Generalized quantum asymptotic equipartition and applications

Kun FANG

Joint work with Hamza Fawzi and Omar Fawzi

香港中文大學(深圳)
The Chinese University of Hong Kong, Shenzhen

UNIVERSITY OF CAMBRIDGE

ENS DE LYON

arXiv: 2411.04035 & 2502.15659

QIP 2025, Raleigh, February 2025

What is “asymptotic equipartition”?

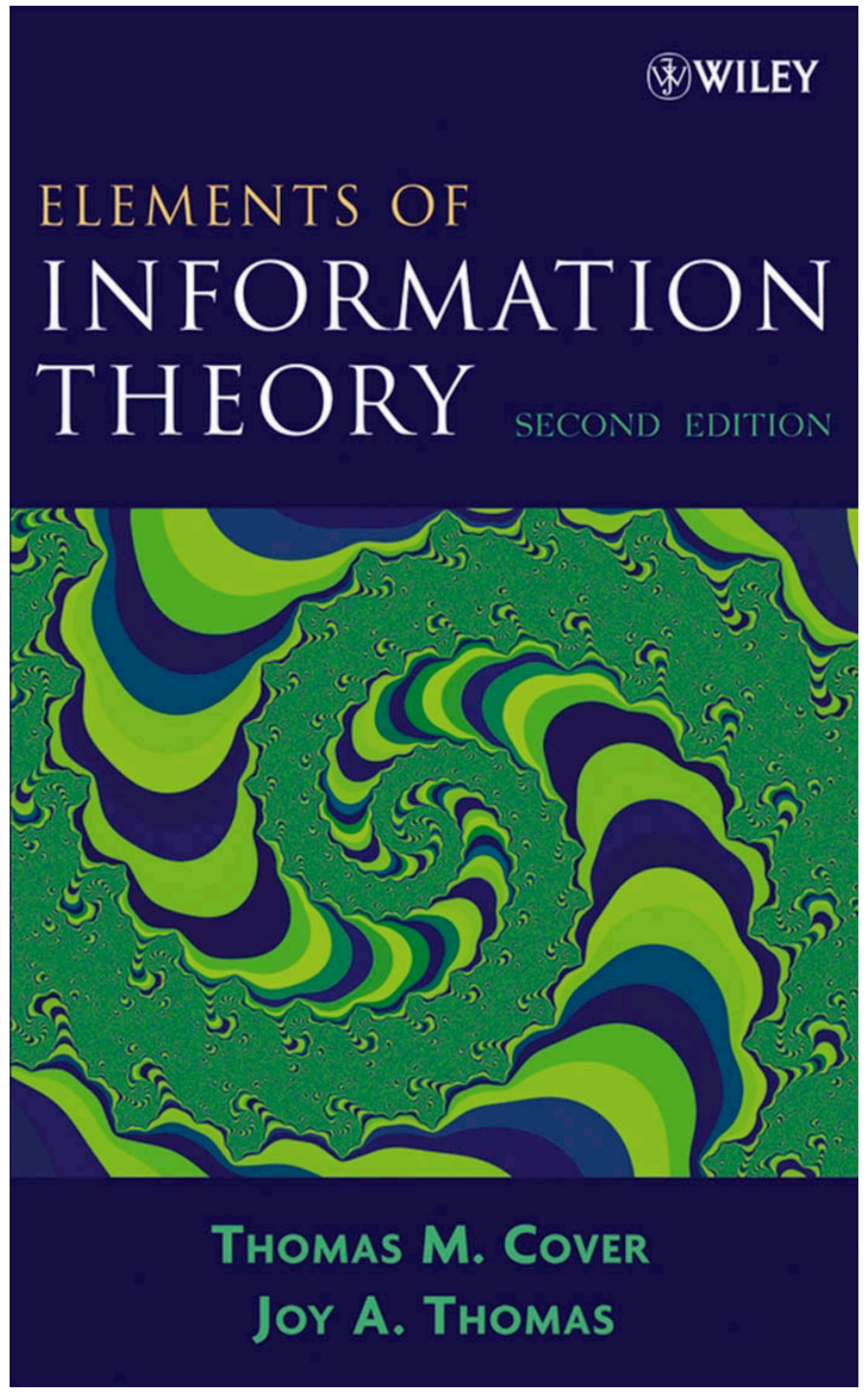
Asymptotic equipartition property (AEP)

A form of the law of large numbers in information theory

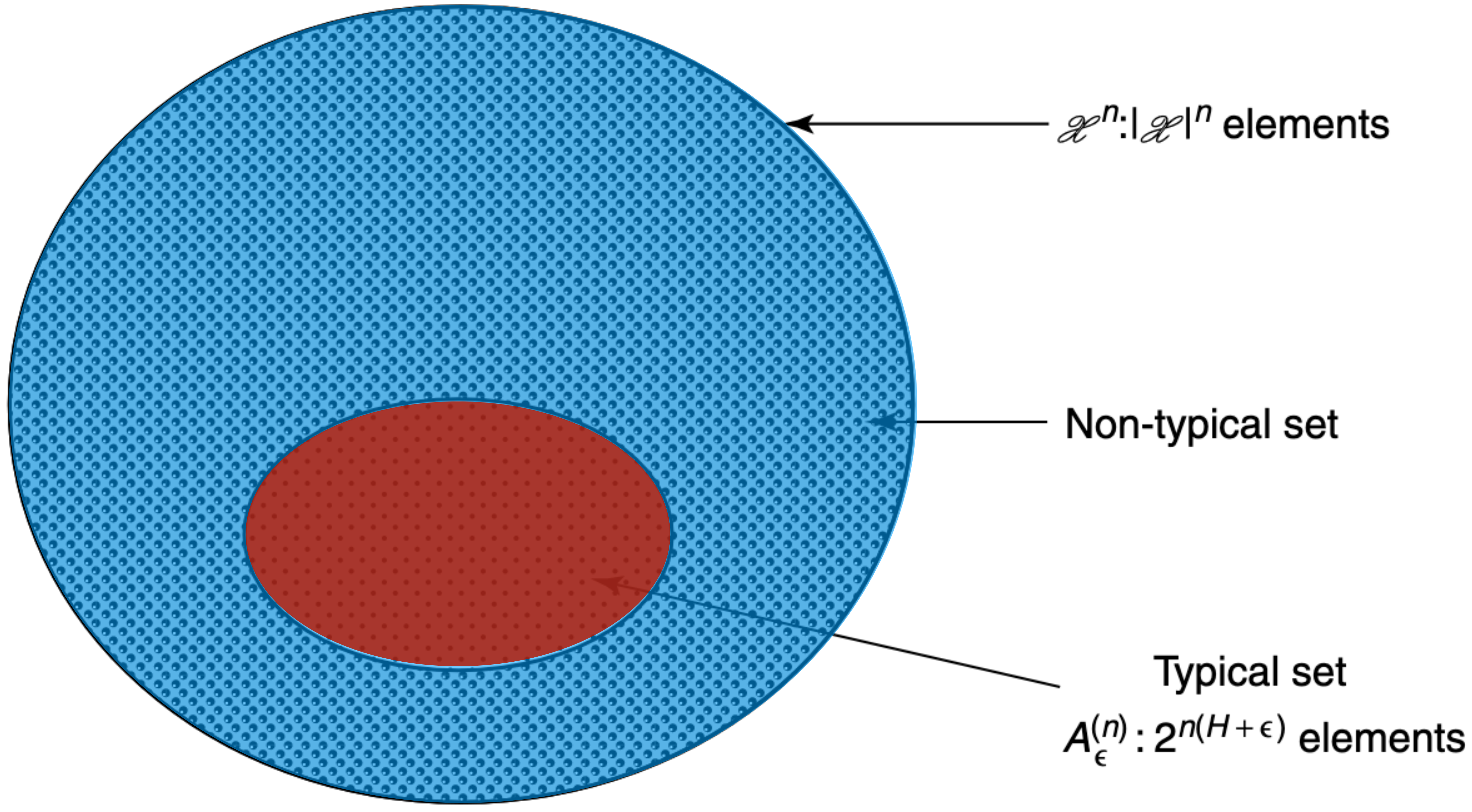
AEP or Shannon-MacMillan-Breiman theorem

Given i.i.d. random variables $X_1, X_2, \cdots, X_n$, the probability $p(X_1, X_2, \cdots, X_n)$ satisfies

$$-\frac{1}{n} \log p(X_1, X_2, \cdots, X_n) \longrightarrow H(X) \quad \text{in probability}$$



What is "asymptotic equipartition"?



Bit strings of length n

Typical set v.s. Non-typical set

Size of the typical set is nearly $2^{nH(X)}$

The typical set has probability nearly 1

Elements in the typical set are nearly **equiprobable**

Lie in the heart of information theory:
data compression, channel coding, cryptography…

More generic form of AEP in divergences

Divergence of interest

Probability distribution

nonnegative function

$$\boxed{\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} \mathbb{D}_{\varepsilon}(P^{\otimes n} \| Q^{\otimes n}) = D(P \| Q)}$$

Smoothing parameter

KL divergence (relative entropy)

More generic form of AEP in divergences

$$\boxed{\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathbb{D}_{\varepsilon}(P^{\otimes n}\|Q^{\otimes n}) = D(P\|Q)}$$

Shannon-McMillan-Breiman theorem:

$\mathbb{D} = H_{\min}$ or $H_{\max}$, $Q = 1$ constant function   e.g. [Tomamichel, Colbeck, Renner 2009]

$H_{\max}$: the size of the typical set & $H_{\min}$: the distribution is uniform on the typical set

Chernoff-Stein Lemma:

$\mathbb{D} = D_H$ hypothesis testing relative entropy

Generalization to quantum AEP?

Generalization to quantum AEP?

Quantum divergence

Density matrix

PSD operator

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathbb{D}_{\varepsilon}(\rho^{\otimes n}\|\sigma^{\otimes n}) = D(\rho\|\sigma)$$

Smoothing parameter

Umegaki (quantum) relative entropy

Generalization to quantum AEP?

$$\boxed{\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathbb{D}_\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) = D(\rho\|\sigma)}$$

- **Hiai and Petz 1991**: $\mathbb{D} = D_H$
- **Ogawa and Nagaoka 2000**: remove ε-dependence in the outer limit

$>$ **Quantum Stein's lemma**

- **Tomamichel, Colbeck, Renner 2009**: $\sigma_{AB} = I_A \otimes \rho_B$, $H_{\min}(A\,|\,B)$ and $H_{\max}(A\,|\,B)$
- **Tomamichel, Hayashi 2013**: $\mathbb{D} = D_{\max}$ ……

Many applications: quantum data compression, quantum state merging, quantum channel coding, quantum cryptography, and quantum resource theory…

Generalization to quantum AEP?

