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

[2002.12004]

<u>Masahito Hayashi</u>[1,2,3,4], Kun Fang[5], and Kun Wang[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]Institute for Quantum Computing, Baidu Research

Beyond IID in Information Theory 8, 2020

Contents

PART 1: Coherence Distillation

[1.1] Coherence theory

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

diagonal map

Resource states: coherent (non-diagonal) states

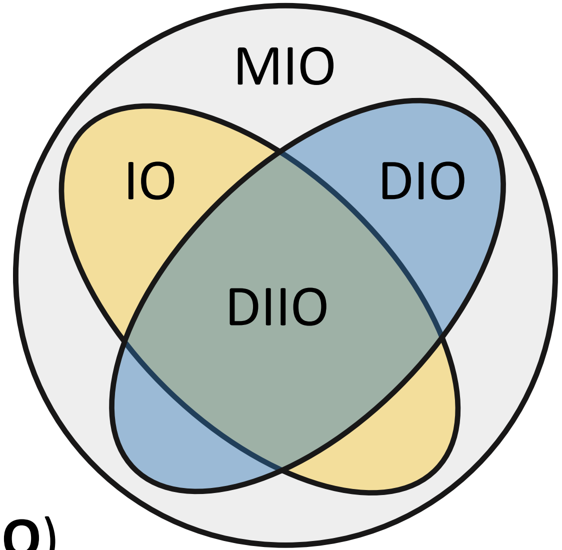
Maximally coherent state: $|\Psi_m\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle$

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**)

$\mathcal{E}(\cdot) = \sum_i E_i \cdot E_i^\dagger,$

$E_i \cdot E_i^\dagger \in \mathrm{MIO}\ \forall i$

DIIO = DIO ∩ IO

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

[1.2] Coherence distillation

$$\rho_B \longrightarrow \boxed{\Lambda \in \mathcal{O}} \longrightarrow \approx_\varepsilon \Psi_m$$

One-shot distillable coherence

$$C_{d,\mathcal{O}}^{(1),\varepsilon}(\rho) := \max_{\Lambda \in \mathcal{O}} \log m \quad \text{s.t. } P(\Lambda(\rho), \Psi_m) \leq \varepsilon$$

Asymptotic distillable coherence

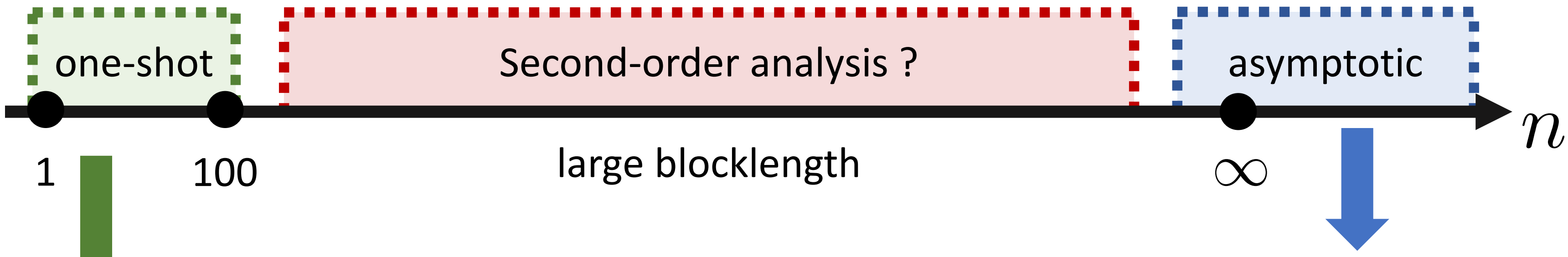
$$C_{d,\mathcal{O}}^{\infty}(\rho) = \lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} C_{d,\mathcal{O}}^{(1),\varepsilon}(\rho^{\otimes n})$$

Why do we do coherence distillation?

