

possible with ***product***-state encodings

possible with ***entangled*** codewords

impossible

rate

$$R = \frac{m}{n}$$

Some information-theoretic quantities

relative entropy

$$D(\rho\|\sigma) = \mathrm{tr}(\rho(\log\rho - \log\sigma))$$

Holevo quantity for ensembles

$$\rho_{XQ} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_x^Q$$

$$\chi(\rho_{XQ}) = \min_{\sigma_Q} D(\rho_{XQ}\|\rho_X \otimes \sigma_Q)$$

=upper bound on accessible (Shannon)-information

Holevo quantity for channels

$$\Phi : \mathbf{B}(\mathbb{C}^d) \to \mathbf{B}(\mathbb{C}^d)$$

$$\chi^*(\Phi) = \max_{\rho_{XQ}} \chi\left((\mathrm{id} \otimes \Phi)(\rho_{XQ})\right)$$

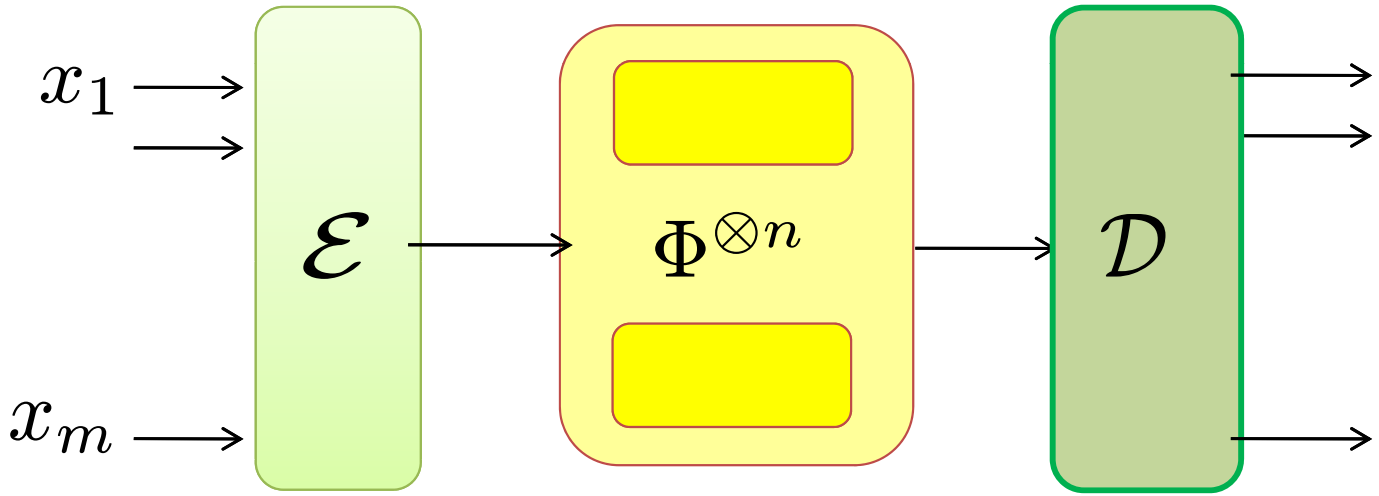
=product-state capacity C_{prod}

regularized Holevo quantity

$$\bar{\chi}^*(\Phi) = \lim_{n\to\infty} \frac{1}{n}\chi^*(\Phi^{\otimes n})$$

=capacity C

Weak converse to channel coding (Holevo'73)



general:

$$\max_{\mathcal{E},\mathcal{D}} \Pr_{x\in\{0,1\}^m} [(\mathcal{D}\circ\Phi^{\otimes n}\circ\mathcal{E})(x)=x] < 1 \quad \text{for } R > C$$

for *coding with product states*:

$$\max_{\mathcal{E}_{\mathbf{prod}},\mathcal{D}} \Pr_{x} [(\mathcal{D}\circ\Phi^{\otimes n}\circ\mathcal{E}_{\mathbf{prod}})(x)=x] < 1 \quad \text{for } R > C_{\mathbf{prod}}$$