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathbb{D}_\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) = D(\rho\|\sigma)$$

Limited to singleton and i.i.d. structure

Generalization to quantum AEP?

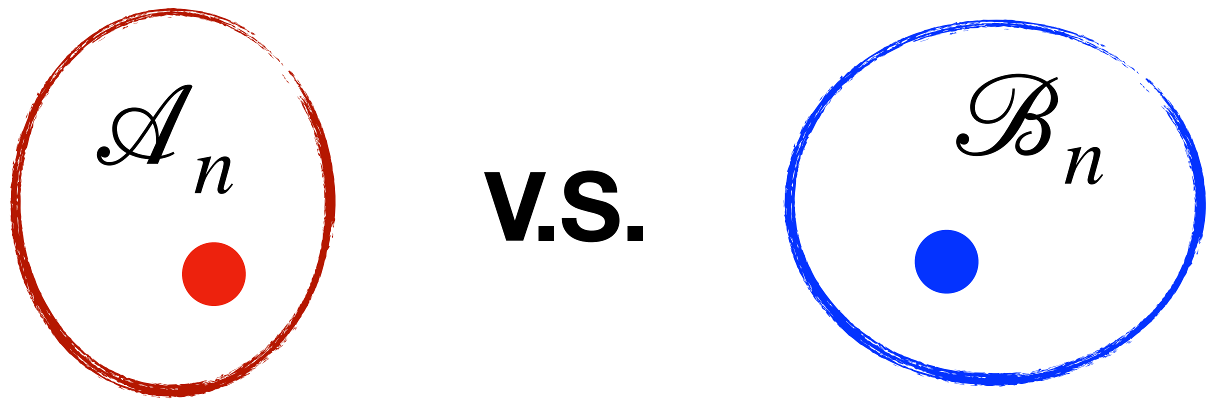
$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathbb{D}_\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) = D(\rho\|\sigma)$$

Limited to singleton and i.i.d. structure

What if?

Correlation: **beyond i.i.d.** source $\rho_n \neq \rho^{\otimes n}$, $\sigma_n \neq \sigma^{\otimes n}$

Uncertainty: **not singleton** $\rho_n \in \mathscr{A}_n$ and $\sigma_n \in \mathscr{B}_n$



e.g. composite hypothesis

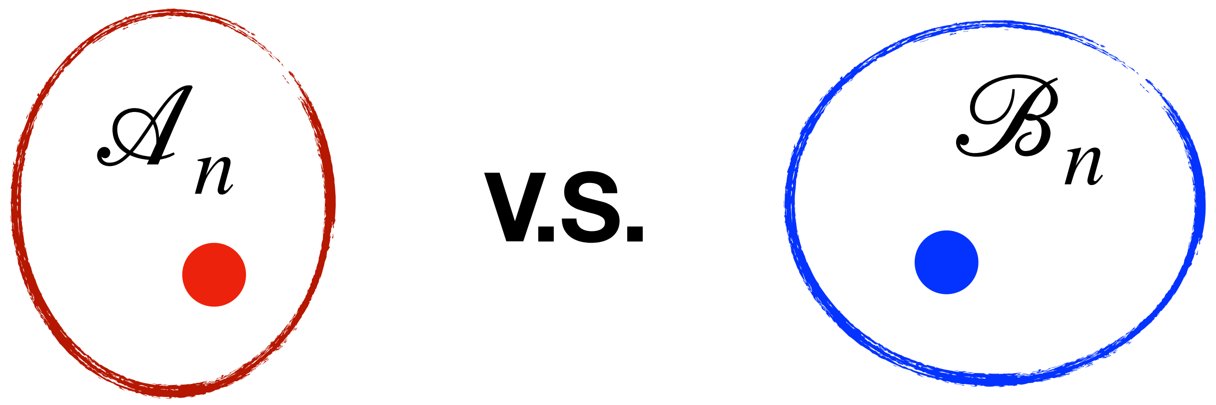
Generalization to quantum AEP?

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} \mathbb{D}_\varepsilon(\rho^{\otimes n} \| \sigma^{\otimes n}) = D(\rho \| \sigma)$$

What if?

Correlation: **beyond i.i.d.** source $\rho_n \neq \rho^{\otimes n}$, $\sigma_n \neq \sigma^{\otimes n}$

Uncertainty: **not singleton** $\rho_n \in \mathscr{A}_n$ and $\sigma_n \in \mathscr{B}_n$



e.g. composite hypothesis

Practical motivations in the classical setting e.g. [Levitan and Nerhav 2002, TIT]

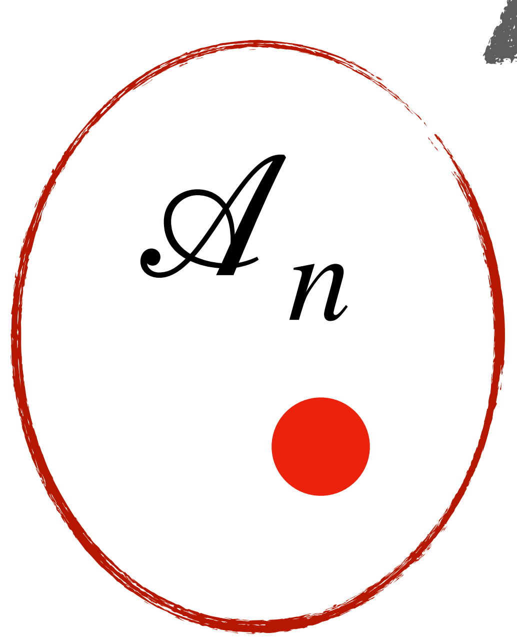
Classification with training sequences (e.g. speech recognition, signal detection)
Detection of messages via unknown channels (e.g. radar target detection, watermark detection)

Generalization to quantum AEP beyond i.i.d. and singleton

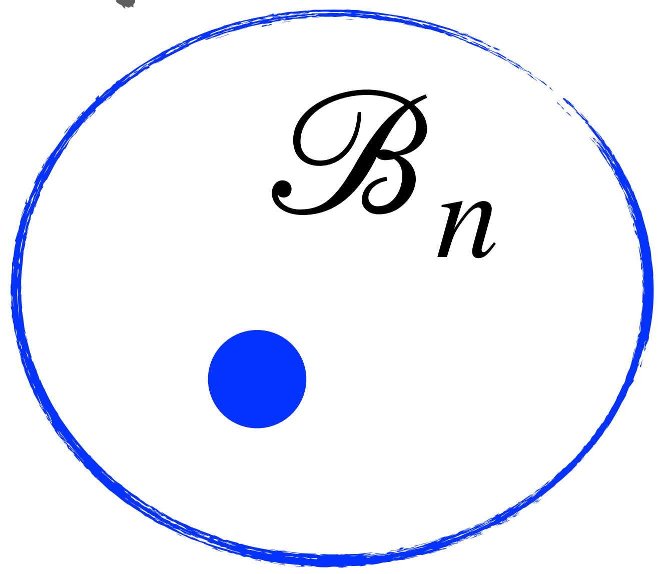
Generalization to quantum AEP beyond i.i.d. and singleton

$$\boxed{\lim_{n\to\infty}\frac{1}{n}\mathbb{D}_\varepsilon(\mathscr{A}_n\|\mathscr{B}_n) = ?}$$

A set of quantum states



V.S.



A set of PSD operators

$$\mathbb{D}_\varepsilon(\mathscr{A}_n\|\mathscr{B}_n) := \inf_{\rho_n\in\mathscr{A}_n,\sigma_n\in\mathscr{B}_n} \mathbb{D}_\varepsilon(\rho_n\|\sigma_n)$$

Generalization to quantum AEP beyond i.i.d. and singleton

$$\boxed{\lim_{n\to\infty} \frac{1}{n} \mathbb{D}_\varepsilon(\mathscr{A}_n \| \mathscr{B}_n) = ?}$$

A very **general framework** that contains almost all existing quantum AEP in the literature
Including *the generalized quantum Stein's lemma*,
where $\mathscr{A}_n = \{\rho^{\otimes n}\}$ and $\mathscr{B}_n$ a set of quantum states

Long Plenary 2 by Hayashi and Yamasaki & **Short Plenary 3** by Lami, Berta, Regula

Generalization to quantum AEP beyond i.i.d. and singleton

Our answer

$$\lim_{n\to\infty} \frac{1}{n} \mathbb{D}_\varepsilon(\mathscr{A}_n \| \mathscr{B}_n) = D^\infty(\mathscr{A} \| \mathscr{B})$$

$$\mathbb{D} \in \{D_H, D_{\max}\}$$

$$D^\infty(\mathscr{A} \| \mathscr{B}) := \lim_{n\to\infty} \frac{1}{n} D(\mathscr{A}_n \| \mathscr{B}_n)$$

Generalization to quantum AEP beyond i.i.d. and singleton

Our answer

$$\lim_{n\to\infty} \frac{1}{n} \mathbb{D}_{\varepsilon}(\mathscr{A}_n \| \mathscr{B}_n) = D^{\infty}(\mathscr{A} \| \mathscr{B})$$

Generality (divergence):

two extreme cases $\mathbb{D} \in \{D_H, D_{\max}\}$

any divergence in between or equivalent, yield the same result

Our answer

$$\lim_{n\to\infty} \frac{1}{n} \mathbb{D}_\varepsilon(\mathscr{A}_n \| \mathscr{B}_n) = D^\infty(\mathscr{A} \| \mathscr{B})$$

Generality (sets):

Polar set $\mathscr{C}^\circ := \{X : \langle X, Y\rangle \leq 1, \forall\, Y \in \mathscr{C}\}$

(A.1) Each $\mathscr{A}_n$ is convex and compact;

(A.2) Each $\mathscr{A}_n$ is permutation-invariant;

(A.3) $\mathscr{A}_m \otimes \mathscr{A}_k \subseteq \mathscr{A}_{m+k}$, for all $m, k \in \mathbb{N}$;

(A.4) $(\mathscr{A}_m)^\circ_+ \otimes (\mathscr{A}_k)^\circ_+ \subseteq (\mathscr{A}_{m+k})^\circ_+$, for all $m, k \in \mathbb{N}$;

Our answer

$$\lim_{n\to\infty} \frac{1}{n} \mathbb{D}_\varepsilon(\mathscr{A}_n \| \mathscr{B}_n) = D^\infty(\mathscr{A} \| \mathscr{B})$$

Generality (sets):

Polar set $\mathscr{C}^\circ := \{X : \langle X, Y \rangle \leq 1, \forall\, Y \in \mathscr{C}\}$

