Encoding classical information in quantum resources

Kamil Korzekwa

Faculty of Physics, Astronomy and Applied Computer Science, Jagiellonian University, Poland

JAGIELLONIAN UNIVERSITY IN KRAKÓW

FNP Foundation for Polish Science

TEAM-NET

Collaborators

Zbigniew Puchała
IITiS, Gliwice

Marco Tomamichel
UTS, Sydney

Karol Życzkowski
UJ, Kraków

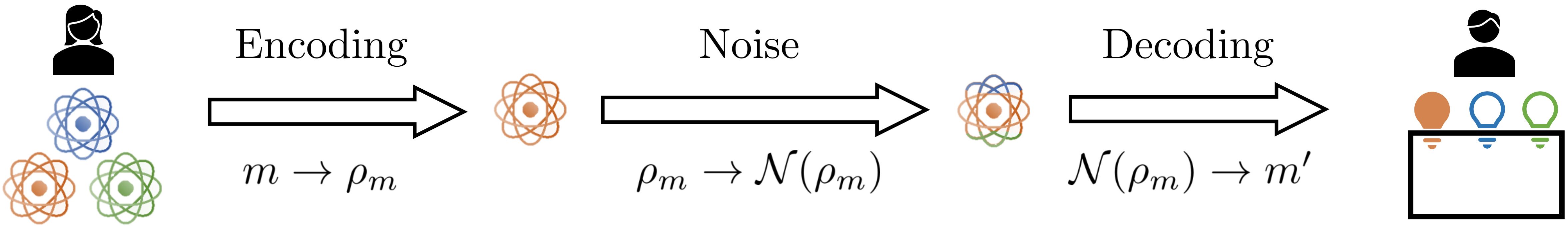
Outline

1. Motivation: communication scenarios
2. Results: optimal encodings into resources
3. Applications:
   - Encoding information in purity
   - Encoding information in coherence
   - Encoding information in entanglement
   - Private communication with shared reference frame
   - Thermodynamicall-free encodings and the Szilard engine
4. Sketch of the proofs
5. Outlook

arXiv:1911.12373

Motivation: communication scenarios

Traditional communication scenario



Set of messages: $\{m\}_{m=1}^{M}$

Encoded messages: $\{\rho_m\}_{m=1}^{M}$

Decoding POVM: $\{E_m\}_{m=1}^{M}$

Decoding prob.: $\mathrm{Tr}\left(\mathcal{N}(\rho_m)E_m\right)$

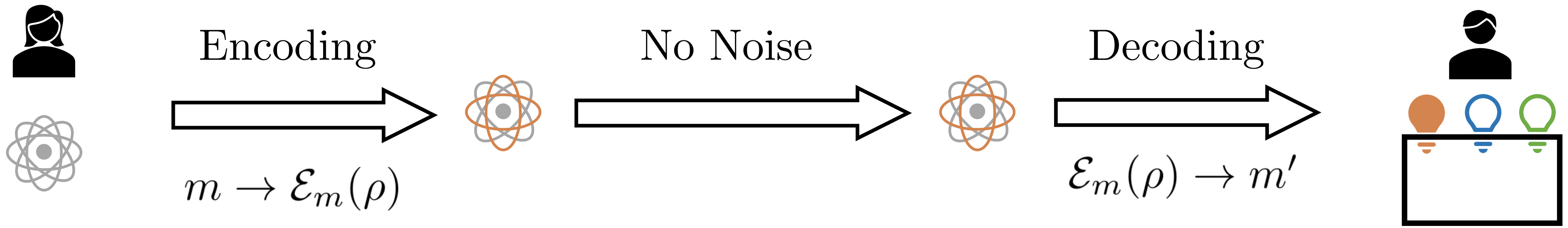
Sender is all powerful
(all encodings allowed)

No control over the channel
(noise is given)

Receiver is all powerful
(all decodings allowed)

Motivation: communication scenarios

Our constrained communication scenario



Set of messages: $\{m\}_{m=1}^{M}$

Information carrier: ρ

Allowed encodings: $\mathcal{E}_m(\rho)$

Decoding POVM: $\{E_m\}_{m=1}^{M}$

Decoding prob.: $\mathrm{Tr}\left(\mathcal{E}_m(\rho)E_m\right)$

Sender is constrained
(only restricted set $\{\mathcal{E}_m\}$)

Perfect control over the channel
(no noise)

Receiver is all powerful
(all decodings allowed)

Motivation: communication scenarios

What constraints do we study?