1. Quantum algorithm: [Hillery-2016-PRA]
2. Quantum state merging: [Streltsov et al-2016-PRL]
3. Quantum state redistribution: [Anshu-Jain-Streltsov-2018-arxiv]
4. Quantum random number generation: [Ma et al.-2019-PRA, Hayashi-Zhu 2018-PRA]

…

[1.3] 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-PRL]
[Regula-Fang-Wang-Adesso-2018-PRL]
[Chitambar-2018-PRA]
[Lami-2020-TIT]

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

[Regula-Fang-Wang-Adesso-2018-PRL]
[Zhao-Liu-Yuan-Chitambar-Winter-2019-TIT]

[1.4] Second-order analysis

For example:

Information variance

Cumulative distribution function of a standard normal random variable

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

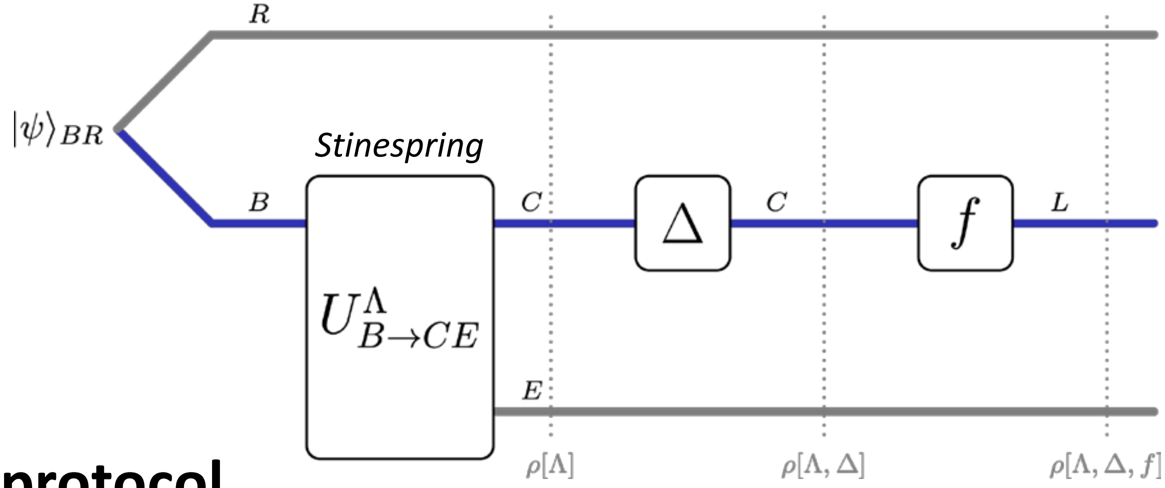
Why do we study the second-order asymptotics?

1. A useful approximation to the distillable coherence for given *finite copies* of resource states.
2. Determines the *rate of convergence* of the distillable coherence to its first order coefficient.
3. Implies the *strong converse property.*

Difficulty

One-shot upper & lower bounds need to *match* dependently on error ε.

[1.5] Incoherent randomness extraction



Blue: Bob
Grey: Eve

Extraction protocol

[Hayashi-Zhu 2018 PRA]

1. Bob holds ρ_B with a purifying system R held by Eve;
2. Bob performs an incoherent operation Λ on system B whose environment system E is also held by Eve;
3. Bob applies a dephasing map (measurement) Δ on his state to obtain classical bits;
4. Bob applies a hash function f to extract randomness that is *secure from Eve.*

One-shot extractable randomness

$$\ell^{\varepsilon}_{\Lambda}(\rho_B) := \max_f \{\log|L| : d_{sec}(\rho[\Lambda,\Delta,f]_{LER}|ER) \le \varepsilon\}$$

$$\ell^{\varepsilon}_{\mathcal{O}}(\rho_B) := \max_{\Lambda\in\mathcal{O}} \ell^{\varepsilon}_{\Lambda}(\rho_B), \quad d_{sec}(\rho_{BR}|R) := \min_{\sigma_R\in\mathcal{S}(R)} P(\rho_{BR}, \pi_B\otimes\sigma_R)$$