(A.1) Each $\mathscr{A}_n$ is convex and compact;

(A.2) Each $\mathscr{A}_n$ is permutation-invariant;

(A.3) $\mathscr{A}_m \otimes \mathscr{A}_k \subseteq \mathscr{A}_{m+k}$, for all $m, k \in \mathbb{N}$;

(A.4) $(\mathscr{A}_m)^\circ_+ \otimes (\mathscr{A}_k)^\circ_+ \subseteq (\mathscr{A}_{m+k})^\circ_+$, for all $m, k \in \mathbb{N}$;

Sets	Mathematical descriptions
Singleton	$\{\rho^{\otimes n}\}$ with $\rho \in \mathscr{D}(\mathcal{H})$
Conditional states	$\{I_n \otimes \rho_n : \rho_n \in \mathscr{D}(\mathcal{H}^{\otimes n})\}$
Channel image	$\{\mathcal{N}^{\otimes n}(\rho_n) : \rho_n \in \mathscr{D}(\mathcal{H}^n)\}$ with a quantum channel $\mathcal{N}$
Recovery set	$\{\mathcal{N}_{B^n \to C^n}(\rho_{AB}^{\otimes n}) : \mathcal{N} \in \mathrm{CPTP}(B^n : C^n)\}$ with $\rho \in \mathscr{D}(AB)$
Extensions set	$\{\omega_n \in \mathscr{D}(A^n B^n) : \mathrm{Tr}_{B^n} \omega_n = \rho_A^{\otimes n}\}$ with $\rho_A \in \mathscr{D}(A)$
Incoherent states	$\{\rho_n \in \mathscr{D}(\mathcal{H}^{\otimes n}) : \rho_n = \Delta(\rho_n)\}$ with the completely dephasing channel Δ
Rains set	$\{\rho_n \in \mathscr{H}_+(A^n B^n) : \|\rho_n^{\mathsf{T}_{B_1 \cdots B_n}}\|_1 \leq 1\}$ with the partial transpose T_{B_i}
Nonpositive mana	$\{\rho_n \in \mathscr{H}_+(\mathcal{H}^{\otimes n}) : \|\rho_n\|_{W,1} \leq 1\}$ with the Wigner trace norm $\|\cdot\|_{W,1}$

Our answer

$$\lim_{n\to\infty} \frac{1}{n} \mathbb{D}_{\varepsilon}(\mathscr{A}_n \| \mathscr{B}_n) = D^{\infty}(\mathscr{A} \| \mathscr{B})$$

Generality (sets):

Polar set $\mathscr{C}^{\circ} := \{X : \langle X, Y \rangle \leq 1, \forall\, Y \in \mathscr{C}\}$

(A.1) Each $\mathscr{A}_n$ is convex and compact;

(A.2) Each $\mathscr{A}_n$ is permutation-invariant;

(A.3) $\mathscr{A}_m \otimes \mathscr{A}_k \subseteq \mathscr{A}_{m+k}$, for all $m, k \in \mathbb{N}$;

(A.4) $(\mathscr{A}_m)^{\circ}_{+} \otimes (\mathscr{A}_k)^{\circ}_{+} \subseteq (\mathscr{A}_{m+k})^{\circ}_{+}$, for all $m, k \in \mathbb{N}$;

More importantly, **without (A.4)**, the AEP does not hold in general.

Counterexamples e.g.

arXiv: 2501.09303v2 by Hayashi & **arXiv: 2408.07067** by Lami, Berta, Regula

Our answer

$$\lim_{n\to\infty} \frac{1}{n}\mathbb{D}_{\varepsilon}(\mathscr{A}_n\|\mathscr{B}_n) = D^{\infty}(\mathscr{A}\|\mathscr{B})$$

Efficiency:

Regularization instead of single-letter formula. But it can estimated by

$$\frac{1}{m}D_M(\mathscr{A}_m\|\mathscr{B}_m) \leq D^{\infty}(\mathscr{A}\|\mathscr{B}) \leq \frac{1}{m}D(\mathscr{A}_m\|\mathscr{B}_m)$$

with explicit convergence guarantees,

$$\frac{1}{m}D(\mathscr{A}_m\|\mathscr{B}_m) - \frac{1}{m}D_M(\mathscr{A}_m\|\mathscr{B}_m) \leq \frac{1}{m}2(d^2+d)\log(m+d)$$

Efficiently approximate $D^{\infty}(\mathscr{A}\|\mathscr{B})$ within an additive error by a quantum relative entropy program of polynomial size. [arXiv: 2502.15659]

Our answer

$$\lim_{n\to\infty} \frac{1}{n} \mathbb{D}_\varepsilon(\mathscr{A}_n \| \mathscr{B}_n) = D^\infty(\mathscr{A} \| \mathscr{B})$$

Explicit finite n estimate:

$$nD^\infty(\mathscr{A}\|\mathscr{B}) - O(n^{2/3}\log n) \leq \mathbb{D}_\varepsilon(\mathscr{A}_n\|\mathscr{B}_n) \leq nD^\infty(\mathscr{A}\|\mathscr{B}) + O(n^{2/3}\log n)$$

Leading term is regularized, but **still provide an explicit estimate** for finite n, making its **convergence controllable; a rare case in QIT**

Leading term independent of ε (strong converse property)

The second order in $O(n^{2/3}\log n)$ instead of $O(\sqrt{n})$, potential improvement exists

Key technical tools

Measured relative entropy $D_M(\rho\|\sigma) := \sup_M D(P_{\rho,M}\|P_{\sigma,M})$

Superadditivity $D_M(\rho_1 \otimes \rho_2\|\sigma_1 \otimes \sigma_2) \geq D_M(\rho_1\|\sigma_1) + D_M(\rho_2\|\sigma_2)$

$$D(\rho\|\sigma) = \lim_{n\to\infty} \frac{1}{n} D_M(\rho^{\otimes n}\|\sigma^{\otimes n})$$

Subadditivity

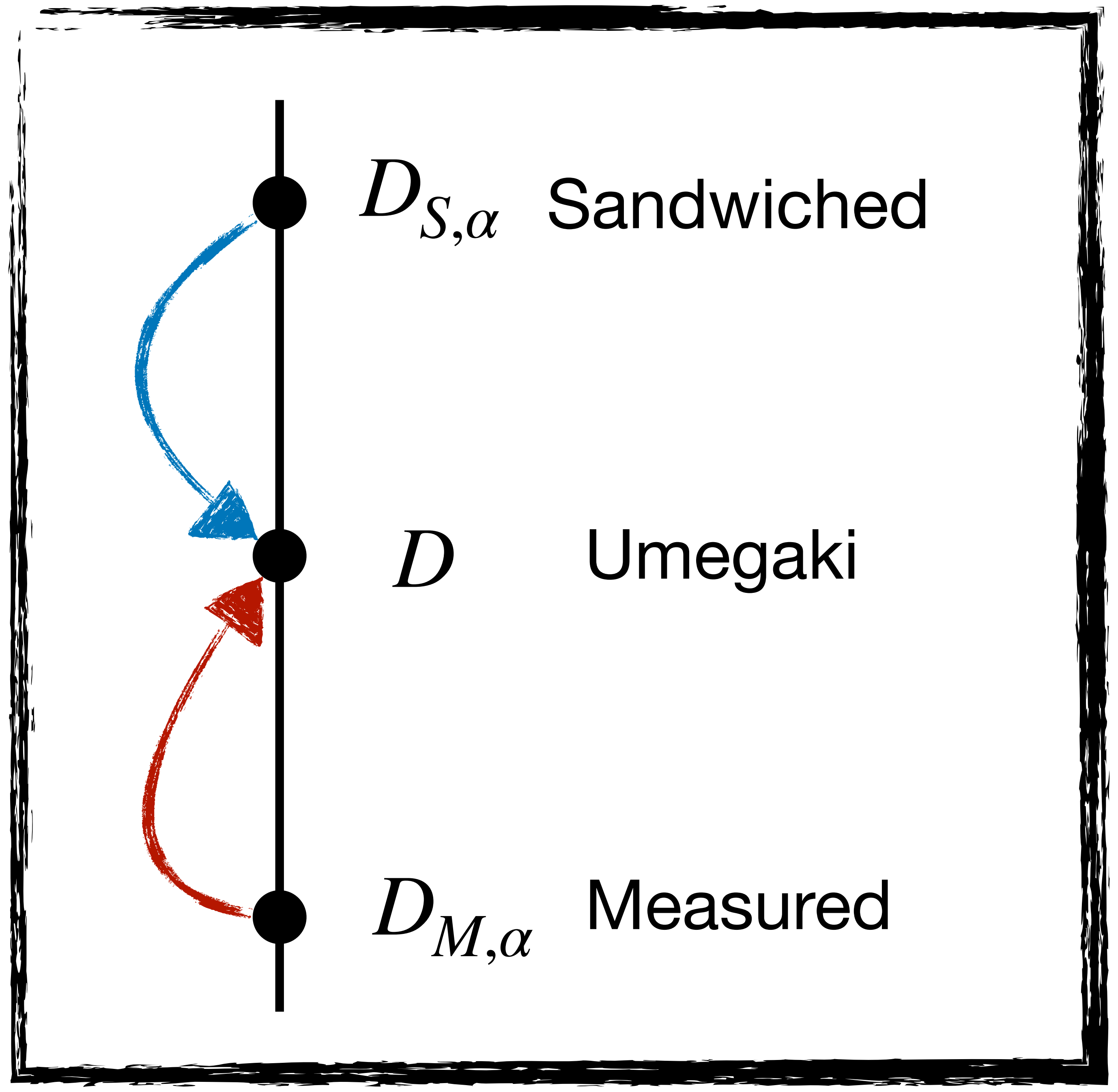
Suppose $\mathscr{A}_1 \otimes \mathscr{A}_2 \subseteq \mathscr{A}_{12}$ and $\mathscr{B}_1 \otimes \mathscr{B}_2 \subseteq \mathscr{B}_{12}$

$$D_{S,\alpha}(\mathscr{A}_{12}\|\mathscr{B}_{12}) \leq D_{S,\alpha}(\mathscr{A}_1\|\mathscr{B}_1) + D_{S,\alpha}(\mathscr{A}_2\|\mathscr{B}_2) \qquad \forall \alpha > 1$$

