Efficient Quantum Measurements: Computational Max- and Measured Rényi Divergences and Applications

Quantum Resource Theories 2026 - Tokyo

Álvaro Yángüez, Thomas A. Hahn, **Jan Kochanowski***

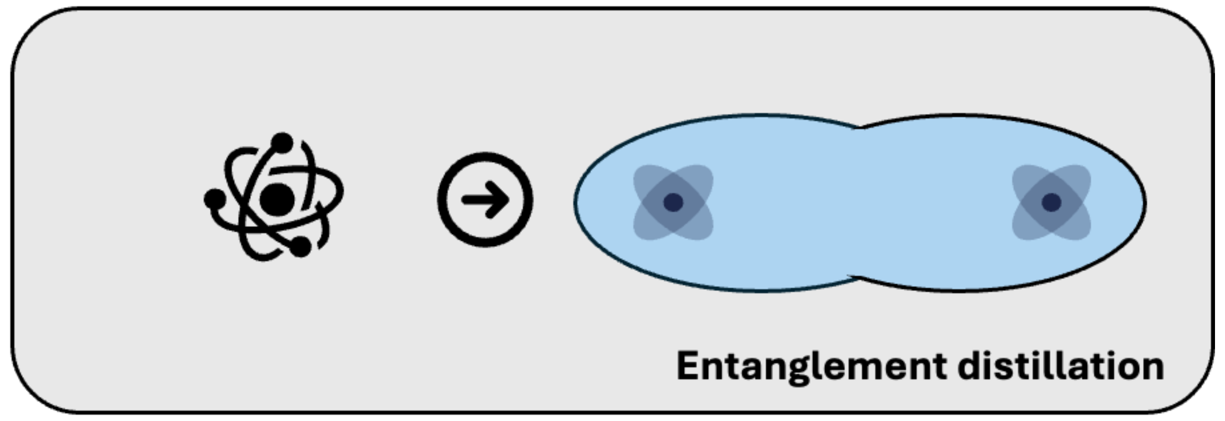
*Institut Polytechnique de Paris; Inria

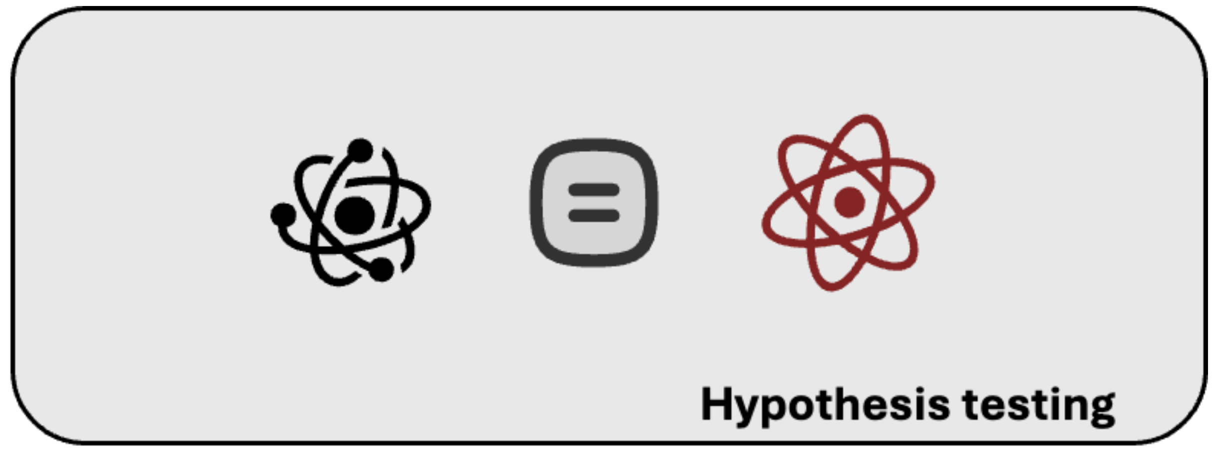
arXiv:2509.21308

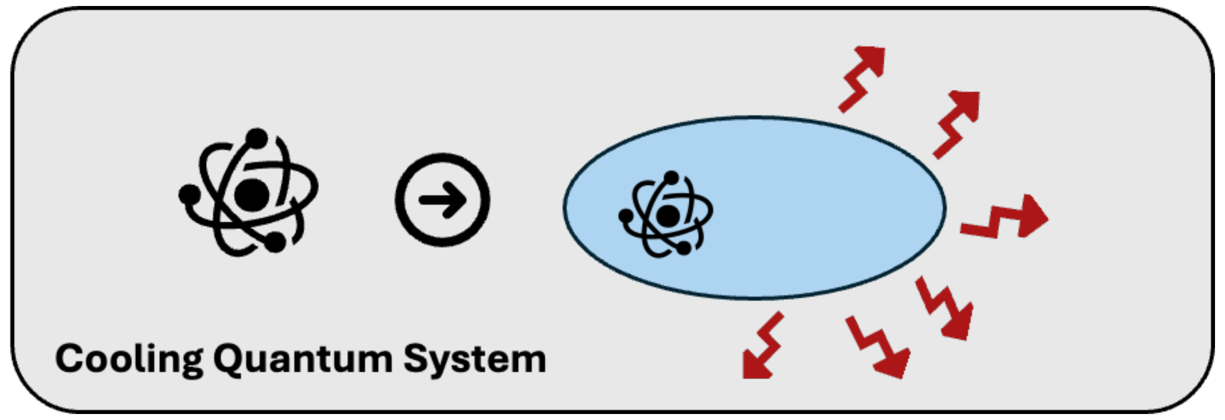
Q. divergences are central to quantum info. theory

- „divergence“ = standard ‚distance’ measures in QI
  - Satisfy: Data-processing, positivity,…
- Resource theories
  - Quantifying amounts, distillation rates
- Hypothesis testing
  - Steins Lemma: Optimal decay of type II error
- Channel Coding and Cryptography
  - Security, Randomness, Channel capacities,
- Q. Thermodynamics