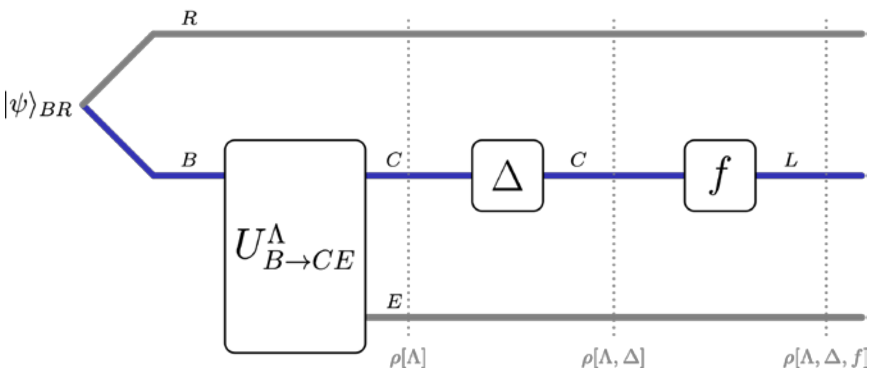
[1.6] Main result 1: one-shot equivalence

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

$$C^{\varepsilon}_{d,\mathcal{O}}(\rho_B) = \ell^{\varepsilon}_{\mathcal{O}}(\rho_B)$$

Coherence distillation   Incoherent randomness extraction

$$\approx$$



maximum number of coherent bits that can be distilled

maximum number of secure random bits that can be extracted

[1.7] Proof ideas

Distillation protocol -> Randomness extraction protocol

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

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

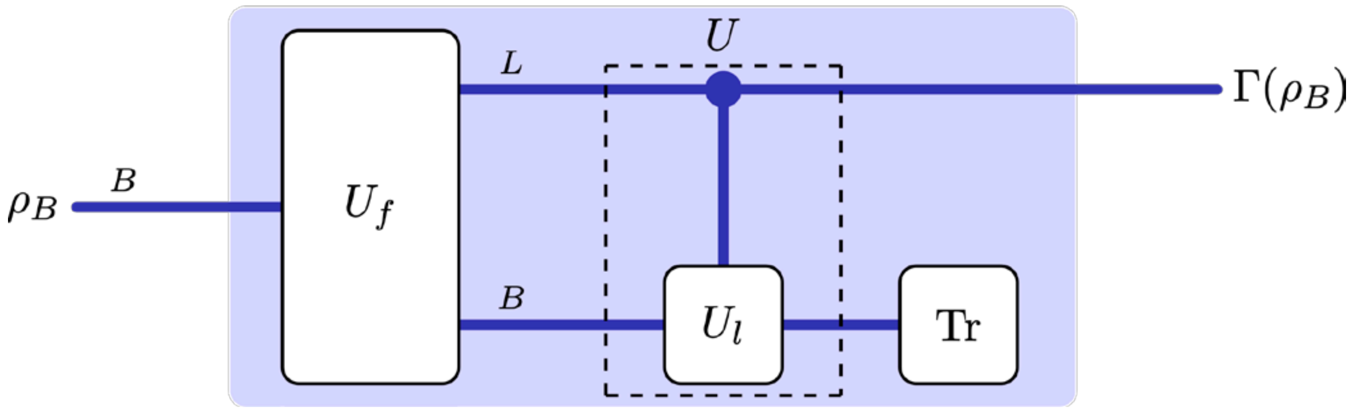
$$d_{sec}(\rho[\Lambda, \Delta, \mathrm{id}]_{CER}|ER) \leq \varepsilon$$

Randomness extraction protocol -> Distillation protocol

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

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

Then there exists Γ in DIIO such that $P(\Gamma_{B\to L}(\rho_B), \Psi_L) \leq \varepsilon$



[1.8] Main result 2: second-order expansions

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

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

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-PRL, Lami-2019-TIT], 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-TIT] and randomness extraction.

[1.9] Proof ideas

[Regula-Fang-Wang-Adesso-2018-PRL]

Converse: $C^{\varepsilon}_{d,\mathcal{O}}(\rho_B^{\otimes n}) \leq C^{\varepsilon}_{d,\mathrm{MIO}}(\rho_B^{\otimes n}) \leq D_H^{\varepsilon^2}(\rho_B^{\otimes n} \| \Delta(\rho_B)^{\otimes n})$

[This work, one-shot equivalence]

Achievability: $\ell^{\varepsilon}_{\mathcal{O}}(\rho_B^{\otimes n}) \geq \ell^{\varepsilon}_{\mathrm{id}}(\rho_B^{\otimes n}) \geq H_{\min}^{\varepsilon-\eta}(A^n | R^n)_{\tilde{\rho}^{\otimes n}} + 4 \log \eta - 3$

[Tomamichel-Hayashi-2013-TIT]