Superadditivity

Suppose $(\mathscr{A}_1)^\circ_+ \otimes (\mathscr{A}_2)^\circ_+ \subseteq (\mathscr{A}_{12})^\circ_+$ and $(\mathscr{B}_1)^\circ_+ \otimes (\mathscr{B}_2)^\circ_+ \subseteq (\mathscr{B}_{12})^\circ_+$

$$D_{M,\alpha}(\mathscr{A}_{12}\|\mathscr{B}_{12}) \geq D_{M,\alpha}(\mathscr{A}_1\|\mathscr{B}_1) + D_{M,\alpha}(\mathscr{A}_2\|\mathscr{B}_2) \qquad \forall 0 < \alpha < 1$$



Recap: from AEP to generalized quantum AEP

$$-\frac{1}{n}\log p(X_1, X_2, \cdots, X_n) \longrightarrow H(X) \quad \text{in probability}$$

AEP

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathbb{D}_\varepsilon(P^{\otimes n}\|Q^{\otimes n}) = D(P\|Q)$$

Quantum

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathbb{D}_\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) = D(\rho\|\sigma)$$

Generalized

$$\lim_{n\to\infty}\frac{1}{n}\mathbb{D}_\varepsilon(\mathscr{A}_n\|\mathscr{B}_n) = D^\infty(\mathscr{A}\|\mathscr{B})$$

Applications

1. **Quantum hypothesis testing between two sets of states**

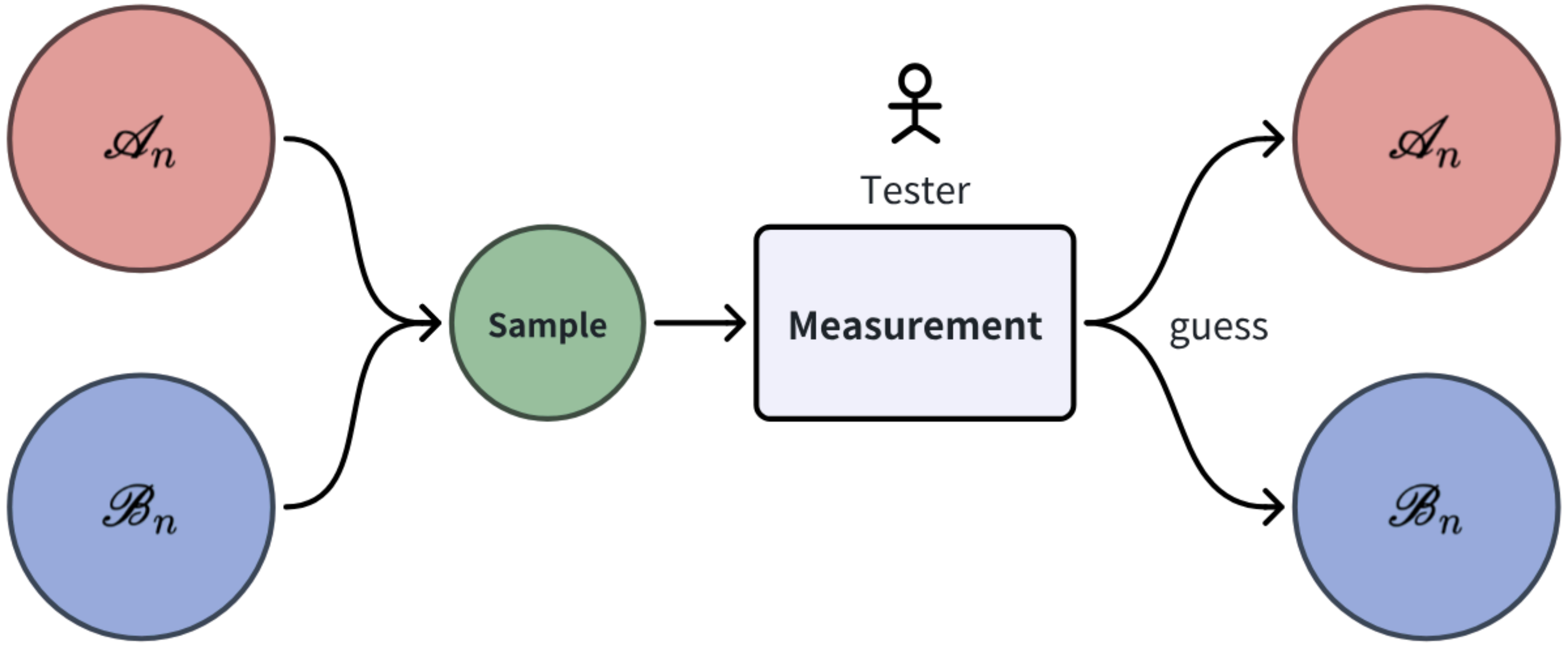
2. **Adversarial quantum channel discrimination**

3. A relative entropy accumulation theorem

4. Efficient bounds for quantum resource theory

Application 1: Quantum hypothesis testing between two sets of states

A tester draws samples from *two sets of quantum states*,
and performs measurements to determine which set the sample belongs to.



Type-I error

$$\alpha(\mathscr{A}_n, M_n) := \sup_{\rho_n \in \mathscr{A}_n} \mathrm{Tr}\,[\rho_n(I - M_n)]$$

Worst-case

Type-II error

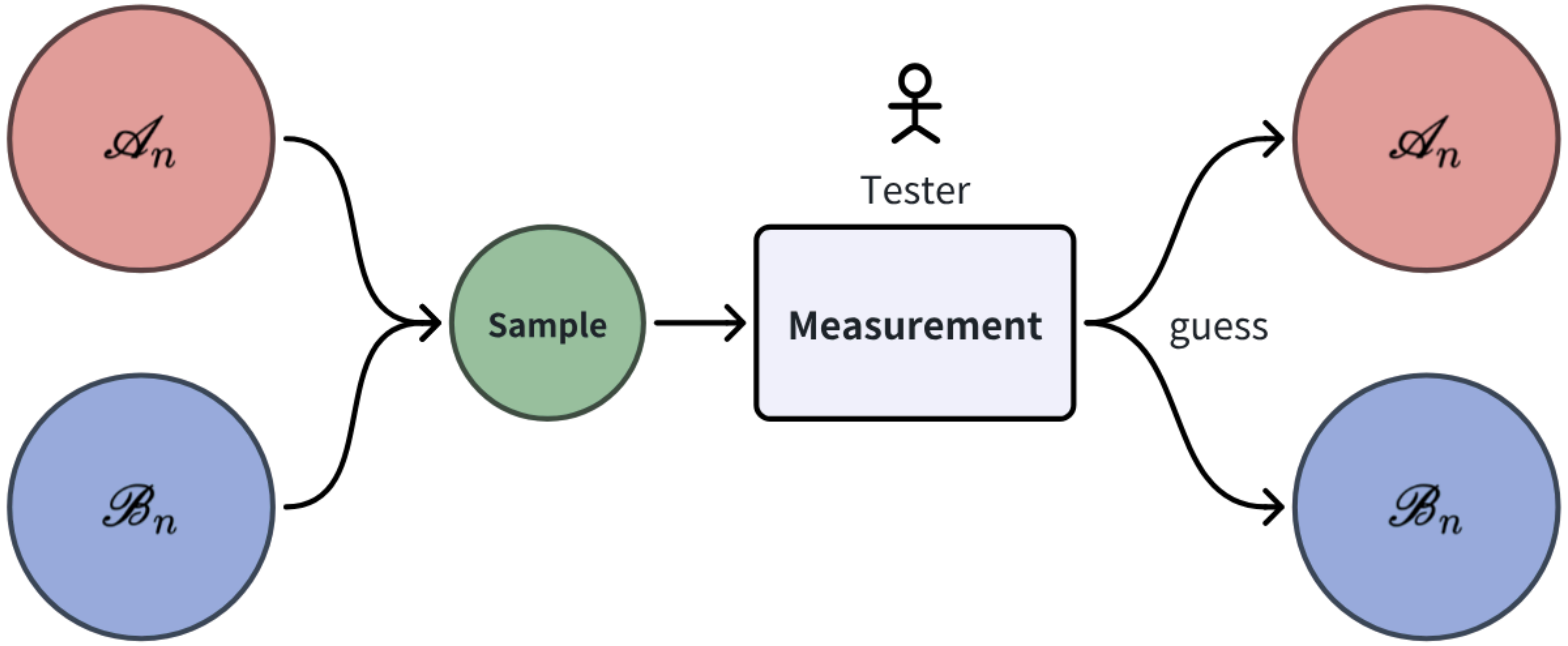
$$\beta(\mathscr{B}_n, M_n) := \sup_{\sigma_n \in \mathscr{B}_n} \mathrm{Tr}\,[\sigma_n M_n]$$

As in standard hypothesis testing, the tester will make two types of errors:

Type-I error: sample from $\mathscr{A}_n$, but classified as from $\mathscr{B}_n$,
Type-II error: sample from $\mathscr{B}_n$, but classified as from $\mathscr{A}_n$.

Application 1: Quantum hypothesis testing between two sets of states

A tester draws samples from *two sets of quantum states*,
and performs measurements to determine which set the sample belongs to.



Type-I error

$$\alpha(\mathscr{A}_n, M_n) := \sup_{\rho_n \in \mathscr{A}_n} \operatorname{Tr}[\rho_n(I - M_n)]$$

Worst-case

Type-II error

$$\beta(\mathscr{B}_n, M_n) := \sup_{\sigma_n \in \mathscr{B}_n} \operatorname{Tr}[\sigma_n M_n]$$

Goal: Determine the optimal exponent at which the type-II error probability decays, while keeping the type-I error within a fixed threshold ε (to control over false positives)

e.g. COVID-19: healthy people get a positive test

$$\beta_\varepsilon(\mathscr{A}_n \| \mathscr{B}_n) := \inf_{0 \le M_n \le I} \left\{ \beta(\mathscr{B}_n, M_n) : \alpha(\mathscr{A}_n, M_n) \le \varepsilon \right\}$$

$$\beta_\varepsilon(\mathscr{A}_n \| \mathscr{B}_n) \approx ?$$

Application 1: Quantum hypothesis testing between two sets of states

Our answer

$$\lim_{n\to\infty} -\frac{1}{n}\log \beta_\varepsilon(\mathscr{A}_n\|\mathscr{B}_n) = D^\infty(\mathscr{A}\|\mathscr{B}) \qquad \forall \varepsilon \in (0,1)$$

✔ **Classical Chernoff-Stein Lemma**

✔ **Quantum Stein's Lemma [Hiai, Petz 1991; Ogawa, Nagaoka**

Let $\mathscr{A}_n = \{\rho^{\otimes n}\}$ and $\mathscr{B}_n = \{\sigma^{\otimes n}\}$ be two singletons.