error-free decoding

possible with ***product***-state encodings

possible with ***entangled*** codewords

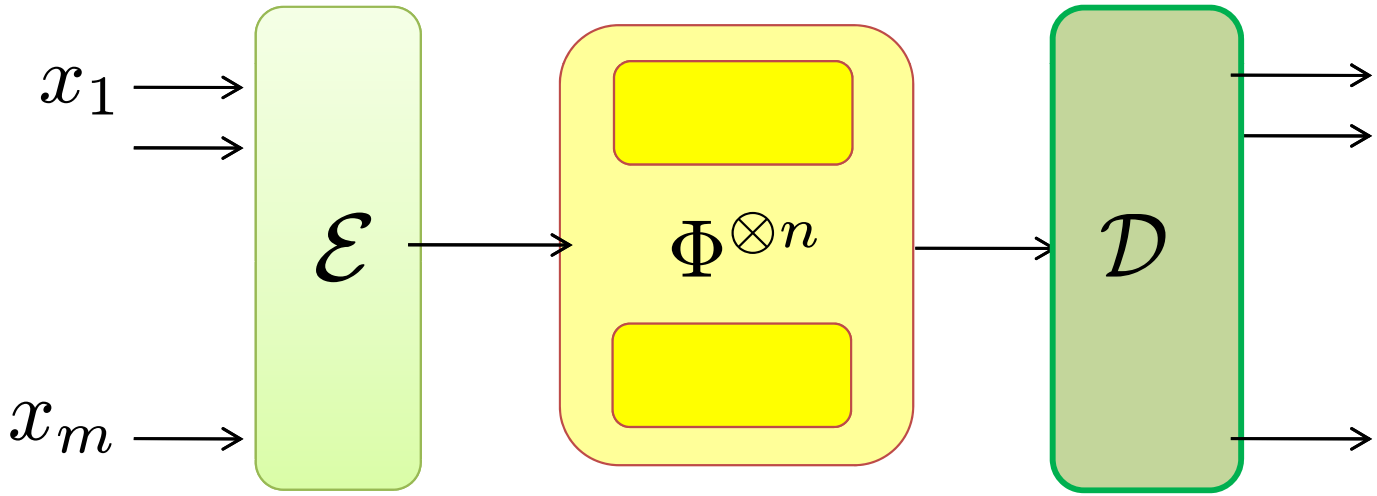
impossible

rate

$$R = \frac{m}{n}$$

0 C_{prod} C $\log_2 d$

Strong converse (statement) to channel coding



general: $\exists \gamma > 0$

$$\max_{\mathcal{E},\mathcal{D}} \Pr_{x \in \{0,1\}^m} \left[(\mathcal{D} \circ \Phi^{\otimes n} \circ \mathcal{E})(x) = x \right] < 2^{-n\gamma(R-C)}$$

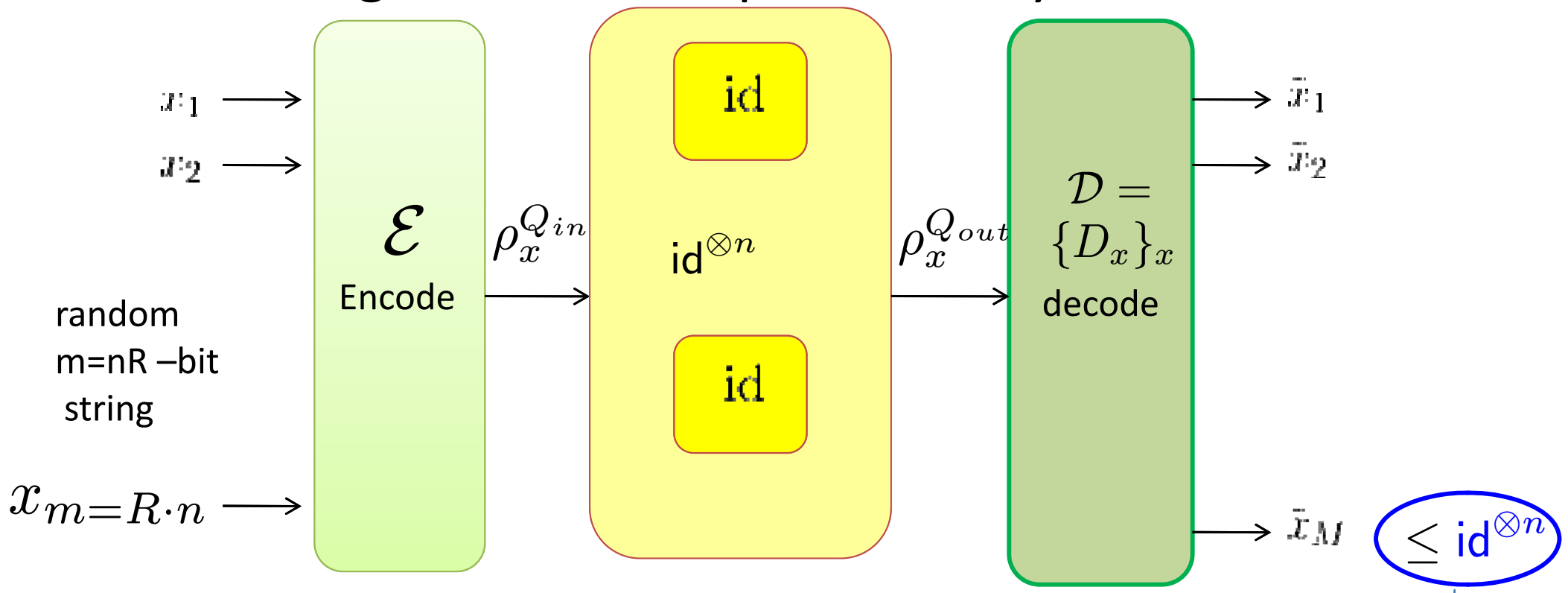
established for:
- classical channels (Wolfowitz'64)
- qudit identity channel

for *coding with product states*:

$$\max_{\mathcal{E}_{\mathbf{prod}},\mathcal{D}} \Pr_{x} \left[(\mathcal{D} \circ \Phi^{\otimes n} \circ \mathcal{E}_{\mathbf{prod}})(x) = x \right] < 2^{-n\gamma(R-C_{\mathbf{prod}})}$$

established for arbitrary quantum channels
(Winter '99, Ogawa & Nagaoka '99)