[Tomamichel-Hayashi-2013-TIT; Li-2014-AS]

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

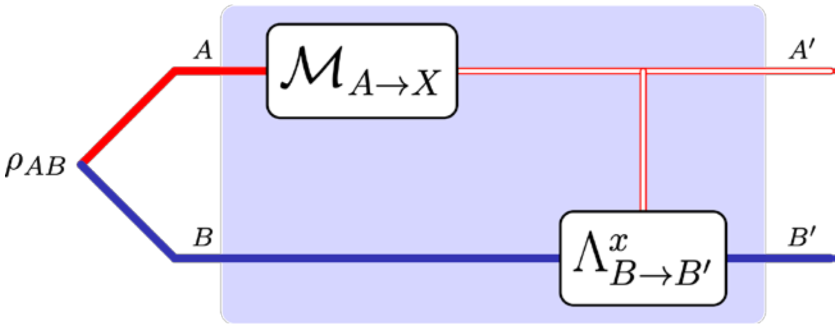
$$D_{\max}^{\varepsilon}(\rho^{\otimes n} \| \sigma^{\otimes n}) = nD(\rho\|\sigma) - \sqrt{nV(\rho\|\sigma)}\, \Phi^{-1}(\varepsilon^2) + O(\log n),$$

PART 2: Assisted Coherence Distillation

[2.1] Assisted coherence theory

Free states: quantum-incoherent states

$$\rho_{AB} = \sum p_i \rho_A^i \otimes |i\rangle\langle i|_B$$



Alice assists Bob to manipulate coherence

Free operations:

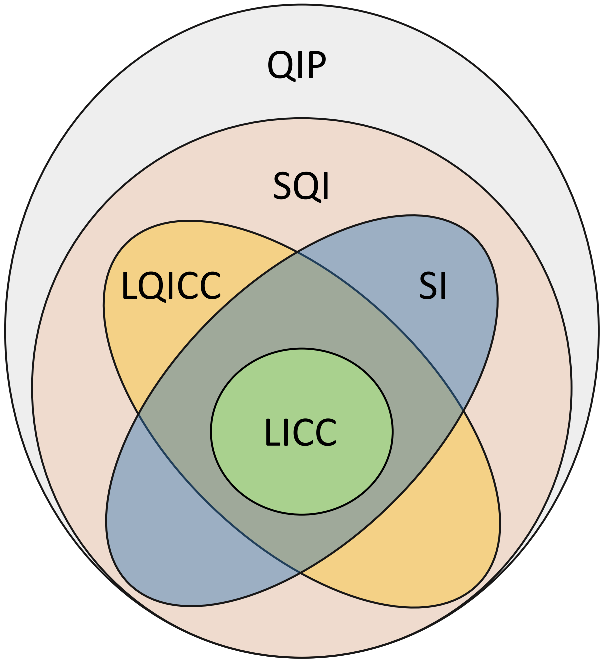
Local incoherent operations and classical com. (**LICC**)

Local quantum-incoherent operations and CC (**LQICC**)

Separable incoherent operations (**SI**)