Generalized Quantum Stein's Lemma ($\mathscr{A}_n = \{\rho^{\otimes n}\}$)

Long Plenary 2 by Hayashi and Yamasaki & **Short Plenary 3** by Lami, Berta, Regula

Story: Generalized Quantum Stein's Lemma ($\mathscr{A}_n = \{\rho^{\otimes n}\}$)

Two different solutions

Trigger

2010

Brandão and Plenio

Initial statement
Plenty of applications

(Related to
1k+citations)

2021

KF, Gour, Wang

Channel Stein's lemma

Triggers the finding
of a gap
in the original proof

2023

Berta, Brandão, Gour, Lami,
Plenio, Regula, Tomamichel

Formally point out
the gap and
study the consequences

2024

Hayashi and Yamasaki

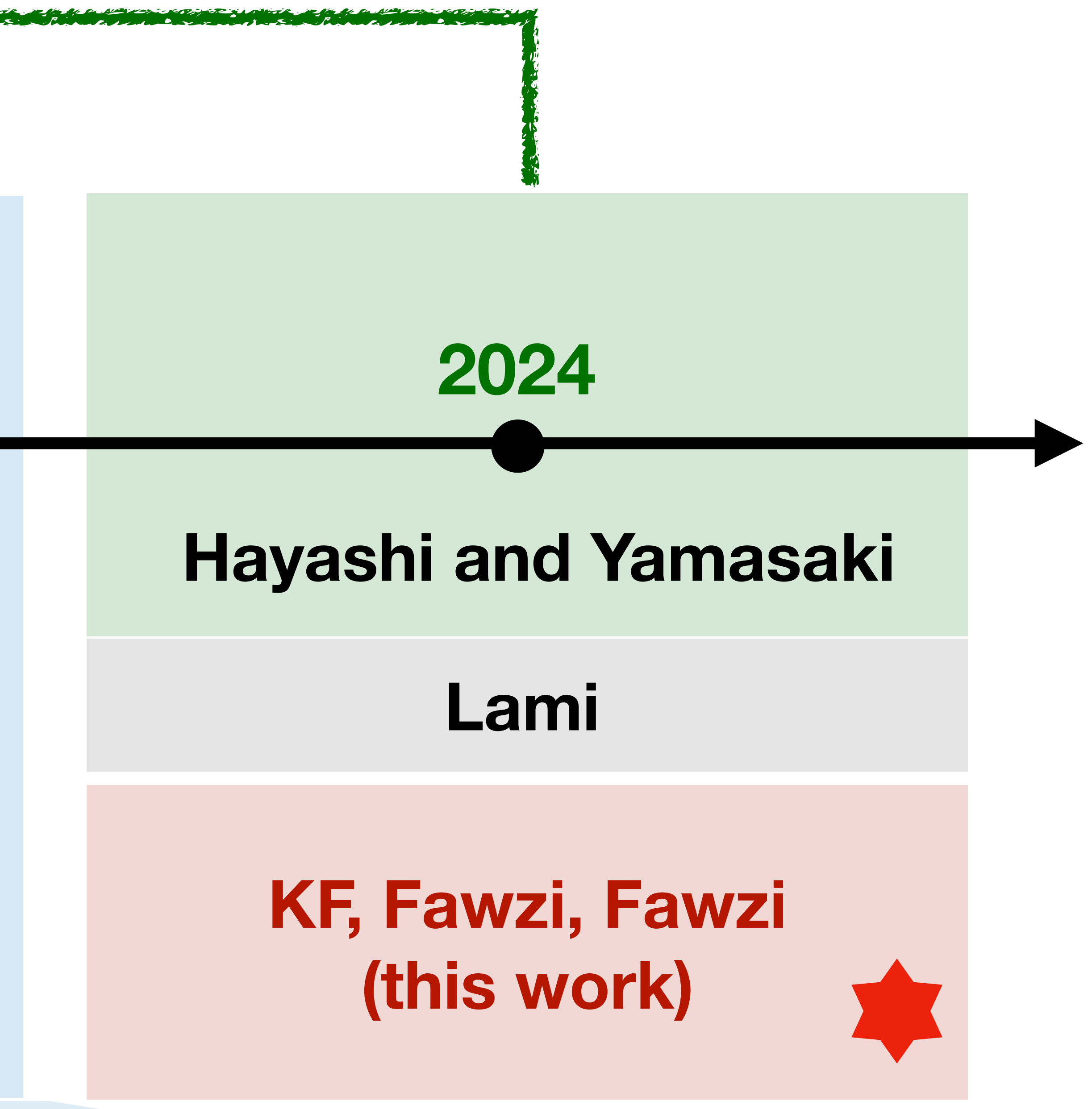
Lami

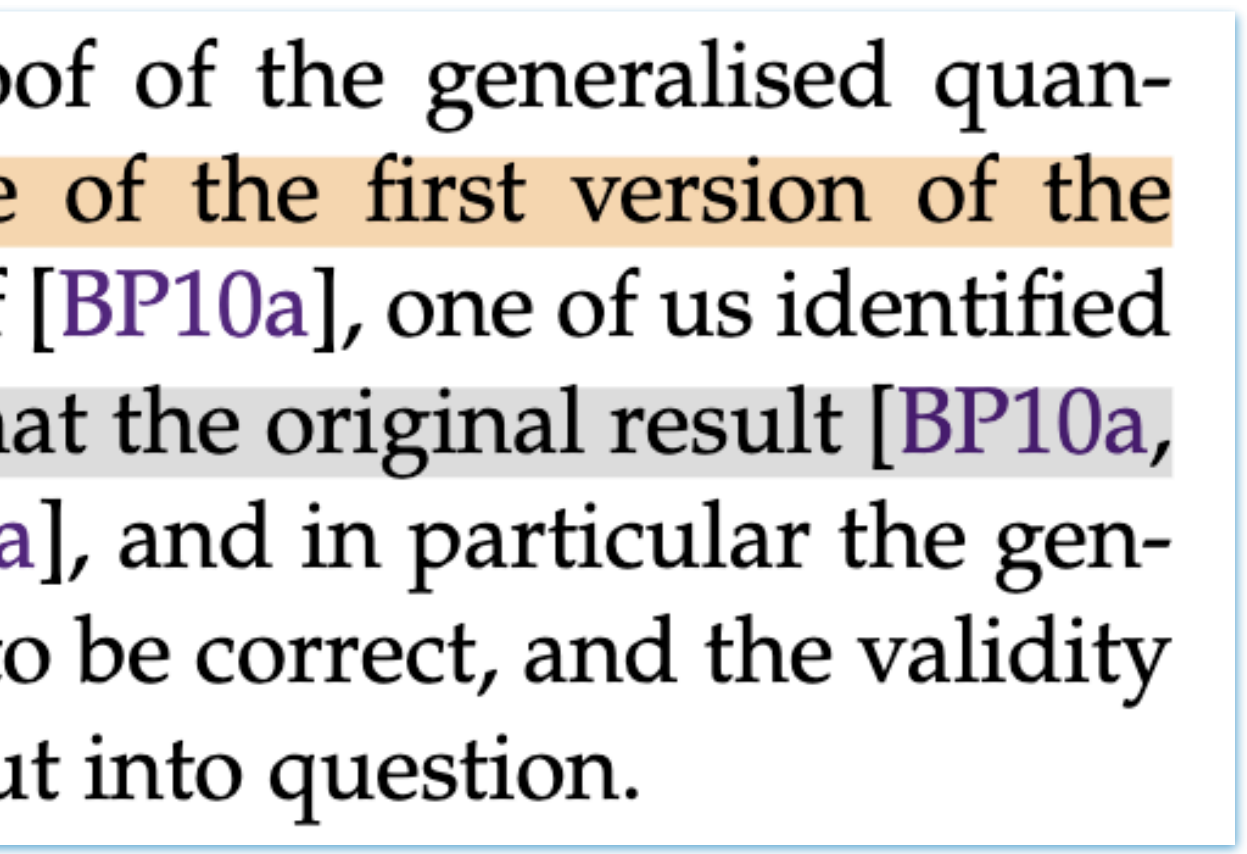
KF, Fawzi, Fawzi
(this work)

A.1		A.3
A.1	A.2	A.3
A.1	A.2	A.3

However, an issue has recently been found in the claimed proof of the generalised quantum Stein's lemma in [BP10a]. Specifically, after the appearance of the first version of the preprint [FGW21] that studied a related setting using the methods of [BP10a], one of us identified a mistake in [FGW21, Lemma 16], which then led to the discovery that the original result [BP10a, Lemma III.9] is incorrect. This means that the main claims of [BP10a], and in particular the generalised quantum Stein's lemma introduced therein, are not known to be correct, and the validity of a number of results that build on those findings is thus directly put into question.

Story: Generalized Quantum Stein's Lemma ($\mathscr{A}_n = \{\rho^{\otimes n}\}$)




…of of the generalised quan-
…e of the first version of the
…f [BP10a], one of us identified
…at the original result [BP10a,
…a], and in particular the gen-
…o be correct, and the validity
…ut into question.

A.1		A.3		A.5	
A.1	A.2	A.3		A.5	A.6
A.1	A.2	A.3	A.4		

(A.1) Each $\mathscr{A}_n$ is convex and compact;

(A.2) Each $\mathscr{A}_n$ is permutation-invariant;

(A.3) $\mathscr{A}_m \otimes \mathscr{A}_k \subseteq \mathscr{A}_{m+k}$, for all $m, k \in \mathbb{N}$;

(A.5) $\mathscr{A}_1$ contains a full-rank state

(A.6) Each $\mathscr{A}_n$ is closed under partial traces

(A.4) $(\mathscr{A}_m)_+^\circ \otimes (\mathscr{A}_k)_+^\circ \subseteq (\mathscr{A}_{m+k})_+^\circ$, for all $m, k \in \mathbb{N}$;

Story: Generalized Quantum Stein's Lemma ($\mathscr{A}_n = \{\rho^{\otimes n}\}$)

2024

Hayashi and Yamasaki	A.1		A.3		A.5	
Lami	A.1	A.2	A.3		A.5	A.6
KF, Fawzi, Fawzi (this work)	A.1	A.2	A.3	A.4		

(A.1) Each $\mathscr{A}_n$ is convex and compact;

(A.2) Each $\mathscr{A}_n$ is permutation-invariant;

(A.3) $\mathscr{A}_m \otimes \mathscr{A}_k \subseteq \mathscr{A}_{m+k}$, for all $m, k \in \mathbb{N}$;

(A.5) $\mathscr{A}_1$ contains a full-rank state

(A.6) Each $\mathscr{A}_n$ is closed under partial traces

(A.4) $(\mathscr{A}_m)^\circ_+ \otimes (\mathscr{A}_k)^\circ_+ \subseteq (\mathscr{A}_{m+k})^\circ_+$, for all $m, k \in \mathbb{N}$;

Our result is incomparable to the previous generalized quantum Stein lemma.