Mathematically:

Only encoding channels satisfying:

$$\mathcal{E}_m \circ \mathcal{D} = \mathcal{D}$$

$$\mathcal{D} \circ \mathcal{E}_m = \mathcal{D}$$

for a fixed idempotent channel $\mathcal{D}$.

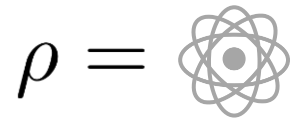
Example:

$$\mathcal{G}(\rho) := \frac{1}{|G|} \sum_{g \in G} U^{(g)} \rho U^{(g)\dagger}$$

Physically:

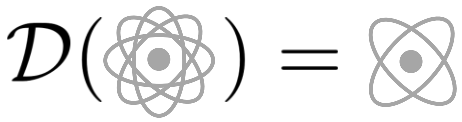
System

All degrees of freedom (DOGs)



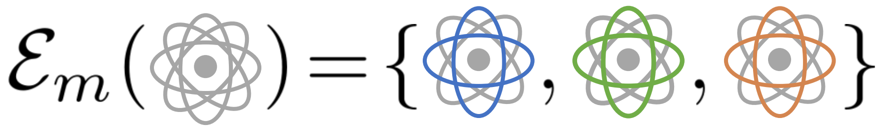
Resource-destroying map

Erasing information from some DOGs



Encodings

Encoding only in erased DOGs



Example: $\Delta(\rho) := \sum_i \langle i| \rho |i\rangle \, |i\rangle\langle i|$

Results: optimal encodings

Crucial quantities

Average probability of decoding error: $$\epsilon := 1 - \frac{1}{M}\sum_{m=1}^{M} \mathrm{Tr}\left(\mathcal{E}_m(\rho) E_m\right)$$

Optimal number of messages that can be encoded in ρ, using encodings constrained by $\mathcal{D}$, so that the average decoding error is smaller than ϵ: $$M_{\mathcal{D}}(\rho, \epsilon)$$

Optimal encoding rate into multiple copies of ρ: $$R_{\mathcal{D}}(\rho, N, \epsilon) := \frac{\log\left[M_{\mathcal{D}}(\rho^{\otimes N}, \epsilon)\right]}{N}$$

Results: optimal encoding rates

Result 1: General single-shot upper-bound

$$\boxed{M_{\mathcal{D}}(\rho,\epsilon) \leq e^{D_H^{\epsilon}(\rho\|\mathcal{D}(\rho))}}$$

D_H^{ϵ} is the hypothesis testing relative entropy:

$$D_H^{\epsilon}(\rho\|\sigma) := -\log\inf\left\{\mathrm{Tr}\left(Q\sigma\right) \;\middle|\; 0 \leq Q \leq \mathbb{1}, \mathrm{Tr}\left(Q\rho\right) \geq 1-\epsilon\right\}$$

Result 2: Single-shot lower- & upper-bounds for G-twirling maps

$$\boxed{\forall_{\delta\in(0,\min(\epsilon,1-\epsilon))} : \quad \delta e^{D_s^{\epsilon-\delta}(\rho\|\mathcal{G}(\rho))} \leq M_{\mathcal{G}}(\rho,\epsilon) \leq \frac{1}{\delta} e^{D_s^{\epsilon+\delta}(\rho\|\mathcal{G}(\rho))}}$$

D_s^{δ} is the information spectrum relative entropy:

$D_s^{\delta}(\rho\|\sigma) := \sup\left\{K \mid \mathrm{Tr}\left(\rho\Pi^{+}_{2^K\sigma-\rho}\right) \leq \delta\right\}$, with Π^{+}_{A} a projection on the positive eigenspace of A

Results: optimal encoding rates

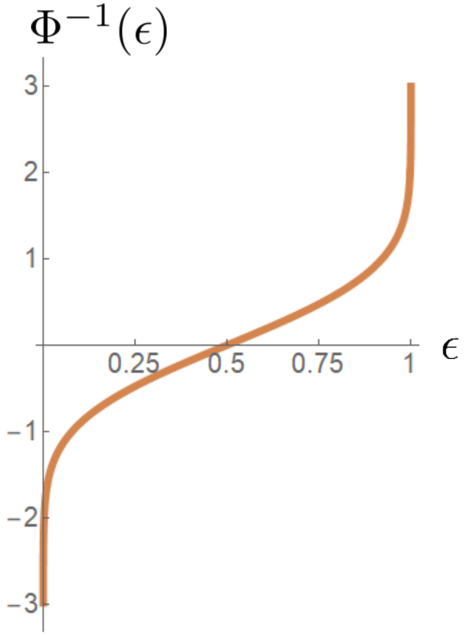
Result 3: Optimal asympotic encoding rate for G-twirling maps

$$\boxed{R_{\mathcal{G}}(\rho, N, \epsilon) = D(\rho\|\mathcal{G}(\rho)) + \frac{\Phi^{-1}(\epsilon)}{\sqrt{N}}\sqrt{V(\rho\|\mathcal{G}(\rho))} + O\left(\frac{\log N}{N}\right)}$$