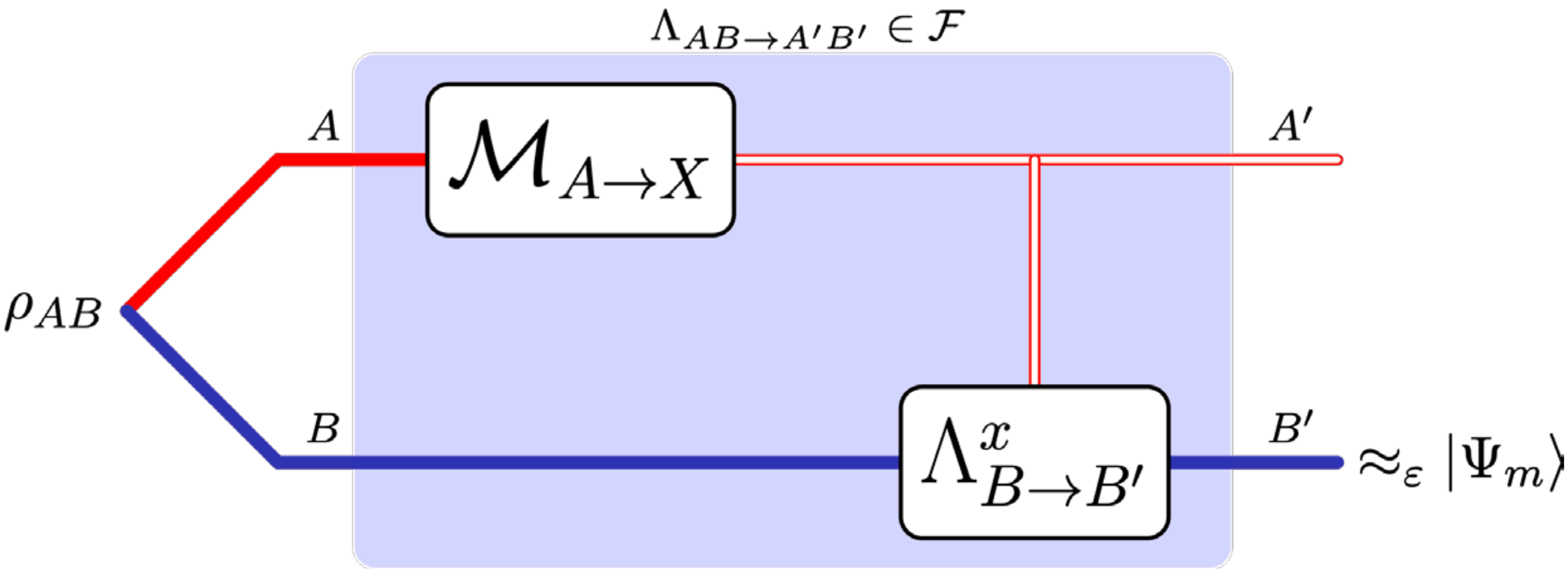
Separable quantum-incoherent operations (**SQI**)

Quantum-incoherent state preserving operations (**QIP**)



Chitambar-Streltsov-Rana-Bera-Adesso-Lewenstein-2016-PRL
Streltsov-Rana-Bera-Lewenstein-2017-PRX

[2.2] Assisted coherence distillation



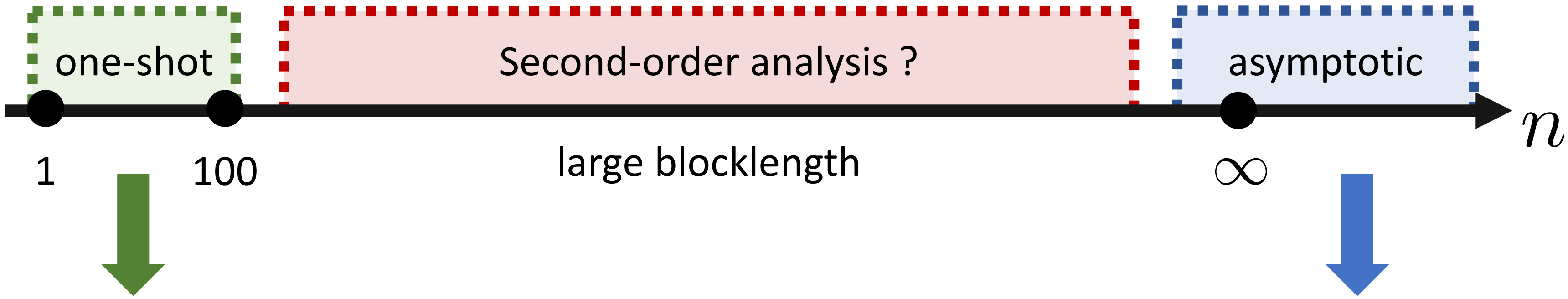
One-shot assisted distillable coherence

$$C^{(1),\varepsilon}_{d,\mathcal{F}}(\rho_{AB}) := \max_{\Lambda\in\mathcal{F}} \log m$$
$$\text{s.t. } P(\operatorname{Tr}_{A'} \Lambda_{AB\to A'B'}(\rho_{AB}), \Psi_m) \le \varepsilon$$

Asymptotic assisted distillable coherence

$$C^{\infty}_{d,\mathcal{F}}(\rho_{AB}) := \lim_{\varepsilon\to 0} \lim_{n\to\infty} \frac{1}{n} C^{(1),\varepsilon}_{d,\mathcal{F}}(\rho^{\otimes n}_{AB})$$