Proof of strong converse for qubit identity channel $\longleftrightarrow$ BSM



$$\Pr_{x\in\{0,1\}^m}\left[(\mathcal{D}\circ\Phi^{\otimes n}\circ\mathcal{E})(x)=x\right]=\frac{1}{2^{nR}}\sum_{x\in\{0,1\}^{nR}}\mathrm{tr}(D_x\rho_x^{Q_{out}})$$

$$\leq \frac{1}{2^{nR}}\sum_x \mathrm{tr}(D_x\mathrm{id}^{\otimes n})$$

$$\sum_x D_x = \mathrm{id}^{\otimes n}$$

$$= \frac{1}{2^{nR}}\mathrm{tr}(\mathrm{id}^{\otimes n})$$

$$= 2^{-n(R-1)}$$

Key step:

common bound

on states in ensemble leads to bound for all POVMs

Main result: strong converse for a class of quantum channels

Theorem: if $\Phi : \mathcal{B}(\mathcal{H}_{in}) \to \mathcal{B}(\mathcal{H}_{out})$ has

additive minimum output Rényi entropy

$$S_\alpha^{\min}(\Phi^{\otimes n}) = n \cdot S_\alpha^{\min}(\Phi)$$

$$\alpha \geq 1$$

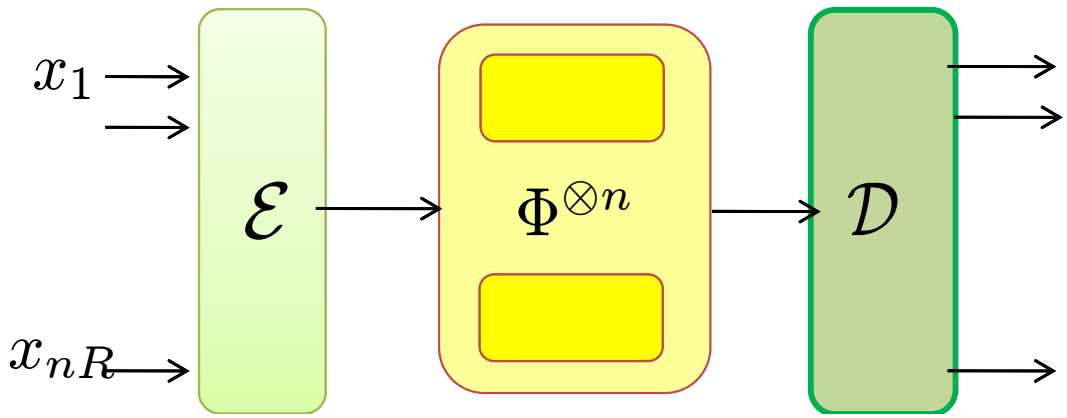
& covariance property

$$g\Phi(\rho)g^\dagger = \Phi(g\rho g^\dagger)\ \forall g$$

wrt. representations of a group G, irreducible on $\mathcal{H}_{out}$

then strong converse property holds: $\exists \gamma > 0$

$$\max_{\mathcal{E},\mathcal{D}} \Pr_{\vec{x}\in\{0,1\}^{nR}} [(\mathcal{D} \circ \Phi^{\otimes n} \circ \mathcal{E})(\vec{x}) = \vec{x}] \leq 2^{-n\gamma(R-C)}$$



e.g.,

- qudit depolarizing channel $\Phi_\varepsilon(\rho) = (1-\varepsilon)\rho + \varepsilon \cdot \frac{\mathrm{id}}{d}$
- any unital qubit channel
- Werner-Holevo channel

Main result: strong converse for a class of quantum channels

Theorem: if $\Phi : \mathcal{B}(\mathcal{H}_{in}) \to \mathcal{B}(\mathcal{H}_{out})$ has

additive minimum output Rényi entropy

$$S_\alpha^{\min}(\Phi) = \min_\rho \frac{1}{1-\alpha} \log \mathrm{tr}\Phi(\rho)^\alpha$$

& covariance property

$$g\Phi(\rho)g^\dagger = \Phi(g\rho g^\dagger)\ \forall g$$

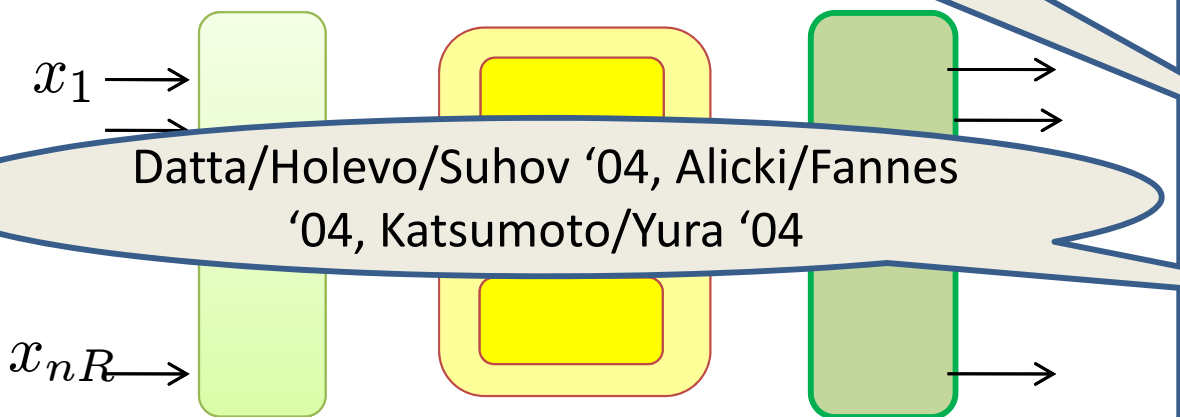
wrt. representations of a group G, irreducible on $\mathcal{H}_{out}$