$$\mathbb{D}(\rho\|\sigma)$$





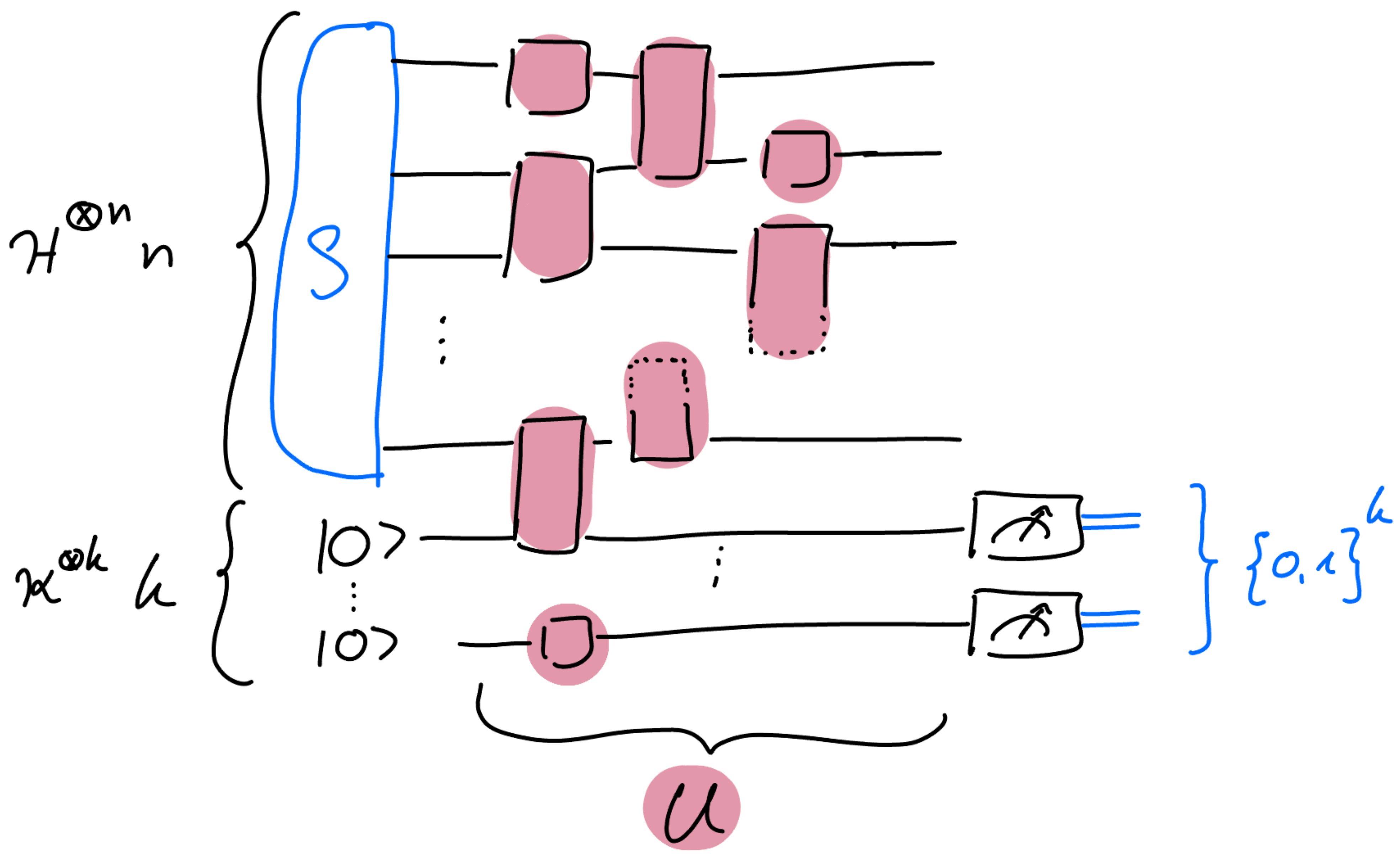


Real experiments are complexity constrained

- Practical constraints:
  - Polynomial gate complexity and fixed gate set
  - Number of ancillary qubits k
  - Classical pre- & post-processing