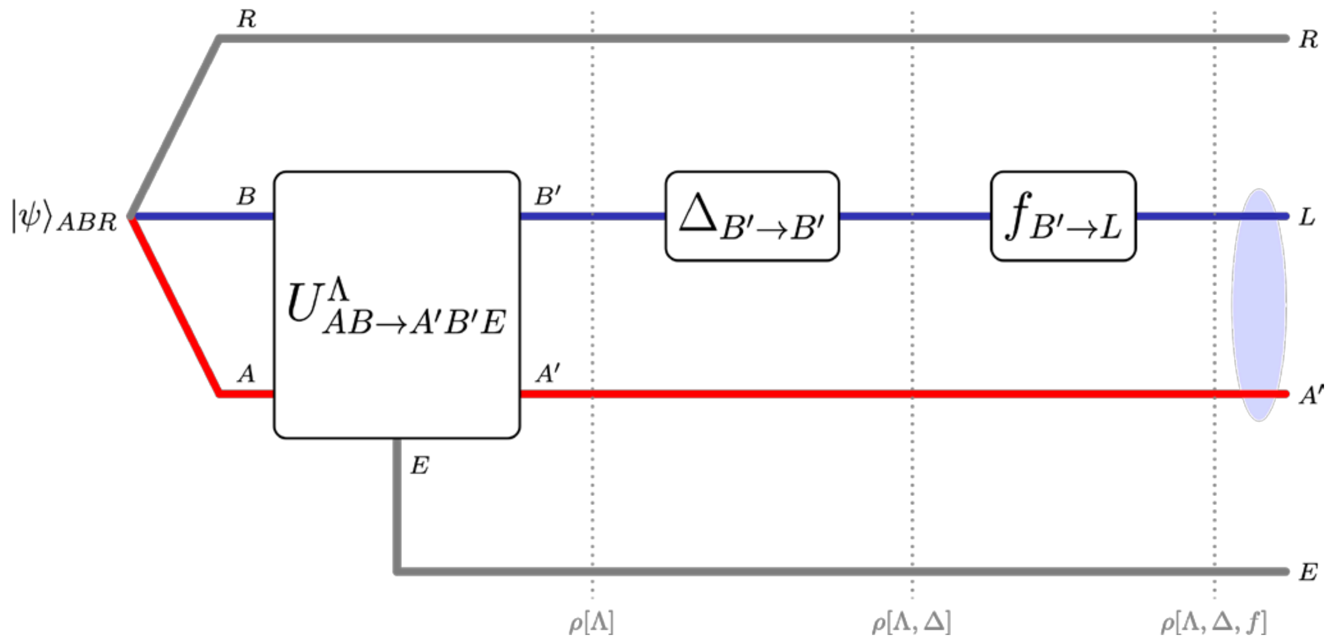
[2.3] Previous works



[Regula-Lami-Streltsov-2018-PRA]
[Vijayan-Chitambar-Hsieh-2018-JPA]

[Chitambar et al-2016-PRL]
[Streltsov-Rana-Bera-Lewenstein-2017-PRX]
[Yamasaki-Vijayan-Hsieh-2019-arxiv]

[2.4] Assisted incoherent randomness extraction



Red: Alice
Blue: Bob
Grey: Eve

Extraction protocol:

1. Alice and Bob hold state ρ_{AB} with a purifying system R held by Eve;
2. Alice and Bob performs an quantum-incoherent operation Λ on AB and the environment system E is held by Eve;
3. Bob applies a dephasing map Δ on his state and obtains the classical bits;
4. Bob applies a hash function f to extract randomness that is *secure from Eve*.