then strong converse property holds: $\exists \gamma > 0$

$$\max_{\mathcal{E},\mathcal{D}} \Pr_{\vec{x}\in\{0,1\}^{\cdot}} [(\mathcal{D}\circ\Phi^{\otimes n}\circ\mathcal{E})(\vec{x}) \quad \geq 2^{n\gamma(R-C)}$$

King, JMP '02 + King/Ruskai IEEE IT '01

King, IEEE IT, '03



Datta/Holevo/Suhov '04, Alicki/Fannes '04, Katsumoto/Yura '04

e.g.,

- qudit depolarizing channel $\Phi_\varepsilon(\rho) = (1-\varepsilon)\rho + \varepsilon \cdot \frac{\mathrm{id}}{d}$
- any unital qubit channel
- Werner-Holevo channel

Outline of rest of talk

- α-Holevo quantities and their properties

- connecting α-Holevo quantities to the coding problem

- proof of strong converse: reduction to additivity of α-Holevo quantities

Some information-theoretic quantities

relative entropy

$$D(\rho\|\sigma) = \mathrm{tr}(\rho(\log\rho - \log\sigma))$$

Holevo quantity (for ensembles)

$$\chi(\rho_{XQ}) = \min_{\sigma_Q} D(\rho_{XQ}\|\rho_X \otimes \sigma_Q)$$

=upper bound on accessible (Shannon)-information

Holevo quantity (for channels)

$$\chi^*(\Phi) = \max_{\rho_{XQ}} \chi\left((\mathrm{id}\otimes\Phi)(\rho_{XQ})\right)$$

=product-state capacity C_{prod}

regularized Holevo quantity

$$\bar{\chi}^*(\Phi) = \lim_{n\to\infty} \frac{1}{n}\chi^*(\Phi^{\otimes n})$$

=capacity C

A useful relation

(Schumacher & Westmoreland '01)

$$D(\rho\|\sigma) = \mathrm{tr}(\rho(\log\rho - \log\sigma)) \geq 0 \quad \text{equality iff} \quad \rho = \sigma$$

$$D(\rho_{XQ}\|\rho_X \otimes \sigma_Q) = D(\rho_{XQ}\|\rho_X \otimes \rho_Q) + \underbrace{D(\rho_Q\|\sigma_Q)}_{\geq 0}$$

insert explicit expression for **minimum:**

$$\sigma_Q^{\min} = \rho_Q$$

$$\chi(\rho_{XQ}) = \min_{\sigma_Q} D(\rho_{XQ}\|\rho_X \otimes \sigma_Q)$$

$$= D(\rho_{XQ}\|\rho_X \otimes \rho_Q)$$

$$= S(\rho_Q) - \sum_x P_X(x) S(\rho_x)$$

Some information-theoretic quantities

relative entropy

$$D(\rho\|\sigma) = \mathrm{tr}(\rho(\log\rho - \log\sigma))$$

Holevo quantity (for ensembles)

$$\chi(\rho_{XQ}) = \min_{\sigma_Q} D(\rho_{XQ}\|\rho_X \otimes \sigma_Q)$$

$$= S(\rho_Q) - \sum_x P_X(x) S(\rho_x)$$

=upper bound on accessible (Shannon)-information

Holevo quantity (for channels)

$$\chi^*(\Phi) = \max_{\rho_{XQ}} \chi((\mathrm{id}\otimes\Phi)(\rho_{XQ}))$$

$$= \min_\sigma \max_\rho D(\Phi(\rho)\|\sigma)$$

=product-state capacity C_{prod}

regularized Holevo quantity

$$\bar{\chi}^*(\Phi) = \lim_{n\to\infty} \frac{1}{n}\chi^*(\Phi^{\otimes n})$$

=capacity C

Some more information-theoretic quantities

$\alpha \geq 1$

relative α-entropy

$$D_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1}\log \mathrm{tr}(\rho^\alpha \sigma^{1-\alpha})$$

α-Holevo quantity (for ensembles)

$$\chi_\alpha(\rho_{XQ}) = \min_{\sigma_Q} D_\alpha(\rho_{XQ}\|\rho_X \otimes \sigma_Q)$$

↔upper bound on

$$\max_{\mathcal{D}} \ \Pr_x[\mathcal{D}(\rho_x^Q) = x]$$

α-Holevo quantity (for channels)

$$\chi^*_\alpha(\Phi) = \max_{\rho_{XQ}} \chi_\alpha\left((\mathrm{id}\otimes\Phi)(\rho_{XQ})\right)$$