Weaker: assume (A.4) for $\mathscr{B}_n$

Stronger: 1. composite null hypothesis $\mathscr{A}_n$ instead of $\rho^{\otimes n}$

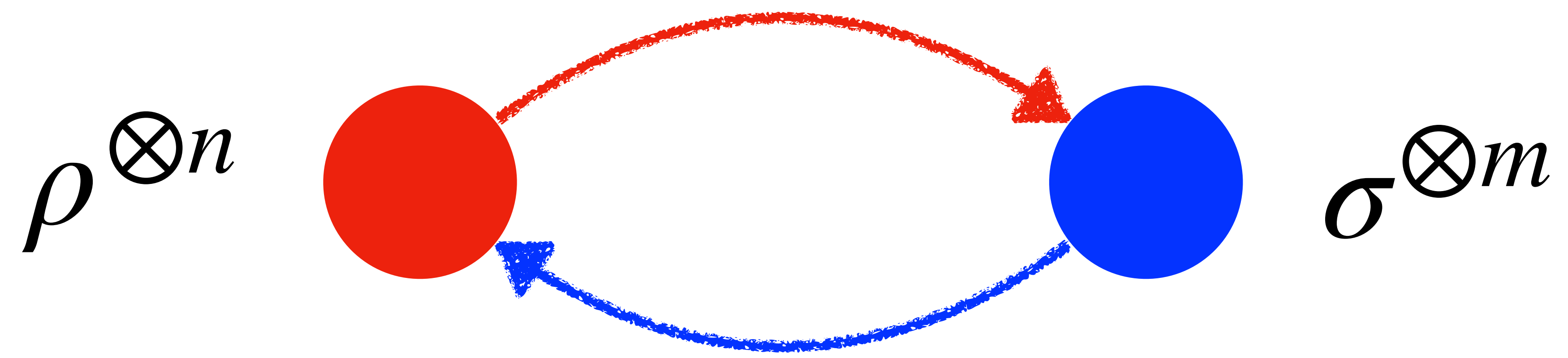
2. efficient and controlled approximations of the Stein's exponent $D^\infty(\mathscr{A}\|\mathscr{B})$

solves open problems

in [Brandão, Harrow, Lee, Peres, 2020, TIT] and [Mosonyi, Szilagyi, Weiner, 2022, TIT]

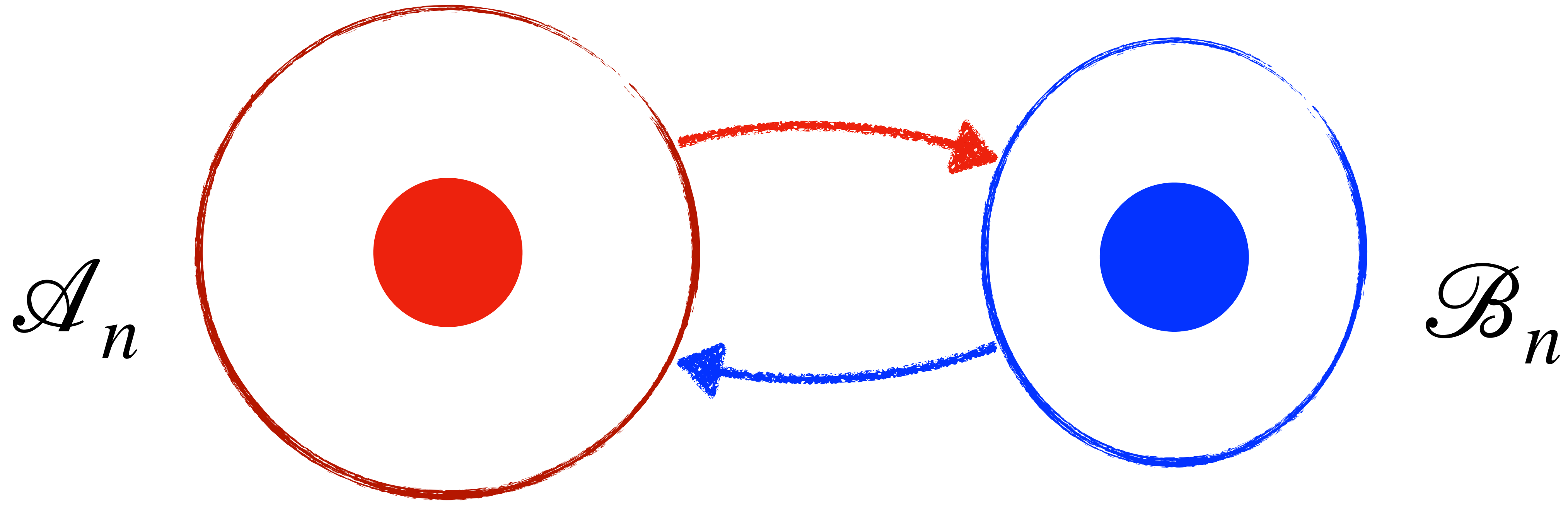
Application 1’: Quantum resource theory and its reversibility

a.k.a, second law



Standard resource manipulation

Asymptotic resource nongenerating operations
[Brandão and Plenio, 2010]



Resource manipulation with partial information

Lack of knowledge of the states
Different copies of the sources
can exhibit correlation in nature

Our answer

Optimal transformation rate

$$r\left(\mathscr{A} \xrightarrow{\text{RNG}} \mathscr{B}\right) = \frac{D^{\infty}(\mathscr{A}\|\mathscr{F})}{D^{\infty}(\mathscr{B}\|\mathscr{F})}$$

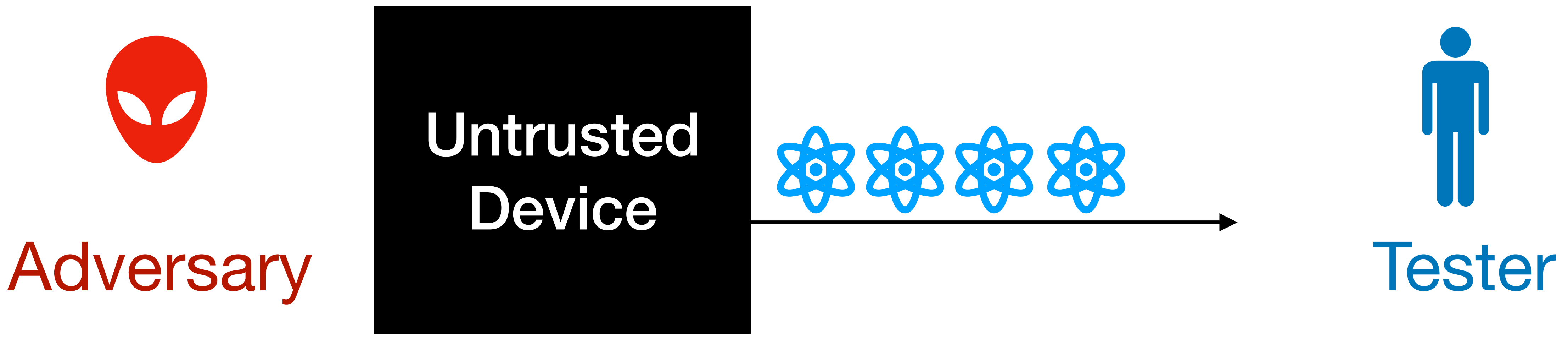
$\mathscr{F}$ is the set of free states

Application 2: adversarial quantum channel discrimination

Operational setting:

A tester is working with an **untrusted** quantum device that generates a quantum state upon request

Guarantee: either $\mathscr{N}$ (the bad case) or $\mathscr{M}$ (the good case)



Request samples

Perform measurement

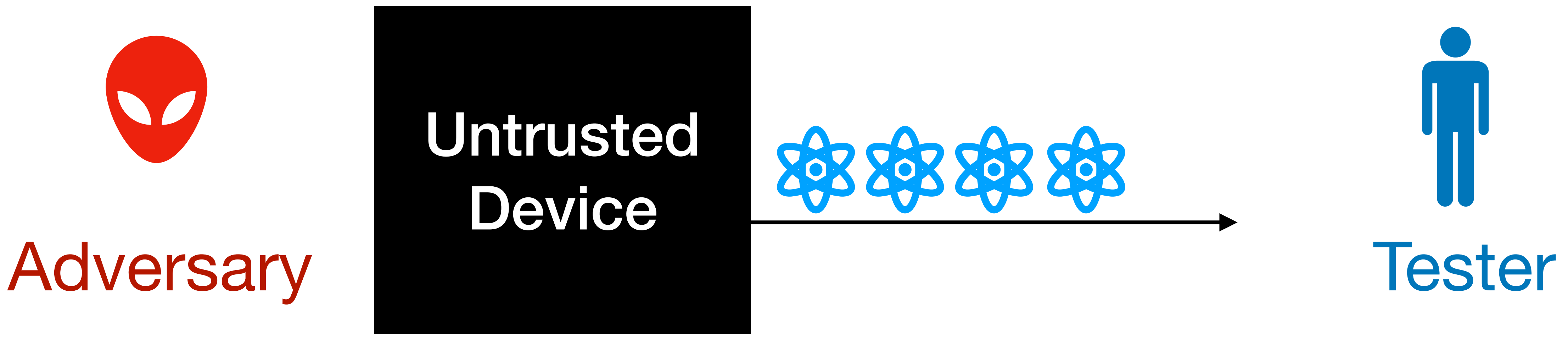
Make a guess

Application 2: adversarial quantum channel discrimination

Operational setting:

A tester is working with an **untrusted** quantum device that generates a quantum state upon request

Guarantee: either $\mathscr{N}$ (the bad case) or $\mathscr{M}$ (the good case)



Request samples
Perform measurement
Make a guess

Environmental system of the channel

Internal memory correlates with the generated samples

Actively misleading the tester to correctly identify the channel

How effectively can the tester distinguish between the two cases while playing against the adversary?