One-shot assisted extractable randomness

$$\ell^{\varepsilon}_{\Lambda}(\rho_{AB}) := \max_{f}\{\log|L| : d_{sec}(\rho[\Lambda,\Delta,f]_{LER}|ER) \le \varepsilon\}\,, \quad \ell^{\varepsilon}_{\mathcal{F}}(\rho_{AB}) := \max_{\Lambda\in\mathcal{F}} \ell^{\varepsilon}_{\Lambda}(\rho_{AB})$$

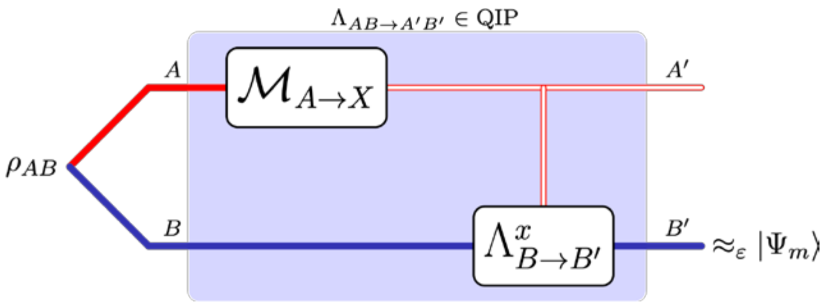
[2.5] Main result 3: one-shot equivalence

For any quantum state ρ_{AB} , error tolerance $\varepsilon \in [0,1]$, and free operation class QIP, it holds

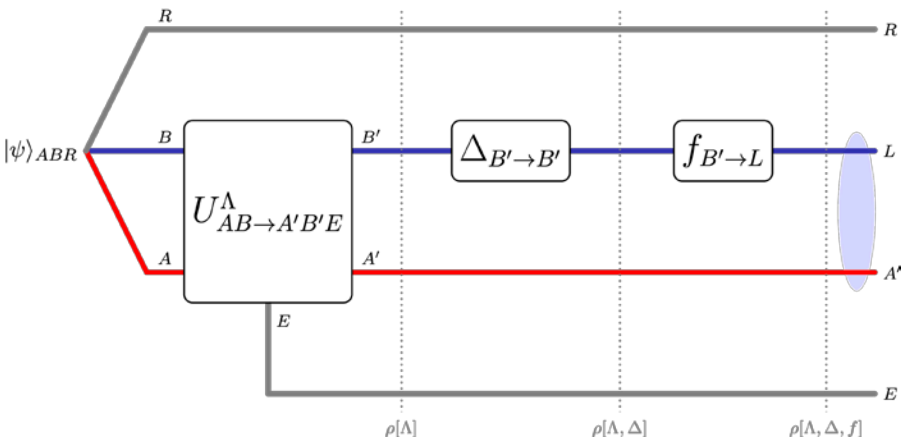
$$C^{\varepsilon}_{d,\mathrm{QIP}}(\rho_{AB}) = \ell^{\varepsilon}_{\mathrm{QIP}}(\rho_{AB})$$

Assisted coherence distillation

Assisted incoherent randomness extraction



$\approx$



maximum number of coherent bits that can be assisted distilled

maximum number of secure random bits that can be assisted extracted

[2.6] Main result 4: second-order expansions

For any quantum state ρ_{AB}, error tolerance $\varepsilon \in [0,1]$, and free operation class $\mathcal{F} \in \{\mathrm{LICC}, \mathrm{LQICC}, \mathrm{SI}, \mathrm{SQI}, \mathrm{QIP}\}$, it holds that

$$C^{\varepsilon}_{d,\mathrm{QIP}}\left(\rho_{AB}^{\otimes n}\right) = nD\left(\rho_{AB}\|\Delta_B(\rho_{AB})\right) + \sqrt{nV\left(\rho_{AB}\|\Delta_B(\rho_{AB})\right)}\Phi^{-1}(\varepsilon^2) + O(\log n),$$
$$\ell^{\varepsilon}_{\mathcal{F}}\left(\rho_{AB}^{\otimes n}\right) = nD\left(\rho_{AB}\|\Delta_B(\rho_{AB})\right) + \sqrt{nV\left(\rho_{AB}\|\Delta_B(\rho_{AB})\right)}\Phi^{-1}(\varepsilon^2) + O(\log n).$$

Remarks:

1. This is the *first* second-order analysis in assisted coherence theory.
2. Recover the unassisted case when ρ_{AB} is product.
3. LICC/LQICC/SI/SQI/QIP have *equivalent power* for assisted randomness extraction in the large block length regime.

[3] Open problems

1. Second order expansion of assisted distillation for LICC/LQICC/SI/SQI

2. Coherence distillation in the unassisted & assisted settings
   - Strong converse exponents
   - Error exponents

1. Coherence cost
   - What are the second order asymptotics of **coherence cost**?