↔ upper bound on single-shot

$$\max_{\mathcal{E},\mathcal{D}} \ \Pr_x[\mathcal{D}\circ\Phi\circ\mathcal{E}(x) = x]$$

regularized α-Holevo quantity

$$\bar{\chi}^*_\alpha(\Phi) = \lim_{n\to\infty} \frac{1}{n}\chi^*_\alpha(\Phi^{\otimes n})$$

↔ asymptotic upper bound on

$$\max_{\mathcal{E},\mathcal{D}} \ \Pr_x[\mathcal{D}\circ\Phi^{\otimes n}\circ\mathcal{E}(x) = x]$$

A useful relation (again)

$$D_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1}\log \mathrm{tr}(\rho^\alpha \sigma^{1-\alpha}) \geq 0$$ equality iff $\rho = \sigma$

$$D_\alpha(\rho_{XQ}\|\rho_X \otimes \sigma_Q) = D_\alpha(\rho_{XQ}\|\rho_X \otimes \rho_Q) + \underbrace{D_\alpha(\mu_Q\|\sigma_Q)}_{\geq 0}$$

insert explicit expression for **minimum:**

$$\sigma_Q^{\min} = \mu_Q \propto \left(\sum_x P_X(x)\rho_x^\alpha\right)^{1/\alpha}$$

$$\chi_\alpha(\rho_{XQ}) = \min_{\sigma_Q} D_\alpha(\rho_{XQ}\|\rho_X \otimes \sigma_Q)$$

$$= D_\alpha(\rho_{XQ}\|\rho_X \otimes \mu_Q)$$

$$= \frac{\alpha}{\alpha-1}\log \mathrm{tr}\left(\sum_x P_X(x)\rho_x^\alpha\right)^{1/\alpha}$$

Some more information-theoretic quantities

$\alpha \geq 1$

relative α-entropy

$$D_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1}\log \mathrm{tr}(\rho^\alpha \sigma^{1-\alpha})$$

α-Holevo quantity (for ensembles)

$$\chi_\alpha(\rho_{XQ}) = \min_{\sigma_Q} D_\alpha(\rho_{XQ}\|\rho_X \otimes \sigma_Q)$$
$$= \frac{\alpha}{\alpha-1}\log \mathrm{tr}\left(\sum_x P_X(x)\rho_x^\alpha\right)^{1/\alpha}$$

↔upper bound on

$$\max_{\mathcal{D}} \Pr_x[\mathcal{D}(\rho_x^Q) = x]$$

α-Holevo quantity (for channels)

$$\chi_\alpha^*(\Phi) = \max_{\rho_{XQ}} \chi_\alpha\left((\mathrm{id}\otimes\Phi)(\rho_{XQ})\right)$$

↔ upper bound on single-shot

$$\max_{\mathcal{E},\mathcal{D}} \Pr_x[\mathcal{D}\circ\Phi\circ\mathcal{E}(x) = x]$$

regularized α-Holevo quantity

$$\bar{\chi}_\alpha^*(\Phi) = \lim_{n\to\infty} \frac{1}{n}\chi_\alpha^*(\Phi^{\otimes n})$$

↔ asymptotic upper bound on

$$\max_{\mathcal{E},\mathcal{D}} \Pr_x[\mathcal{D}\circ\Phi^{\otimes n}\circ\mathcal{E}(x) = x]$$

Yet another useful relation (again)

α-Holevo quantity (for channels)

$$\chi^*_\alpha(\Phi) = \max_{\rho_{XQ}} \min_{\sigma_Q} D_\alpha(\rho_{X\Phi(Q)} \| \rho_X \otimes \sigma_Q)$$

$$= \frac{1}{\alpha-1} \min_{\sigma_Q} \max_{\rho_{XQ}} \log \mathrm{tr}\left(\sum_x P_X(x) \Phi(\rho_x)^\alpha \sigma_Q^{1-\alpha}\right)$$

$$= \min_{\sigma_Q} \max_{\rho_Q} \frac{1}{\alpha-1} \log \mathrm{tr}(\Phi(\rho_Q)^\alpha \sigma_Q^{1-\alpha})$$

.....optimization over **input** and **output**-state instead of **ensembles/cq-states**

(for standard Holevo quantity: Schumacher & Westmoreland '01)

$$= \min_\sigma \max_\rho D_\alpha(\Phi(\rho) \| \sigma)$$

Some more information-theoretic quantities

$\alpha \geq 1$

relative α-entropy

$$D_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1}\log \mathrm{tr}(\rho^\alpha \sigma^{1-\alpha})$$

α-Holevo quantity (for ensembles)

$$\chi_\alpha(\rho_{XQ}) = \min_{\sigma_Q} D_\alpha(\rho_{XQ}\|\rho_X \otimes \sigma_Q)$$

$$= \frac{\alpha}{\alpha-1}\log \mathrm{tr}\left(\sum_x P_X(x)\rho_x^\alpha\right)^{1/\alpha}$$