Classical setting refers to [Brandão, Harrow, Lee, Peres, 2020, TIT]

Application 2: adversarial quantum channel discrimination

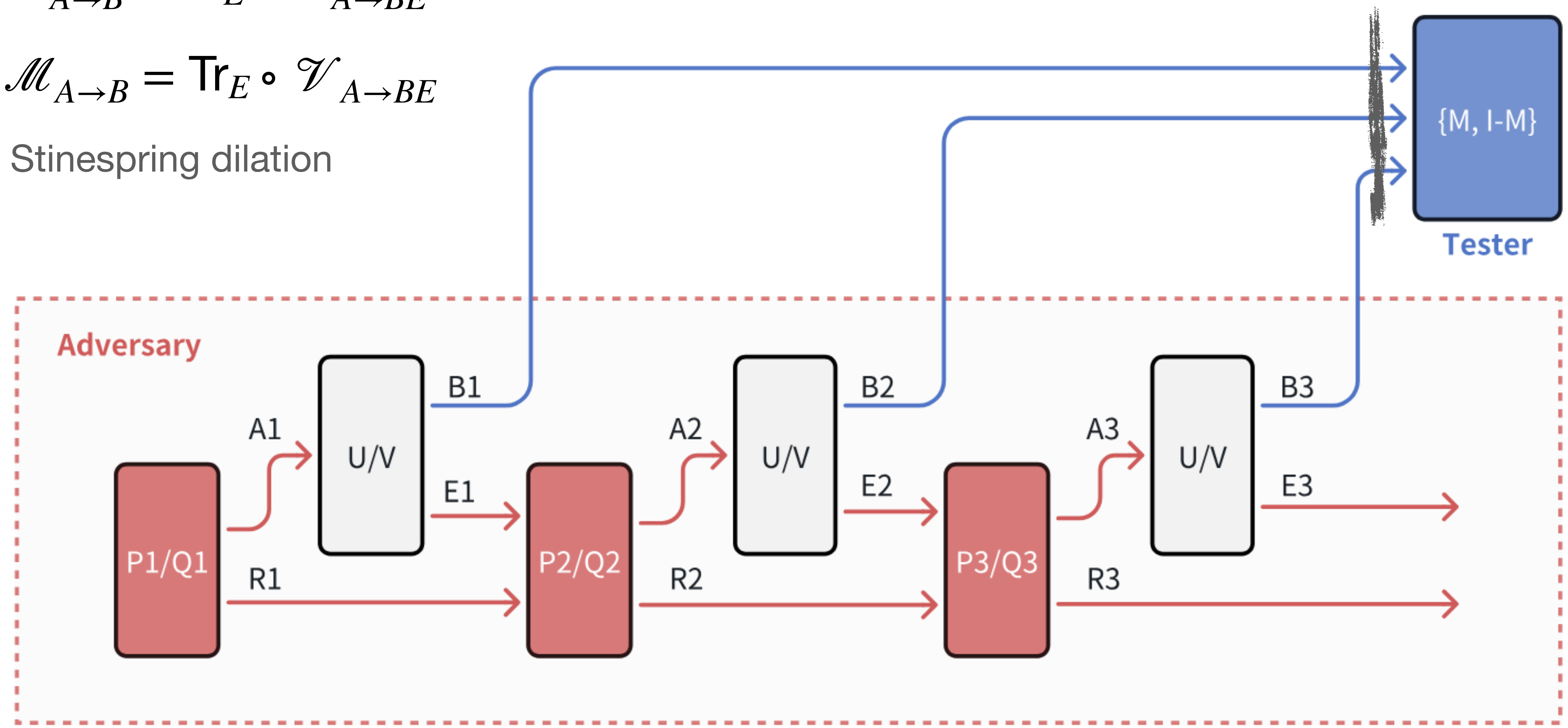
Operational setting:

A tester is working with an **untrusted** quantum device that generates a quantum state upon request

$\mathcal{N}_{A\to B} = \mathrm{Tr}_E \circ \mathcal{U}_{A\to BE}$

$\mathcal{M}_{A\to B} = \mathrm{Tr}_E \circ \mathcal{V}_{A\to BE}$

Stinespring dilation



E_i environmental systems, R_i internal memories, P_i/Q_i internal operations by adversary

Due to the lack of knowledge of what the adversary do:

- $\mathcal{A}_n$ if device is $\mathcal{N}$;
- $\mathcal{B}_n$ if device is $\mathcal{M}$

Adaptive strategies by adversary

Application 2: adversarial quantum channel discrimination

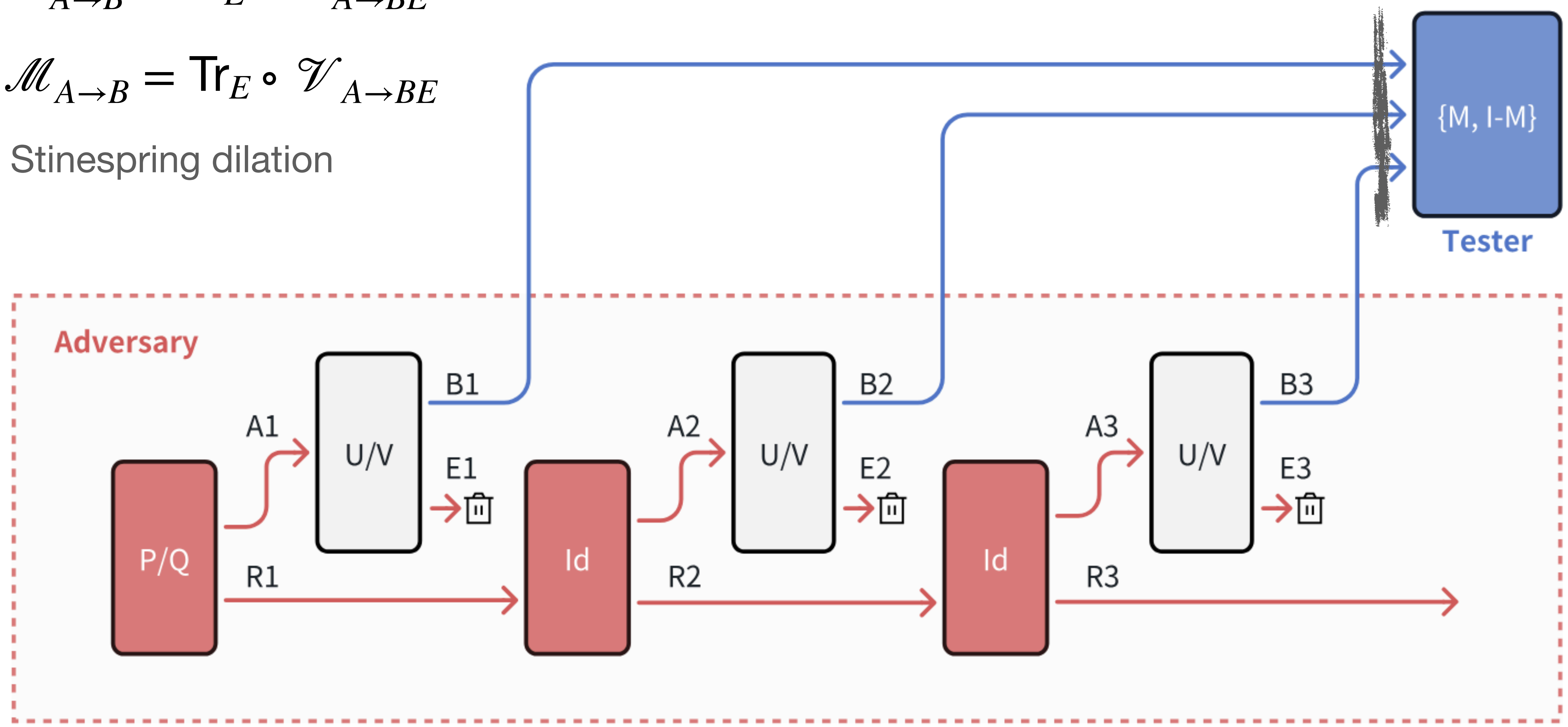
Operational setting:

A tester is working with an **untrusted** quantum device that generates a quantum state upon request

$\mathscr{N}_{A\to B} = \mathrm{Tr}_E \circ \mathscr{U}_{A\to BE}$

$\mathscr{M}_{A\to B} = \mathrm{Tr}_E \circ \mathscr{V}_{A\to BE}$

Stinespring dilation



E_i environmental systems, R_i internal memories, P_i/Q_i internal operations by adversary

Due to the lack of knowledge of what the adversary do:

- $\mathscr{A}'_n$ if device is $\mathscr{N}$;
- $\mathscr{B}'_n$ if device is $\mathscr{M}$

Non-adaptive strategies by adversary

Application 2: adversarial quantum channel discrimination

The best performance of the tester playing against the adversary is given by:

Our answer

$$\lim_{n\to\infty} -\frac{1}{n}\log \beta_\varepsilon(\mathscr{A}_n\|\mathscr{B}_n) = \lim_{n\to\infty} -\frac{1}{n}\log \beta_\varepsilon(\mathscr{A}'_n\|\mathscr{B}'_n) = D^{\inf,\infty}(\mathscr{N}\|\mathscr{M})$$

Adaptive strategies by adversary

Non-adaptive strategies by adversary

Minimum output quantum channel divergence

$$D^{\inf}(\mathscr{N}\|\mathscr{M}) := \inf_{\rho,\sigma\in\mathscr{D}} D(\mathscr{N}(\rho)\|\mathscr{M}(\sigma)) \qquad D^{\inf,\infty}(\mathscr{N}\|\mathscr{M}) := \lim_{n\to\infty}\frac{1}{n}D^{\inf}(\mathscr{N}^{\otimes n}\|\mathscr{M}^{\otimes n})$$

Adaptive strategies offer **no advantage** over non-adaptive ones in adversarial quantum channel discrimination.

Good news for the tester!