$\Rightarrow$ State and measurement preparation

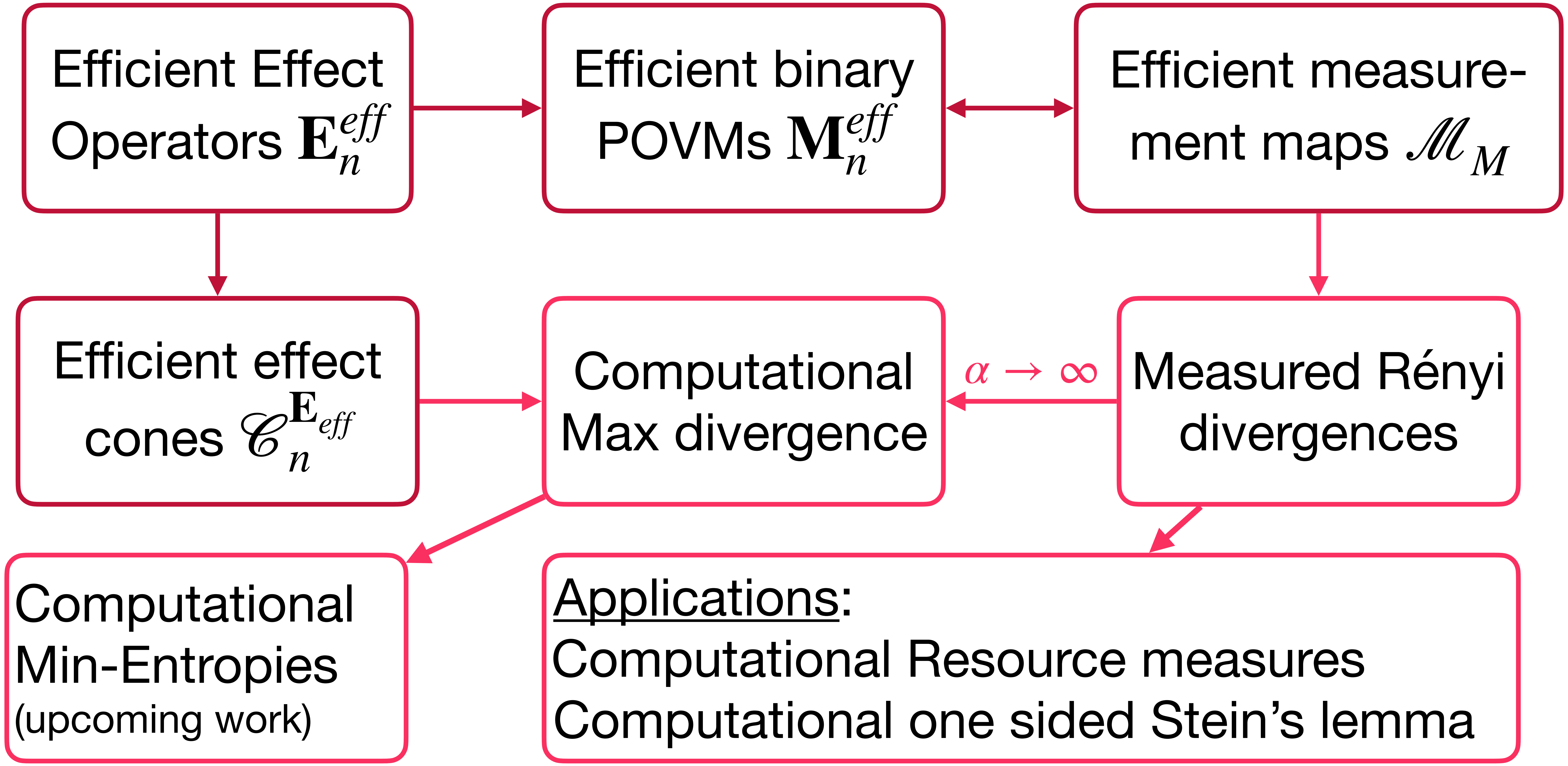
$\Rightarrow$ Resource manipulation



- Example: binary hypothesis testing
  - $H_0 : \rho^{\otimes n}$ vs. $H_1 : \sigma^{\otimes n}$
  - Optimal $\mathbb{M} = \{E, \mathbb{I} - E\}$: $E = [\rho^{\otimes n} - \sigma^{\otimes n}]_+$ (i.g. not efficient to implement)

Q. Divergences are not complexity constrained

- Operational importance of divergences neglects practical feasibility
- How to define useful complexity constrained divergences?
- Strategy:



Efficient quantum measurements

- Require divergencies that capture practical complexity constraints
- Binary POVM: $M = \{E_1, E_2 = \mathbb{I} - E_1\}$,
  - $E_i = \mathscr{M}^*_M(|i\rangle\langle i|)$ for CPU map $\mathscr{M}^*_M : B(\mathbb{C}^2) \mapsto B(\mathscr{H}_n)$, dual of