↔upper bound on

$$\max_{\mathcal{D}} \ \Pr_x[\mathcal{D}(\rho_x^Q) = x]$$

α-Holevo quantity (for channels)

$$\chi^*_\alpha(\Phi) = \max_{\rho_{XQ}} \chi_\alpha\left((\mathrm{id}\otimes\Phi)(\rho_{XQ})\right)$$

$$= \min_\sigma \max_\rho D_\alpha(\Phi(\rho)\|\sigma)$$

↔ upper bound on single-shot

$$\max_{\mathcal{E},\mathcal{D}} \ \Pr_x[\mathcal{D}\circ\Phi\circ\mathcal{E}(x) = x]$$

regularized α-Holevo quantity

$$\bar{\chi}^*_\alpha(\Phi) = \lim_{n\to\infty} \frac{1}{n}\chi^*_\alpha(\Phi^{\otimes n})$$

↔ asymptotic upper bound on

$$\max_{\mathcal{E},\mathcal{D}} \ \Pr_x[\mathcal{D}\circ\Phi^{\otimes n}\circ\mathcal{E}(x) = x]$$

α-Holevo quantity and success probability

(Ogawa & Nagaoka '99)

uniform ensemble $\{P_X(x) = \frac{1}{2^m}, \rho_x\}_{x\in\{0,1\}^m}$

$$\Pr_x[\mathcal{D}(\rho_x^Q) = x] = 2^{-m}\sum_x \mathrm{tr}(D_x\rho_x) \le \Theta$$

$$\le 2^{-m}\sum_x \mathrm{tr}\,(D_x\Theta)$$

$$\le 2^{-m}\mathrm{tr}\Theta$$

$\sum_x D_x = \mathrm{id}^{\otimes n}$

$$\le 2^{\frac{\alpha-1}{\alpha}(\chi_\alpha(\rho_{XQ})-m)}$$

$$\rho_x^\alpha \le \sum_y \rho_y^\alpha$$

⇓ operator monotony of $z \mapsto z^{1/\alpha} \quad (\alpha \ge 1)$

$$\rho_x \le \left(\sum_y \rho_y^\alpha\right)^{1/\alpha} =: \Theta$$

Key step:

common (but *ensemble-dependent*) bound on states in ensemble leads to bound for all POVMs

Some more information-theoretic quantities

$\alpha \geq 1$

relative α-entropy

$$D_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1}\log \mathrm{tr}(\rho^\alpha \sigma^{1-\alpha})$$

α-Holevo quantity (for ensembles)

$$\chi_\alpha(\rho_{XQ}) = \min_{\sigma_Q} D_\alpha(\rho_{XQ}\|\rho_X \otimes \sigma_Q)$$

$$= \frac{\alpha}{\alpha-1}\log \mathrm{tr}\left(\sum_x P_X(x)\rho_x^\alpha\right)^{1/\alpha}$$

↔upper bound on

$$\max_{\mathcal{D}} \Pr_x[\mathcal{D}(\rho_x^Q) = x]$$

α-Holevo quantity (for channels)

$$\chi^*_\alpha(\Phi) = \max_{\rho_{XQ}} \chi_\alpha\left((\mathrm{id}\otimes\Phi)(\rho_{XQ})\right)$$

$$= \min_\sigma \max_\rho D_\alpha(\Phi(\rho)\|\sigma)$$

↔ upper bound on single-shot

$$\max_{\mathcal{E},\mathcal{D}} \Pr_x[\mathcal{D}\circ\Phi\circ\mathcal{E}(x) = x]$$

regularized α-Holevo quantity

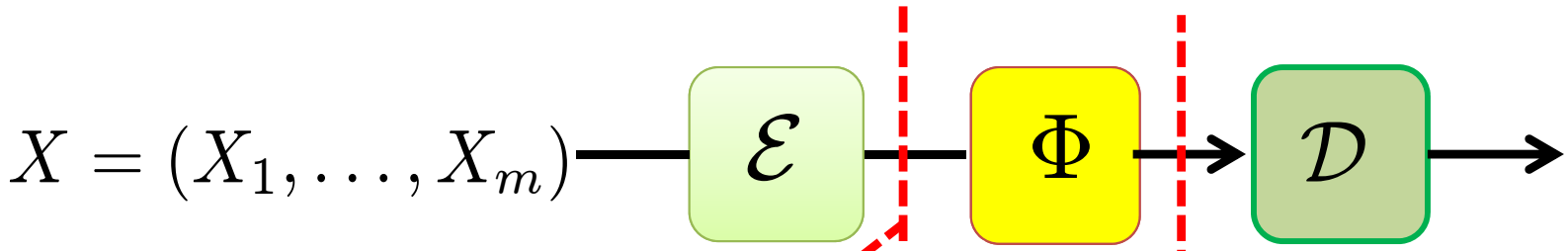
$$\bar{\chi}^*_\alpha(\Phi) = \lim_{n\to\infty} \frac{1}{n}\chi^*_\alpha(\Phi^{\otimes n})$$

↔ asymptotic upper bound on

$$\max_{\mathcal{E},\mathcal{D}} \Pr_x[\mathcal{D}\circ\Phi^{\otimes n}\circ\mathcal{E}(x) = x]$$

