Finite Block Length Analysis on Quantum Coherence Distillation and Incoherent Randomness Extraction [2002.12004]

Masahito Hayashi[1,2,3,4] and Kun Fang[5,6]

[1]Shenzhen Institute for Quantum Science and Engineering
Southern University of Science and Technology
[2] Guangdong Provincial Key Laboratory of Quantum Science and Engineering
[3] Shenzhen Key Laboratory of Quantum Science and Engineering
[4]Graduate School of Mathematics, Nagoya University
[5]Institute for Quantum Computing, University of Waterloo
[6]Department of Applied Mathematics and Theoretical Physics, University of Cambridge

QCrypt 2020, Amsterdam

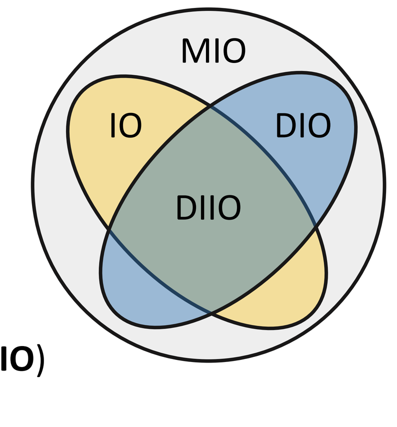
[1]. Coherence theory

Free states: incoherent (diagonal) states $\mathcal{I} := \{\rho \geq 0 : \operatorname{Tr}\rho = 1, \rho = \Delta(\rho)\}$ (diagonal map)

Resource states: coherent (non-diagonal) states

Maximally coherent state: $|\Psi_m\rangle = \frac{1}{\sqrt{m}}\sum_{i=1}^{m}|i\rangle$ Coherent bit (cobit): $|\Psi_2\rangle$

Free operations:



Maximally incoherent operations (**MIO**)
$\rho \in \mathcal{I} \Longrightarrow \mathcal{E}(\rho) \in \mathcal{I}$
$[\Delta \circ \mathcal{E} \circ \Delta = \mathcal{E} \circ \Delta]$

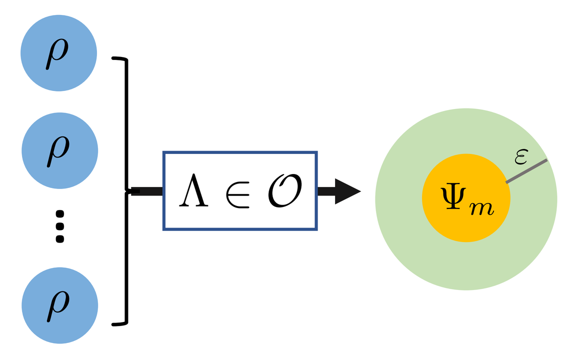
Dephasing-covariant incoherent operations (**DIO**) $\mathcal{E} \circ \Delta = \Delta \circ \mathcal{E}$

Incoherent operations (**IO**)
$\mathcal{E}(\cdot) = \sum_i E_i \cdot E_i^\dagger,$
$E_i \cdot E_i^\dagger \in \text{MIO}\ \forall i$

DIIO = DIO ∩ IO

[Streltsov-Adesso-Plenio-2017] RMP **1609.02439**

[2]. Coherence distillation



One-shot distillable coherence

$$C_{d,\mathcal{O}}^{(1),\varepsilon}(\rho) := \max_{\Lambda \in \mathcal{O}} \log_2 m$$

$$\text{s.t. } F(\Lambda(\rho), \Psi_m) \geq 1 - \varepsilon.$$

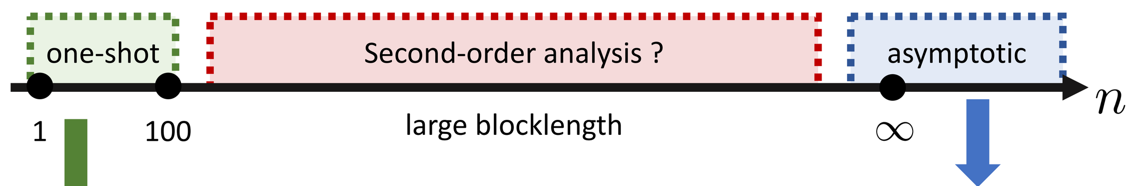
Asymptotic distillable coherence

$$C_{d,\mathcal{O}}^{\infty}(\rho) = \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}C_{d,\mathcal{O}}^{(1),\varepsilon}(\rho^{\otimes n})$$

Why do we do coherence distillation?