D is rel. ent.: $D(\rho\|\sigma) := \mathrm{Tr}\left(\rho(\log\rho - \log\sigma)\right)$

V is the rel. ent. var.: $V(\rho\|\sigma) := \mathrm{Tr}\left(\rho(\log\rho - \log\sigma)^2\right) - D^2(\rho\|\sigma)$

Φ^{-1} is the inverse of the cdf of normal distribution



Applications: encodings into purity

Choice of the group G: All unitaries

Corresponding G-twirling map: (Purity-destroying map) $\mathcal{G}(\rho) = \frac{\mathbb{1}}{d}$

Resulting allowed encodings: Unital maps: $\mathcal{E}(\mathbb{1}) = \mathbb{1}$

Optimal encoding rate:

$$\left(R = R_1 + \sqrt{R_2}\frac{\Phi^{-1}(\epsilon)}{\sqrt{N}} + O\left(\frac{\log N}{N}\right)\right)$$

$$\boxed{R_1 = \log d - S(\rho), \quad R_2 = V(\rho)}$$

S, V: von Neumann entropy and variance

Communication scenario:
Sender cannot decrease the mixedness of the system (cannot dump entropy).

Applications: encodings into coherence

Choice of the group G: Unitaries diagonal in a fixed basis $\{|i\rangle\}$

Corresponding G-twirling map:
(coherence-destroying map)

$$\mathcal{G}(\rho) = \Delta(\rho) = \sum_i \langle i|\,\rho\,|i\rangle\,|i\rangle\!\langle i|$$

Resulting allowed encodings: Population-preserving maps: $\langle i|\mathcal{E}(|j\rangle\!\langle j|)|i\rangle = \delta_{ij}$

Optimal encoding rate:

$$\left(R = R_1 + \sqrt{R_2}\frac{\Phi^{-1}(\epsilon)}{\sqrt{N}} + O\left(\frac{\log N}{N}\right)\right)$$

$$\boxed{R_1 = D(\rho\|\Delta(\rho)), \quad R_2 = V(\rho\|\Delta(\rho))}$$

Communication scenario:
Sender can only control the phase degrees of freedom of the system (off-diagonal elements of ρ).

Applications: encodings into entanglement

Choice of the group G: All unitaries on A of a bipartite system AB

Corresponding G-twirling map:
(entanglement-destroying map)

$$\mathcal{G}(\rho_{AB}) = \frac{\mathbb{1}_A}{d_A} \otimes \mathrm{Tr}_A(\rho_{AB})$$

Resulting allowed encodings: Local unital channels on A

Optimal encoding rate:

$$\left(R = R_1 + \sqrt{R_2}\frac{\Phi^{-1}(\epsilon)}{\sqrt{N}} + O\left(\frac{\log N}{N}\right)\right)$$

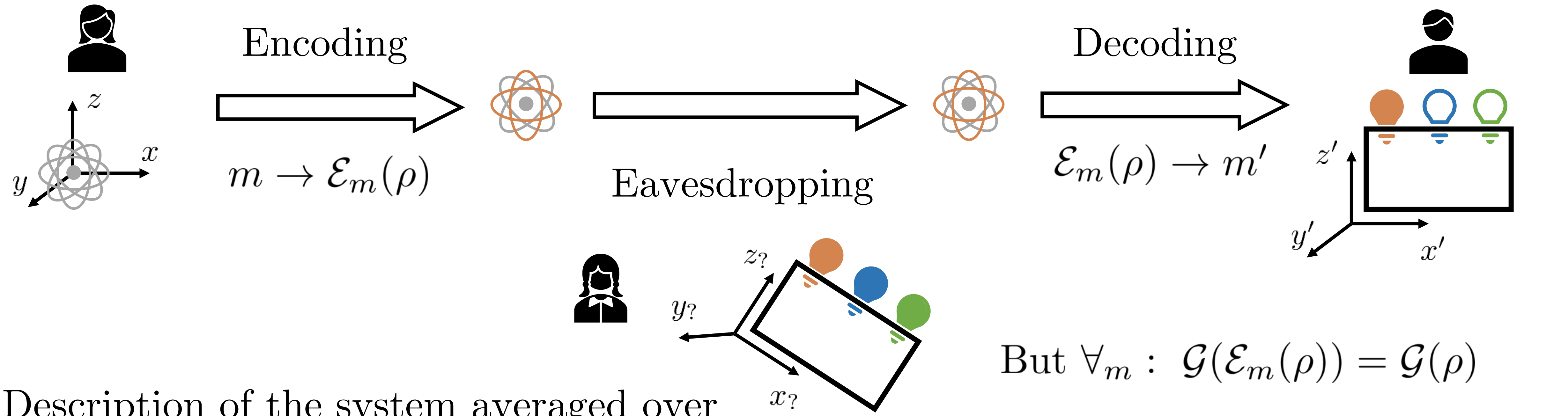
$$\boxed{R_1 = \log d_A - S(A|B), \quad R_2 = V(A|B)}$$