α-Holevo quantity for a channel (single-use)

$$\max_{\mathcal{E},\mathcal{D}} \Pr[(\mathcal{D}\Phi\mathcal{E})(x) = x] \leq 2^{\frac{\alpha-1}{\alpha}(\chi^*_\alpha(\Phi) - m)}$$



apply ensemble-bound
to output ensemble:

$$\Pr_x[\mathcal{D}(\rho_x^{Q_{out}}) = x] \leq 2^{\frac{\alpha-1}{\alpha}(\chi_\alpha(\rho_{XQ_{out}}) - m)}$$

$$\max_{\mathcal{E}} \chi_\alpha(\rho_{X(\Phi\circ\mathcal{E})(X)}) = \max_{\rho_{XQ_{in}}} \chi_\alpha\left((\mathrm{id}\otimes\Phi)(\rho_{XQ_{in}})\right)$$

$$= \chi^*_\alpha(\Phi)$$

maximization over encoders is equivalent to
maximization over inputstates

Some more information-theoretic quantities

$\alpha \geq 1$

relative α-entropy

$$D_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1}\log \mathrm{tr}(\rho^\alpha \sigma^{1-\alpha})$$

α-Holevo quantity (for ensembles)

$$\chi_\alpha(\rho_{XQ}) = \min_{\sigma_Q} D_\alpha(\rho_{XQ}\|\rho_X \otimes \sigma_Q)$$

$$= \frac{\alpha}{\alpha-1}\log \mathrm{tr}\left(\sum_x P_X(x)\rho_x^\alpha\right)^{1/\alpha}$$

↔upper bound on

$$\max_{\mathcal{D}} \Pr_x[\mathcal{D}(\rho_x^Q) = x]$$

α-Holevo quantity (for channels)

$$\chi^*_\alpha(\Phi) = \max_{\rho_{XQ}} \chi_\alpha\left((\mathrm{id}\otimes\Phi)(\rho_{XQ})\right)$$

$$= \min_\sigma \max_\rho D_\alpha(\Phi(\rho)\|\sigma)$$

↔ upper bound on single-shot

$$\max_{\mathcal{E},\mathcal{D}} \Pr_x[\mathcal{D}\circ\Phi\circ\mathcal{E}(x) = x]$$

regularized α-Holevo quantity

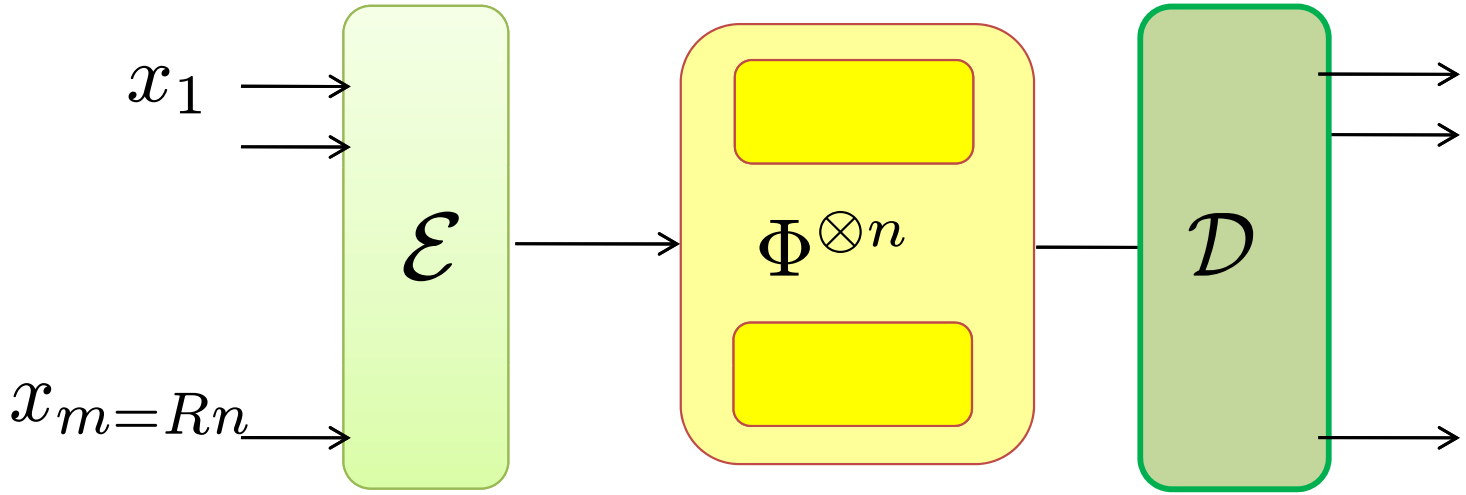
$$\bar{\chi}^*_\alpha(\Phi) = \lim_{n\to\infty} \frac{1}{n}\chi^*_\alpha(\Phi^{\otimes n})$$

↔ asymptotic upper bound on

$$\max_{\mathcal{E},\mathcal{D}} \Pr_x[\mathcal{D}\circ\Phi^{\otimes n}\circ\mathcal{E}(x) = x]$$

(regularized) α-Holevo quantity and strong converse

$$\max_{\mathcal{E},\mathcal{D}} \Pr_x[\mathcal{D}\Phi^{\otimes n}\mathcal{E}(x) = x] \leq \left(2^{(\chi_\alpha^*(\Phi^{\otimes n}) - Rn)}\right)^{\frac{\alpha-1}{\alpha}}$$