1. Quantum algorithm: [Hillery-2016-PRA]
2. Quantum state merging: [Streltsov et al-2016-RPL]
3. Quantum state redistribution: [Anshu-Jain-Streltsov-2018]
4. Quantum random number generation: [Ma et al.-2019-PRA]
5. …

[3]. Previous works



Operations	Distillable coherence	Coherence cost
MIO	C_r	C_r
DIO	C_r	C_r
IO	C_r	C_f
SIO	Q	C_f
PIO	Q	$C_f^{\mathcal{U}}$

[Winter-Yang-2016]
[Regula-Fang-Wang-Adesso-2018]
[Chitambar-2018]
[Lami-2019]

		MIO	DIO	IO	SIO
One-shot	distillation	$\widetilde{C}_H^\varepsilon$ [25]	$\widetilde{C}_H^\varepsilon$ [25]	$\mathbf{C}_{\min}^{\varepsilon'}$ [∗]	**Thm. 10** [∗]
	formation	$C_{\max}^\varepsilon$ [24]	$C_{\Delta,\max}^\varepsilon$ [24]	C_0^ε [24]	C_0^ε [24]

[Regula-Fang-Wang-Adesso-2018]
[Zhao-Liu-Yuan-Chitambar-Winter-2018]

[4]. Second-order analysis

For example:

$$C_{d,\text{MIO}}^{(1),\varepsilon}(\rho^{\otimes n}) \stackrel{?}{=} nD(\rho\|\Delta(\rho)) + \sqrt{nV(\rho\|\Delta(\rho))}\,\Phi^{-1}(\varepsilon) + O(\log n)$$

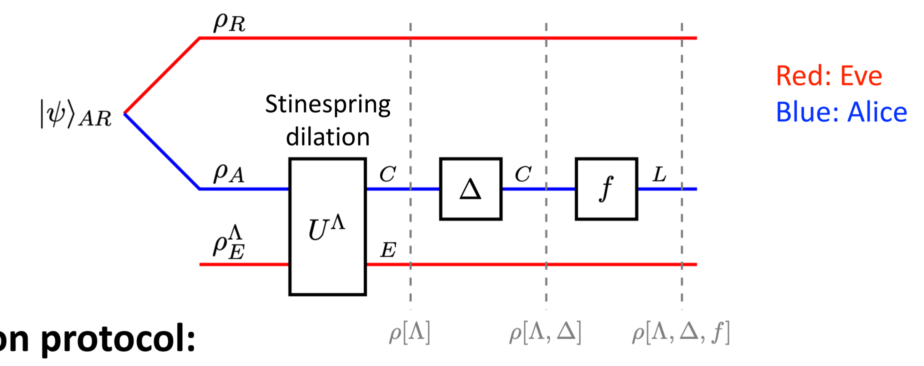
Why do we study the second-order asymptotics:

1. It gives a useful approximation to the averaged distillable coherence for given *finite copies* of resource states.
2. Its determines the *rate of convergence* of the averaged distillable coherence to its first order coefficient (in the same manner of Central Limit Theorem v.s. Berry-Esseen Theorem).
3. It implies the *strong converse property*, an information-theoretic property that rules out a possible tradeoff between the transformation error and the distillable coherence of a protocol.

Difficulty:

one-shot bounds with *matching* epsilon error dependence

[5]. Incoherent randomness extraction



Extraction protocol:

1. Alice holds quantum state ρ_A with a purifying system R held by Eve;
2. Alice performs an incoherent operation Λ on system A and the environment system E is held by Eve;
3. Alice applies a dephasing map Δ on her state and obtains the classical bits;
4. Alice applies a hash function f to extract randomness.

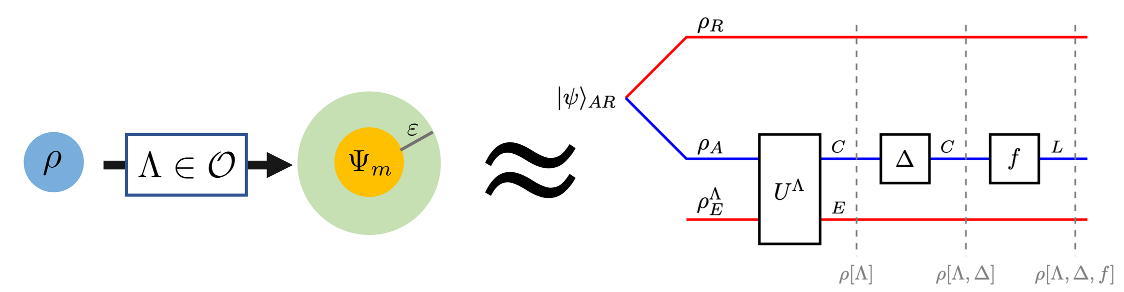
One-shot extractable randomness

$$\ell_\Lambda^\varepsilon(\rho_A) := \max_f \left\{ \log|L| : d_{sec}(\rho[\Lambda,\Delta,f]_{LER}|ER) \leq \varepsilon \right\}.$$

$$\ell_{\mathcal{O}}^\varepsilon(\rho_A) := \max_{\Lambda\in\mathcal{O}} \ell_\Lambda^\varepsilon(\rho_A). \qquad d_{sec}(\rho_{AR}|R) := \min_{\sigma_R\in\mathcal{S}(R)} P(\rho_{AR}, \pi_A\otimes\sigma_R).$$

[6]. Main result 1: one-shot equivalence

The maximum number of secure random bits extractable from a single instance of unstructured quantum state is *precisely equal to* the maximum number of coherent bits that can be distilled from the same state.