$$\mathscr{M}_M : \rho \to \sum_{i=0}^{1} \mathrm{Tr}[E_i\rho]\,|i\rangle\langle i|$$

- <u>Def:</u> [Efficient measurements, informally]: Fix gate set $\mathscr{G}$ and polynomial p
  - Efficient family of POVMs $\{M_n\}_{n\in\mathbb{N}}$ if gate complexity $C(\mathscr{M}_{M_n}) \leq p(n)$.
  - Efficient family of effect operators $\{\mathbf{E}_n^{eff}\}_{n\in\mathbb{N}}$:

$$\mathbf{E}_n^{eff} \subset \{E \in \mathrm{Pos}(\mathscr{H}^{\otimes n})\,|\,0 \leq E \leq \mathbb{I}\}$$

s.t. E or $\mathbb{I} - E$ can be implemented using at most $p(n)$ gates from $\mathscr{G}$.

Efficient quantum measurements

- Fix gate set $\mathscr{G}$ and polynomial p
  - Efficient family of POVMs $\{M_n\}_{n\in\mathbb{N}}$ if gate complexity $C(\mathscr{M}_{M_n}) \leq p(n)$.
  - Efficient family of effect operators $\{\mathbf{E}_n^{eff}\}_{n\in\mathbb{N}}$:

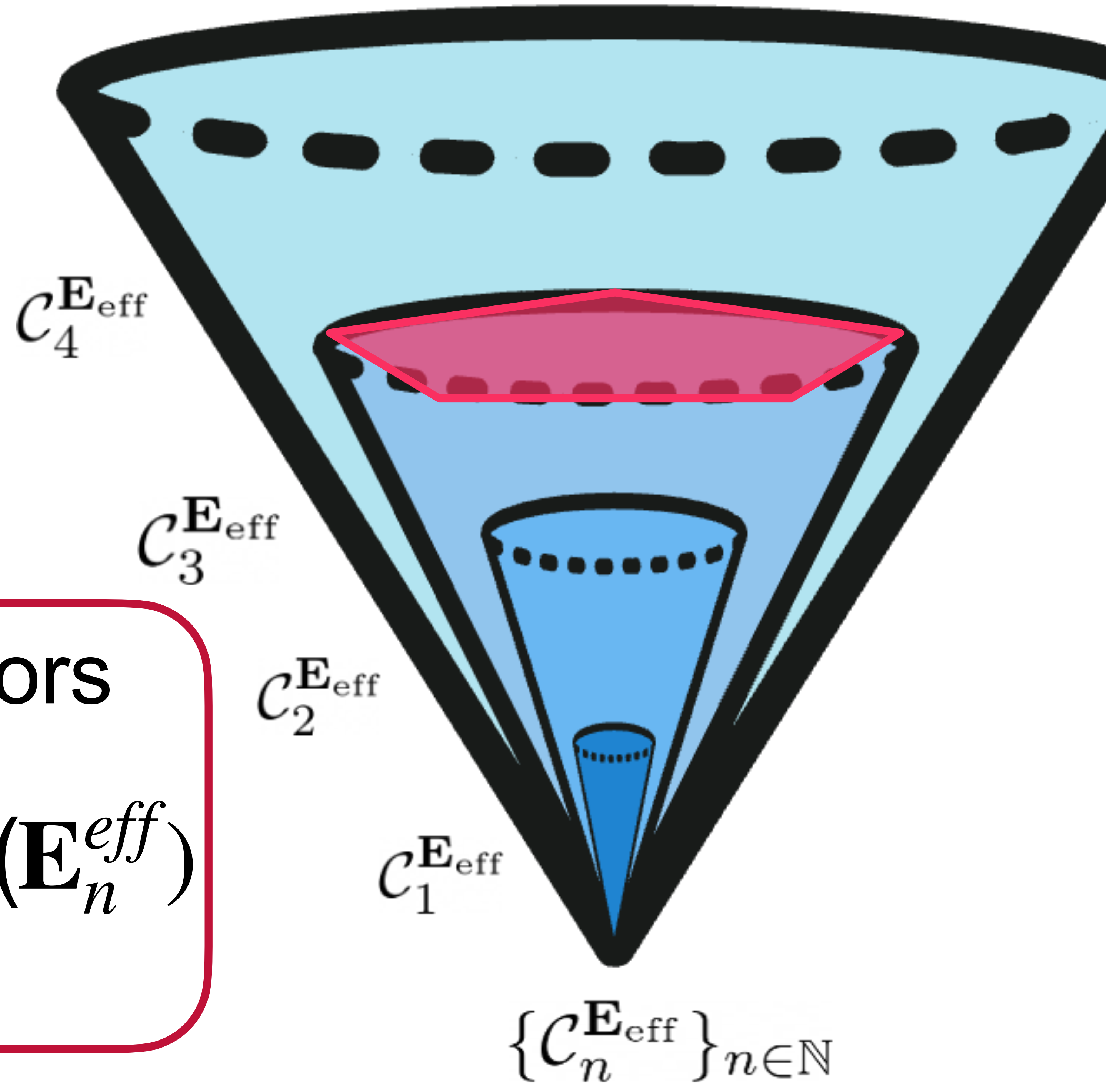
$$\mathbf{E}_n^{eff} \subset \{E \in \mathrm{Pos}(\mathscr{H}^{\otimes n}) \,|\, 0 \leq E \leq \mathbb{I}\}$$

s.t. E or $\mathbb{I} - E$ can be implemented using at most $p(n)$ gates from $\mathscr{G}$.