α-Holevo quantity of covariant channels

$$\chi^*_\alpha(\Phi) = \min_\sigma \max_\rho D_\alpha(\Phi(\rho)\|\sigma)$$

$$= \frac{1}{\alpha-1}\log \min_\sigma \max_\rho \mathrm{tr}\left(\Phi(\rho)^\alpha \sigma^{1-\alpha}\right)$$

$$= \max_\rho \mathrm{tr}\left(\Phi(g\rho g^\dagger)^\alpha \sigma^{1-\alpha}\right) \qquad \forall g \in G$$

using covariance & irreducibility, joint **min**-**max**-optimization can be factorized, and only **max** remains

$$= \max_\rho \mathrm{tr}\left(\Phi(\rho)^\alpha g\sigma^{1-\alpha}g^\dagger\right)$$

$$= \max_\rho \mathrm{tr}\left(\Phi(\rho)^\alpha \frac{1}{|G|}\sum_g g\sigma^{1-\alpha}g^\dagger\right)$$

$$\left(\mathrm{tr}\sigma^{1-\alpha}\right)\cdot\frac{1}{d_{out}}\mathrm{id}$$

$$= \frac{1}{d_{out}}\mathrm{tr}\sigma^{1-\alpha}\cdot\max_\rho \mathrm{tr}\Phi(\rho)^\alpha$$

$$= \log d_{out} - S^{\min}_\alpha(\Phi)$$

Conditions for additivity of α-Holevo quantity

If $\Phi : \mathcal{B}(\mathcal{H}_{in}) \to \mathcal{B}(\mathcal{H}_{out})$ has

additive minimum output Rényi entropy & covariance property

$$S_\alpha^{\min}(\Phi^{\otimes n}) = n \cdot S_\alpha^{\min}(\Phi)$$

$$\alpha \geq 1$$

$$g\Phi(\rho)g^\dagger = \Phi(g\rho g^\dagger)\ \forall g$$

wrt. representations of a group G, irreducible on $\mathcal{H}_{out}$

Then: $$\chi_\alpha^*(\Phi^{\otimes n}) = n \cdot \chi_\alpha^*(\Phi)$$

Proof:

using min-max characterization:

$$n \log d_{out} - S_\alpha^{\min}(\Phi^{\otimes n}) =$$

$$\max_\rho D_\alpha(\Phi^{\otimes n}(\rho) \| \tfrac{\mathrm{id}}{d_{out}^n})$$

$$\geq \chi_\alpha^*(\Phi^{\otimes n})$$

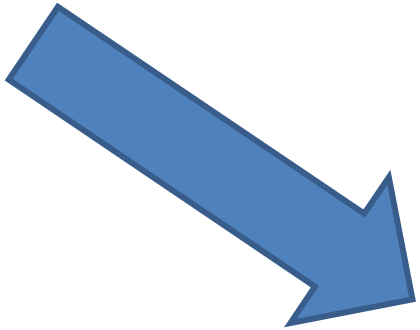
previous calculation using covariance:

$$n \cdot \chi_\alpha^*(\Phi)$$

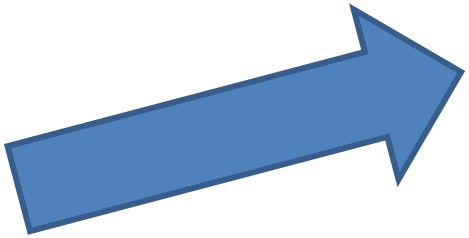
$$= n \log d_{out} - n S_\alpha^{\min}(\Phi)$$

Summary of strong converse proof

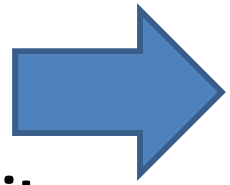
upper bound on decoding probability in terms of α-Holevo quantity



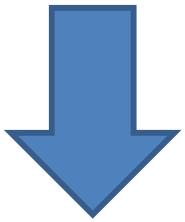
min-max-expression for α-Holevo quantity and α-relative entropy



reformulation as **additivity problem for α-Holevo quantity** (for channels with equal product- and normal capacity)



equivalent to **additivity of minimum output α-entropy** for covariant channels



strong converse for covariant channels with additive minimum output entropy

lower bound on single-shot α-Holevo quantity in terms of product state capacity

Summary

impossibility of coding of classical information at rates $R > C$
even using *arbitrary* (entangled) *codewords:*

- can be used for (efficient) cryptography, if an upper bound of the form

$$\max_{\mathcal{E},\mathcal{D}} \Pr_{x\in\{0,1\}^m} \left[(\mathcal{D}\circ\Phi^{\otimes n}\circ\mathcal{E})(x) = x\right] \leq 2^{-n\gamma(R-C)}$$

determines min-entropy or key-rate

for the adversary's channel Φ is known.

- established for depolarizing, unital qubit-, and Werner-Holevo channels (key properties: *covariance* and additive minimum output Renyi-entropy)

OPEN PROBLEM: More (ALL?) quantum channels!