For any quantum state ρ_A and error tolerance $\varepsilon \in [0,1]$ and free operation class $\mathcal{O}$ ∈{MIO,DIO,IO,DIIO}, it holds

$$C_{d,\mathcal{O}}^\varepsilon(\rho_A) = \ell_{\mathcal{O}}^\varepsilon(\rho_A)$$

[7]. Proof ideas

Distillation protocol -> Randomness extraction protocol

For any free operation Λ such that $P(\Lambda(\rho_A), \Psi_C) \leq \varepsilon$

Then $(\Lambda, \Delta, \text{id})$ is an incoherent randomness extraction protocol such that

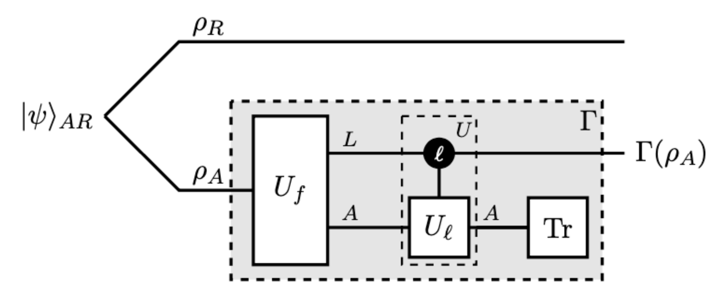
$$d_{sec}(\rho[\Lambda,\Delta,\text{id}]_{CER}|ER) \leq \varepsilon$$

Randomness extraction protocol -> Distillation protocol

For any incoherent randomness extraction protocol (id, Δ, f) such that

$$d_{sec}(\rho[\text{id},\Delta,f]_{LR}|R) \leq \varepsilon$$

Then there exists Λ in DIIO such that $P(\Gamma_{A\to L}(\rho_A), \Psi_L) \leq \varepsilon$



[8]. Main result 2: second-order expansions

For any quantum state ρ_A and error tolerance $\varepsilon \in (0,1)$ and free operation class $\mathcal{O}$ ∈{MIO,DIO,IO,DIIO}, it holds

$$C_{d,\mathcal{O}}^\varepsilon(\rho^{\otimes n}) = \ell_{\mathcal{O}}^\varepsilon(\rho^{\otimes n}) = nD(\rho\|\Delta(\rho)) + \sqrt{nV(\rho\|\Delta(\rho))}\,\Phi^{-1}(\varepsilon^2) + O(\log n).$$

Information variance — cumulative distribution function of a standard normal random variable

Remarks:

1. This is the *first* second-order analysis in coherence theory.
2. MIO/DIO/IO/DIIO have *equivalent power* for coherence distillation and randomness extraction in the large block length regime.
3. As coherence is generically undistillable under SIO/PIO [Lami et al.-2019, Lami-2019], our results have *completed* the second order analysis on distillable coherence under all major classes of free operations.
4. It gives an alternative proof of the strong converse property of coherence distillation [Zhao et al.-2019] and randomness extraction.

[9]. Proof ideas

[Regula-Fang-Wang-Adesso-2018]

Converse part: $C_{d,\mathcal{O}}^\varepsilon(\rho_A^{\otimes n}) \leq C_{d,\text{MIO}}^\varepsilon(\rho_A^{\otimes n}) \leq D_H^{\varepsilon^2}(\rho_A^{\otimes n}\|\Delta(\rho_A)^{\otimes n})$

[This work, one-shot equivalence]

Achievable part: $\ell_{\mathcal{O}}^\varepsilon(\rho_A^{\otimes n}) \geq \ell_{\text{id}}^\varepsilon(\rho_A^{\otimes n}) \geq H_{\min}^{\varepsilon-\eta}(A^n|R^n)_{\tilde{\rho}^{\otimes n}} + 4\log\eta - 3$

[Tomamichel-Hayashi-2013] $\tilde{\rho}_{AR} := \rho[\text{id},\Delta]$

[Tomamichel-Hayashi-2013; Li-2014]

$$D_H^\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) = nD(\rho\|\sigma) + \sqrt{nV(\rho\|\sigma)}\,\Phi^{-1}(\varepsilon) + O(\log n),$$

$$D_{\max}^\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) = nD(\rho\|\sigma) - \sqrt{nV(\rho\|\sigma)}\,\Phi^{-1}(\varepsilon^2) + O(\log n),$$

Remark: alternative approach by a one-shot characterization

$$C_{d,\mathcal{O}}^\varepsilon(\rho_A) \approx D_H^{\varepsilon^2}(\rho_A\|\Delta(\rho_A))$$

[10]. Open problems

1. (Coherence distillation)
Strong converse exponents (the exact rate of error measure converges to one when the achievable rate is over the optimal rate)
Error exponents (the exact rate of error measure decays to zero when the achievable rate is below the optimal rate) ?
2. (Coherence cost)
What are the second order asymptotics of **coherence cost**?
3. (Incoherent randomness extraction)
Is any **advantage** of performing incoherent operations in the **third or higher order terms**?