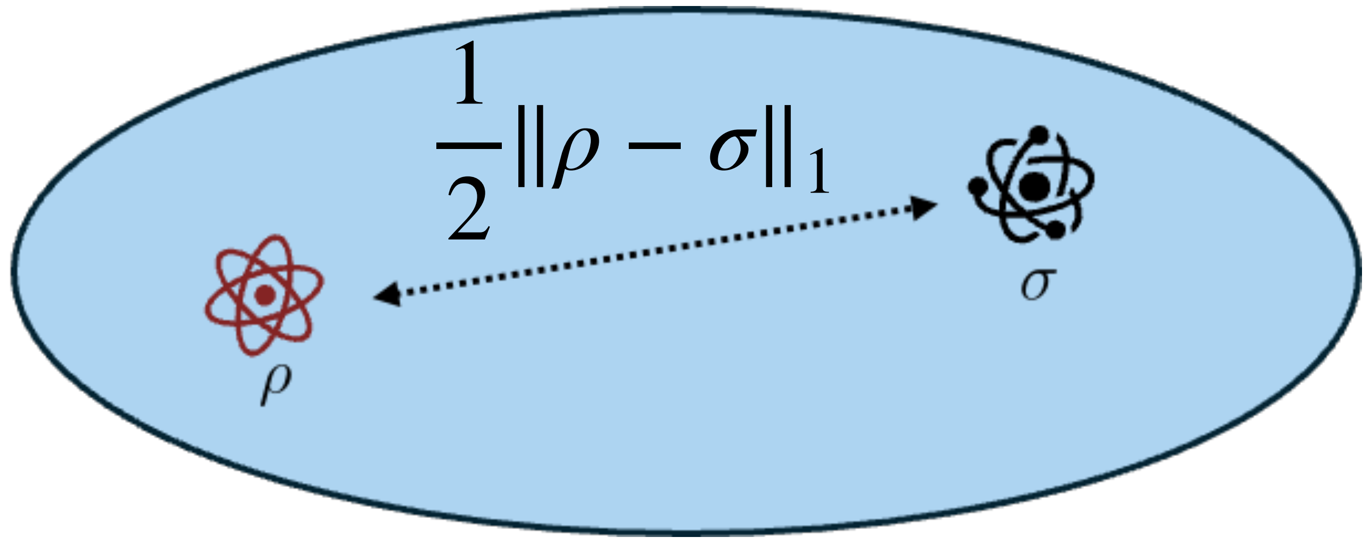
- Def: Family of proper cones of efficient effect operators

$\{\mathscr{C}_n^{\mathbf{E}_{eff}}\}_{n\in\mathbb{N}}$

$$\mathscr{C}_n^{\mathbf{E}_{eff}} := \mathrm{cone}(\mathbf{E}_n^{eff}) = \bigcup_{\lambda\geq 0} \lambda \mathrm{conv}(\mathbf{E}_n^{eff})$$



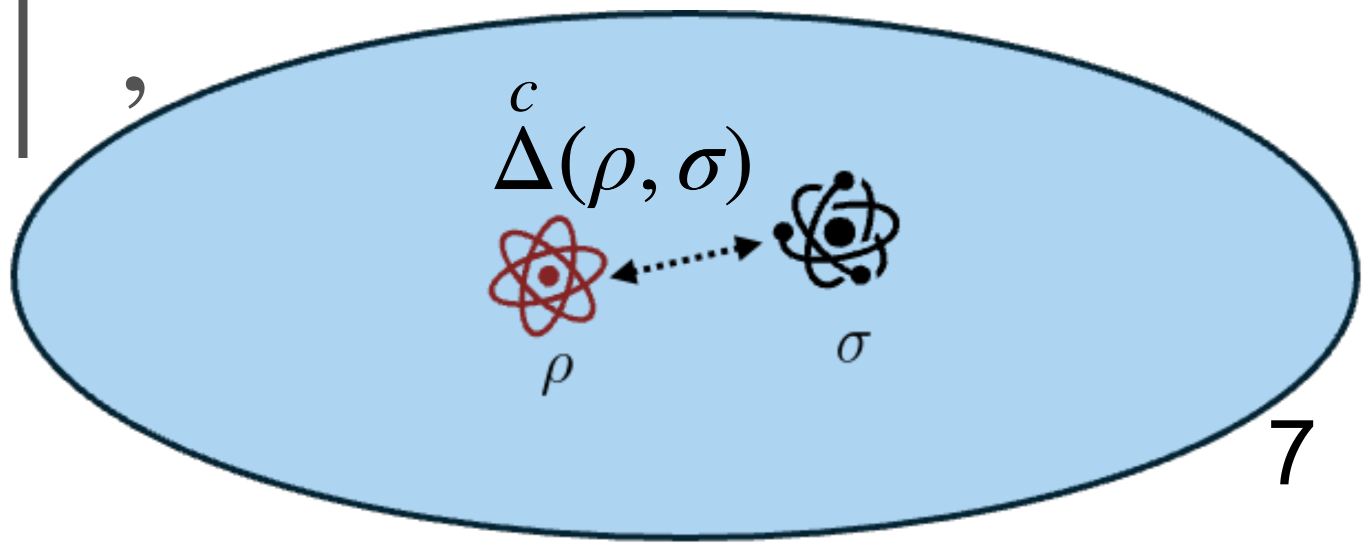
A simple computational trace distance



- Trace distance as optimal one-shot distinguishability
- Given poly-generated set of efficient effect operators $\{\overline{\mathbf{E}}_n^{eff}\}_{n\in\mathbb{N}}$, (or equivalently efficient binary POVMs $\{\overline{\mathbf{M}}_n^{eff}\}_{n\in\mathbb{N}}$) define