$S(A|B), V(A|B)$: conditional entropy and variance

Communication scenario:
Super-dense coding scenario: sender can only locally modify subsystem A, then sends it to B, who tries to recover the message sent.

Applications: private communication

Private classical communication scheme with a shared reference frame (RF)



But $\forall_m : \; \mathcal{G}(\mathcal{E}_m(\rho)) = \mathcal{G}(\rho)$

Description of the system averaged over all possible relative orientations of the RF:

$$\mathcal{G}(\rho) := \frac{1}{|G|} \sum_{g \in G} U^{(g)} \rho U^{(g)\dagger}$$

So: **private communication**, as the eavesdropper cannot intercept any of $M_{\mathcal{G}}(\rho, \epsilon)$ messages.

Applications: thermodynamics

Choose thermalising resource-destroying map: $\mathcal{D}(\rho) = \gamma$

γ - thermal equilibrium state

Resulting allowed encodings: equilibrium-preserving operations $\mathcal{E}(\gamma) = \gamma$

Optimal encoding rate: $R_{\mathcal{D}}(\rho, N, \epsilon) \leq D(\rho\|\gamma) + \frac{\Phi^{-1}(\epsilon)}{\sqrt{N}} \sqrt{V(\rho\|\gamma)}$

Generalised free energy:
$k_B T D(\rho\|\gamma) = \langle E \rangle_\rho - TS(\rho)$

Generalised heat capacity
(arXiv:1711.01193)

Irreversibility of the Szilard engine?

Sketch of the proofs

Optimality (for arbitrary resource destroying map $\mathcal{D}$)

Message correlated with the encoding: $\tau_{MQ} := \frac{1}{M}\sum_{m=1}^{M} |m\rangle\langle m| \otimes \mathcal{E}_m(\rho)$

Message and erased encoding: $\zeta := \frac{1}{M}\sum_{m=1}^{M} |m\rangle\langle m| \otimes \mathcal{D}(\rho)$

Bound hypothesis testing rel. ent.: $D_H^{\epsilon}(\tau_{MQ}\|\zeta) \geq -\log \operatorname{Tr}(Q\zeta) = \log M$

(as a result, bound M)

$\boxed{Q = \sum_{m=1}^{M} |m\rangle\langle m| \otimes E_m}$

Use data-processing inequality twice:

$$\log M \leq D_H^{\epsilon}(\tau_{MQ}\|\zeta) = D_H^{\epsilon}\left(\tilde{\mathcal{E}}\left(\frac{1}{M}\sum_{m=1}^{M} |m\rangle\langle m| \otimes \rho\right)\middle\|\tilde{\mathcal{E}}(\zeta)\right)$$

$\boxed{\tilde{\mathcal{E}} = \sum_{m=1}^{M} |m\rangle\langle m| \otimes \mathcal{E}_m}$

$$\leq D_H^{\epsilon}\left(\frac{1}{M}\sum_{m=1}^{M} |m\rangle\langle m| \otimes \rho\middle\|\zeta\right) \leq D_H^{\epsilon}\left(\rho\middle\|\mathcal{D}(\rho)\right)$$

Sketch of the proofs

Achievability (only for G-twirling maps $\mathcal{G}$)

Define a codebook: $\mathcal{C}: \{1,\ldots,M\} \to \{1,\ldots,|G|\}$

Encoding according to $\mathcal{C}$: $\mathcal{E}_m(\rho) = U^{(g=\mathcal{C}(m))}\rho U^{(g=\mathcal{C}(m))\dagger} =: \sigma_m^{\mathcal{C}}$

$$\boxed{\forall g: \quad \mathcal{G}(U^{(g)}(\cdot)U^{(g)\dagger}) = U^{(g)}\mathcal{G}(\cdot)U^{(g)\dagger} = \mathcal{G}(\cdot)}$$