Application 2: adversarial quantum channel discrimination

The best performance of the tester playing against the adversary is given by:

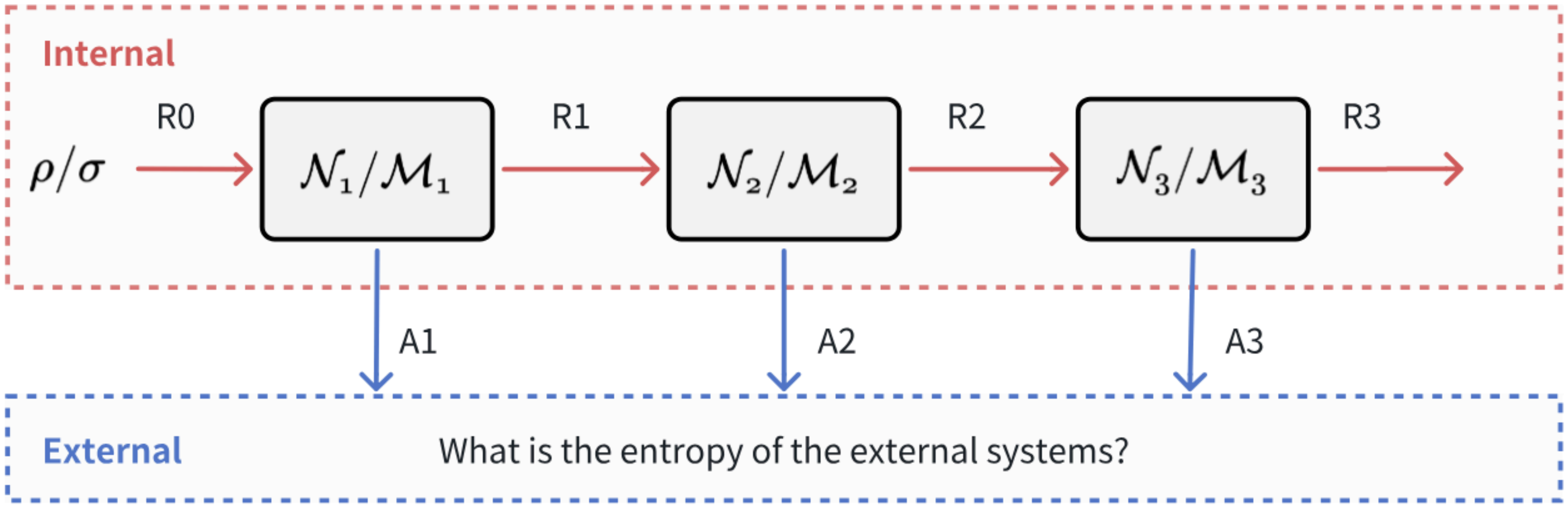
$$\boxed{\lim_{n\to\infty} -\frac{1}{n}\log \beta_\varepsilon(\mathscr{A}_n\|\mathscr{B}_n) = \lim_{n\to\infty} -\frac{1}{n}\log \beta_\varepsilon(\mathscr{A}'_n\|\mathscr{B}'_n) = D^{\inf,\infty}(\mathscr{N}\|\mathscr{M})}$$

Key technical tool (chain rule):

$$D_{M,\alpha}(\mathscr{N}_{A\to B}(\rho_{RA})\|\mathscr{M}_{A\to B}(\sigma_{RA})) \geq D_{M,\alpha}(\rho_R\|\sigma_R) + D^{\inf}_{M,\alpha}(\mathscr{N}_{A\to B}\|\mathscr{M}_{A\to B})$$

$$D_{S,\alpha}(\mathscr{N}_{A\to B}(\rho_{RA})\|\mathscr{M}_{A\to B}(\sigma_{RA})) \geq D_{S,\alpha}(\rho_R\|\sigma_R) + D^{\inf,\infty}_{S,\alpha}(\mathscr{N}_{A\to B}\|\mathscr{M}_{A\to B})$$

Application 3: a relative entropy accumulation theorem



How entropy accumulate for sequential operations on a state?

[Dupuis, Fawzi, Renner, 2020, CMP] Find plenty of applications in quantum cryptography

$$H^{\varepsilon}_{\max}(B_1 \ldots B_n | C_1 \ldots C_n)_{\mathcal{N}_n \circ \cdots \circ \mathcal{N}_1(\rho_{R_0})} \leq \sum_{i=1}^{n} \sup_{\omega_{R_{i-1}}} H(B_i | C_i)_{\mathcal{N}_i(\omega)} + O(\sqrt{n})$$

How to generalize from conditional entropy to relative entropy?

Open question in [Metger, Fawzi, Sutter, Renner, 2022, FOCS] for $D_{\max,\varepsilon}$

Application 3: a relative entropy accumulation theorem

How entropy accumulate for sequential operations on a state?

[Dupuis, Fawzi, Renner, 2020, CMP] Find plenty of applications in quantum cryptography

$$H^{\varepsilon}_{\max}(B_1 \ldots B_n | C_1 \ldots C_n)_{\mathcal{N}_n \circ \cdots \circ \mathcal{N}_1(\rho_{R_0})} \leq \sum_{i=1}^{n} \sup_{\omega_{R_{i-1}}} H(B_i | C_i)_{\mathcal{N}_i(\omega)} + O(\sqrt{n})$$

How to generalize from conditional entropy to relative entropy?

Open question in [Metger, Fawzi, Sutter, Renner, 2022, FOCS] for $D_{\max,\varepsilon}$

Recover with a slightly weaker second order

Our answer

$$D_{H,\varepsilon}\left(\mathrm{Tr}_{R_n} \circ \prod_{i=1}^{n} \mathcal{N}_i(\rho_{R_0}) \middle\| \mathrm{Tr}_{R_n} \circ \prod_{i=1}^{n} \mathcal{M}_i(\sigma_{R_0})\right) \geq \sum_{i=1}^{n} D^{\inf,\infty}(\mathrm{Tr}_{R_i} \circ \mathcal{N}_i \| \mathrm{Tr}_{R_i} \circ \mathcal{M}_i) - O(n^{2/3} \log n)$$

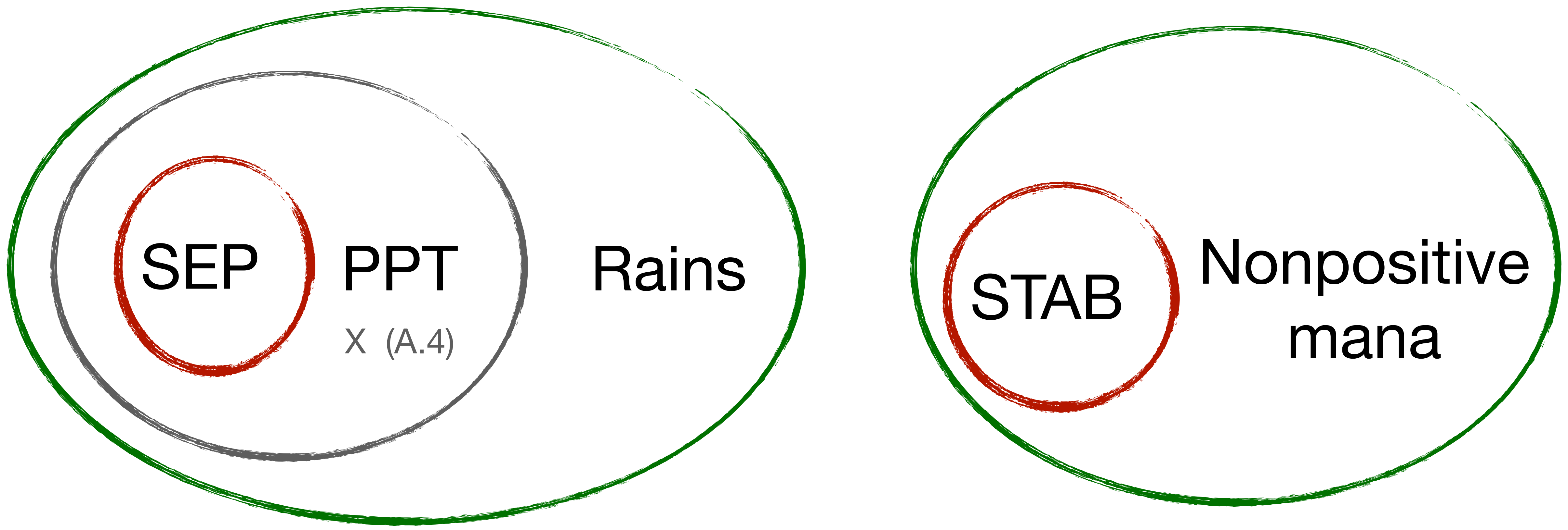
Application 4: efficient bounds for quantum resource theory

(A.1) Each $\mathscr{A}_n$ is convex and compact;

(A.2) Each $\mathscr{A}_n$ is permutation-invariant;

(A.3) $\mathscr{A}_m \otimes \mathscr{A}_k \subseteq \mathscr{A}_{m+k}$, for all $m, k \in \mathbb{N}$;

(A.4) $(\mathscr{A}_m)^\circ_+ \otimes (\mathscr{A}_k)^\circ_+ \subseteq (\mathscr{A}_{m+k})^\circ_+$, for all $m, k \in \mathbb{N}$;



If (A.4) is not directly satisfied, we do relaxation!!!

$$D^\infty(\rho_{AB} \| \text{SEP}) \geq D^\infty(\rho_{AB} \| \text{Rains})$$

Note that $D^\infty(\mathscr{A} \| \mathscr{B}) := \lim_{n\to\infty} \frac{1}{n} D(\mathscr{A}_n \| \mathscr{B}_n)$ is efficiently computable

Improvement (even for the first level of approximation)

- Entanglement cost of quantum states and channels
- Entanglement distillation
- Magic state distillation

Refer to arXiv: 2502.15659 for more details

Summary

Generalized quantum AEP

$$\lim_{n\to\infty} \frac{1}{n} \mathbb{D}_\varepsilon(\mathscr{A}_n \| \mathscr{B}_n) = D^\infty(\mathscr{A} \| \mathscr{B})$$

Generality/efficiency/finite n estimate

(A.1) Each $\mathscr{A}_n$ is convex and compact;

(A.2) Each $\mathscr{A}_n$ is permutation-invariant;

(A.3) $\mathscr{A}_m \otimes \mathscr{A}_k \subseteq \mathscr{A}_{m+k}$, for all $m, k \in \mathbb{N}$;

(A.4) $(\mathscr{A}_m)^\circ_+ \otimes (\mathscr{A}_k)^\circ_+ \subseteq (\mathscr{A}_{m+k})^\circ_+$, for all $m, k \in \mathbb{N}$;

Technical tools (superadditivity & chain rule):

$$D_{M,\alpha}(\mathscr{A}_{12} \| \mathscr{B}_{12}) \geq D_{M,\alpha}(\mathscr{A}_1 \| \mathscr{B}_1) + D_{M,\alpha}(\mathscr{A}_2 \| \mathscr{B}_2)$$

$$D_{M,\alpha}(\mathscr{N}_{A\to B}(\rho_{RA}) \| \mathscr{M}_{A\to B}(\sigma_{RA})) \geq D_{M,\alpha}(\rho_R \| \sigma_R) + D^{\inf}_{M,\alpha}(\mathscr{N}_{A\to B} \| \mathscr{M}_{A\to B})$$

As AEP is in the heart of information theory, we expect further studies and applications.

Already been used in [2502.02563] by Arqand and Tan for quantum cryptography

I am hiring

One Brand, Two Campuses

香港中文大學
The Chinese University of Hong Kong

香港中文大學(深圳)
The Chinese University of Hong Kong, Shenzhen

Looking for postdocs, PhDs, research assistants…

Quantum Information Theory, Quantum Computation

kunfang.info　　✉ kunfang@cuhk.edu.cn

Thanks for your attention!

arXiv: 2411.04035 & 2502.15659