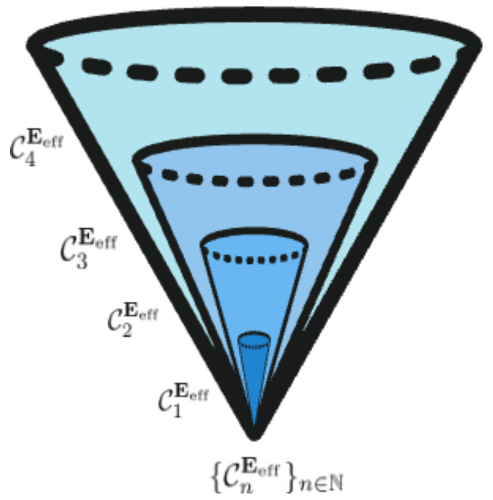
$$\overset{c}{\Delta}(\rho,\sigma) := \frac{1}{2}\|\rho-\sigma\|_{\{\overline{\mathbf{M}}_n^{eff}\}} = \frac{1}{2}\max_{M\in\mathbf{M}_n^{eff}} \|\mathscr{M}_M(\rho)-\mathscr{M}_M(\sigma)\|_1.$$

$$= \frac{1}{2}\begin{cases} 2\max_{E\in\mathbf{E}_n^{eff}} \mathrm{Tr}\left[E\left(\rho-\sigma\right)\right], \\ \max_{M=(E_1,E_2)\in\mathbf{M}_n^{eff}} \sum_{i=1}^{2}\left|\mathrm{Tr}[E_i(\rho-\sigma)]\right|, \\ \max_{M\in\mathbf{M}_n^{eff}} \|\mathscr{M}_M(\rho)-\mathscr{M}_M(\sigma)\|_1. \end{cases}$$



Computational Max-divergence

$\{\mathscr{C}_n^{\mathbf{E}_{eff}}\}_{n\in\mathbb{N}}$



- Max-divergence [Datta'09]: $D_{\max}(\rho\|\sigma) := \log\inf\{\lambda\in\mathbb{R}\,|\,\rho\leq\lambda\sigma\}$
- Naturally defined via cones:

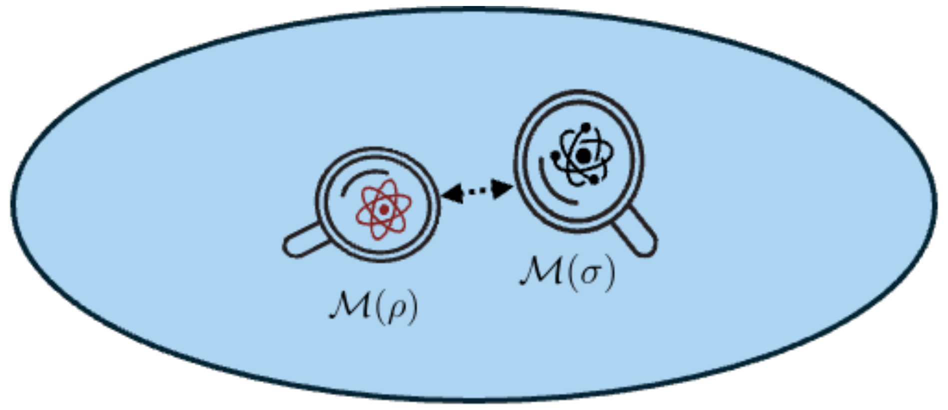
$$\rho \leq_{\mathscr{C}*} \lambda\sigma \Leftrightarrow \lambda\sigma-\rho\in\mathscr{C}^* \Leftrightarrow \forall E\in\mathscr{C}:\quad \mathrm{Tr}[E(\lambda\sigma-\rho)]\geq 0$$

  - E.g. POS, PPT, SEP, LO [RKW'11, RSB'24, J'12, GC'24]
- Def: Computational Max-divergence

$$\overset{c}{D}_{\max}(\rho\|\sigma) := \log\inf\{\lambda\in\mathbb{R}\,|\,\rho\leq_{\mathscr{C}_n^{\mathscr{S}_{eff}}}\lambda\sigma\} = \log\sup_{\nu\in\mathscr{C}_n^{\mathbf{E}_{eff}}}\frac{\mathrm{Tr}[\nu\rho]}{\mathrm{Tr}[\nu\sigma]}$$