Decoding with pretty good measurement: $E_m := S\sigma_m^{\mathcal{C}}S, \qquad S = \left(\sum_{m=1}^{M}\sigma_m^{\mathcal{C}}\right)^{-1/2}$

Average decoding error: $\epsilon(\mathcal{C}) = 1 - \frac{1}{M}\exp D_2(\tau_{MCQ}^{\mathcal{C}}\|\tau_{MC}^{\mathcal{C}}\otimes\tau_Q^{\mathcal{C}})$

Message-classical encoding-quantum encoding state: $\tau_{MCQ}^{\mathcal{C}} = \frac{1}{M}\sum_{m=1}^{M}|m\rangle\langle m|\otimes|\mathcal{C}(m)\rangle\langle\mathcal{C}(m)|\otimes\sigma_m^{\mathcal{C}}$

Sketch of the proofs

Achievability (only for G-twirling maps $\mathcal{G}$)

Decoding error averaged over all codebooks: $\epsilon_{\text{avg}} := \mathbb{E}_{\mathcal{C}}[\epsilon(\mathcal{C})]$ $\boxed{\exists \mathcal{C} : \ \epsilon(\mathcal{C}) \leq \epsilon_{\text{avg}}}$

Bound averaged error using joint convexity:

$$\epsilon_{\text{avg}} = 1 - \frac{1}{M}\mathbb{E}_{\mathcal{C}}\left[\exp D_2(\tau^{\mathcal{C}}_{MCQ} \| \tau^{\mathcal{C}}_{MC} \otimes \tau^{\mathcal{C}}_{Q})\right]$$

$$\leq 1 - \frac{1}{M}\exp D_2(\mathbb{E}_{\mathcal{C}}[\tau^{\mathcal{C}}_{CQ}] \| \mathbb{E}_{\mathcal{C}}[\tau^{\mathcal{C}}_{C} \otimes \tau^{\mathcal{C}}_{Q}])$$

Calculate averaged states: $\epsilon_{\text{avg}} \leq 1 - \frac{1}{M}\exp D_2(\rho \| \frac{1}{M}\rho + \frac{M-1}{M}\mathcal{G}(\rho))$

Bound D_2 with D_s^δ : $\epsilon_{\text{avg}} \leq 1 - (1-\delta)(1 - M\exp\left[-D_s^\delta(\rho\|\mathcal{G}(\rho))\right])$

Which yields: $M \geq \frac{\epsilon_{\text{avg}} - \delta}{1-\delta}\exp D_s^\delta(\rho\|\mathcal{G}(\rho))$ $\boxed{\forall \delta \in (0,1)}$

Sketch of the proofs

Asymptotics

Single-shot bounds: $\delta e^{D_s^{\epsilon-\delta}(\rho\|\mathcal{G}(\rho))} \leq M_{\mathcal{G}}(\rho,\epsilon) \leq \frac{1}{\delta} e^{D_s^{\epsilon+\delta}(\rho\|\mathcal{G}(\rho))}$

Known asymptotic expansion of D_s^δ: $D_s^{\epsilon\pm\delta}\left(\rho^{\otimes N}\|\sigma^{\otimes N}\right) = ND(\rho\|\sigma) + \sqrt{NV(\rho\|\sigma)}\Phi^{-1}(\epsilon) + O(\log N)$

$\boxed{\forall\delta = O(1/\sqrt{N})}$

Simply choose: $\delta = 1/\sqrt{N}$

Take log and notice that both bounds coincide, yielding:

$$R_{\mathcal{G}}(\rho, N, \epsilon) = D(\rho\|\mathcal{G}(\rho)) + \frac{\Phi^{-1}(\epsilon)}{\sqrt{N}}\sqrt{V(\rho\|\mathcal{G}(\rho))} + O\left(\frac{\log N}{N}\right)$$

Outlook

- Look for other unitary subgroups with operational relevance (and thus find second-order asympotic rates for constrained communication scenarios).
- Find single-shot lower-bounds for general resource-destroying maps (optimally: ones that coincide with upper-bounds up to second-order asympotics).
- In particular, study thermodynamically-free encodings.
- For a general group G find optimal states for encoding information using unitary group representations.

Thank you!

arXiv:1911.12373