- Upcoming work:
  - Naturally give rise to meaningful computational min entropies c.f. [AA'66,AHRH'25, KRS'09]
  - Maximal separation between computational and informational min-entropy

Computational measured Rényi-divergences



$\{\overline{\mathbf{M}}_n^{eff}\}_{n\in\mathbb{N}}$

- Sandwiched Rényi divergences: $D_\alpha(\rho\|\sigma) := \frac{\alpha}{\alpha-1}\log\|\sigma^{\frac{1-\alpha}{\alpha}}\rho\sigma^{\frac{1-\alpha}{\alpha}}\|_\alpha$

$-\log F(\rho\|\sigma)$ $\quad D(\rho\|\sigma) = \mathrm{Tr}[\rho(\log\rho - \log\sigma)]$ $\quad D_{\max}(\rho\|\sigma)$

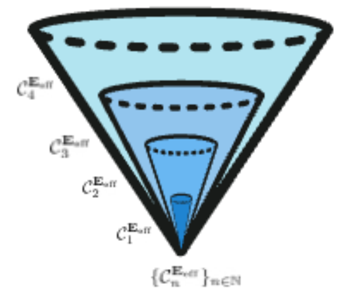
α: 0 — $1/2$ — 1 — ∞

- Def: Computational (measured) Rényi-divergences

$$\overset{c\,\overline{\mathbf{M}}_n^{eff}}{D_\alpha}(\rho\|\sigma) := \sup_{M\in\mathbf{M}_n^{eff}} D_\alpha(\mathscr{M}_M(\rho)\|\mathscr{M}_M(\sigma))$$

- Comp. Rel Entropy: $\overset{c\,\overline{\mathbf{M}}_n^{eff}}{D}(\rho\|\sigma) := \lim_{\alpha\to1}\overset{c\,\overline{\mathbf{M}}_n^{eff}}{D_\alpha}(\rho\|\sigma)$

- Theorem 4.12: Comp. Max-divergence: $\lim_{\alpha\to\infty}\overset{c\,\overline{\mathbf{M}}_n^{eff}}{D_\alpha}(\rho\|\sigma) = \overset{c}{D}_{\max}(\rho\|\sigma)$



Properties of Comp. Rényi divergences

$$\overset{c\,\mathbf{M}_n^{eff}}{D_\alpha}(\rho\|\sigma) := \sup_{M\in\mathbf{M}_n^{eff}} D_\alpha(\mathscr{M}_M(\rho)\|\mathscr{M}_M(\sigma)), \qquad \overset{c}{F}(\rho,\sigma) = \exp(-\overset{c\,\mathbf{M}_n^{eff}}{D_{\frac{1}{2}}}(\rho\|\sigma))$$

- Non-negativity, Joint (quasi)-convexity,
- Monotonicity in α: $\overset{c\,\mathbf{M}_n^{eff}}{D_\alpha}(\rho\|\sigma) \leq \overset{c\,\mathbf{M}_n^{eff}}{D_\beta}(\rho\|\sigma)$ for $\alpha \leq \beta$,
- Data-processing inequality: $\overset{c\,\mathbf{M}_n^{eff}}{D_\alpha}(\Lambda(\rho)\|\Lambda(\sigma)) \leq \overset{c\,\mathbf{M}_n^{eff}}{D_\alpha}(\rho\|\sigma)$ for $\Lambda^*(\mathbf{E}_n^{eff}) \subset \overline{\mathbf{E}}_n^{eff}$.
- Lemma 4.11: Computational Pinsker's Inequality

$$\overset{c\,\mathbf{M}_n^{eff}}{D_\alpha}(\rho\|\sigma) \geq 2\frac{\min\{1,\alpha\}}{\ln 2}\overset{c}{\Delta}(\rho,\sigma)^2$$

- Lemma 4.22: Computational Fuchs-van de Graaf

$$1 - \sqrt{\overset{c}{F}(\rho,\sigma)} \leq \overset{c}{\Delta}(\rho,\sigma) \leq \sqrt{1 - \overset{c}{F}(\rho,\sigma)^2}$$

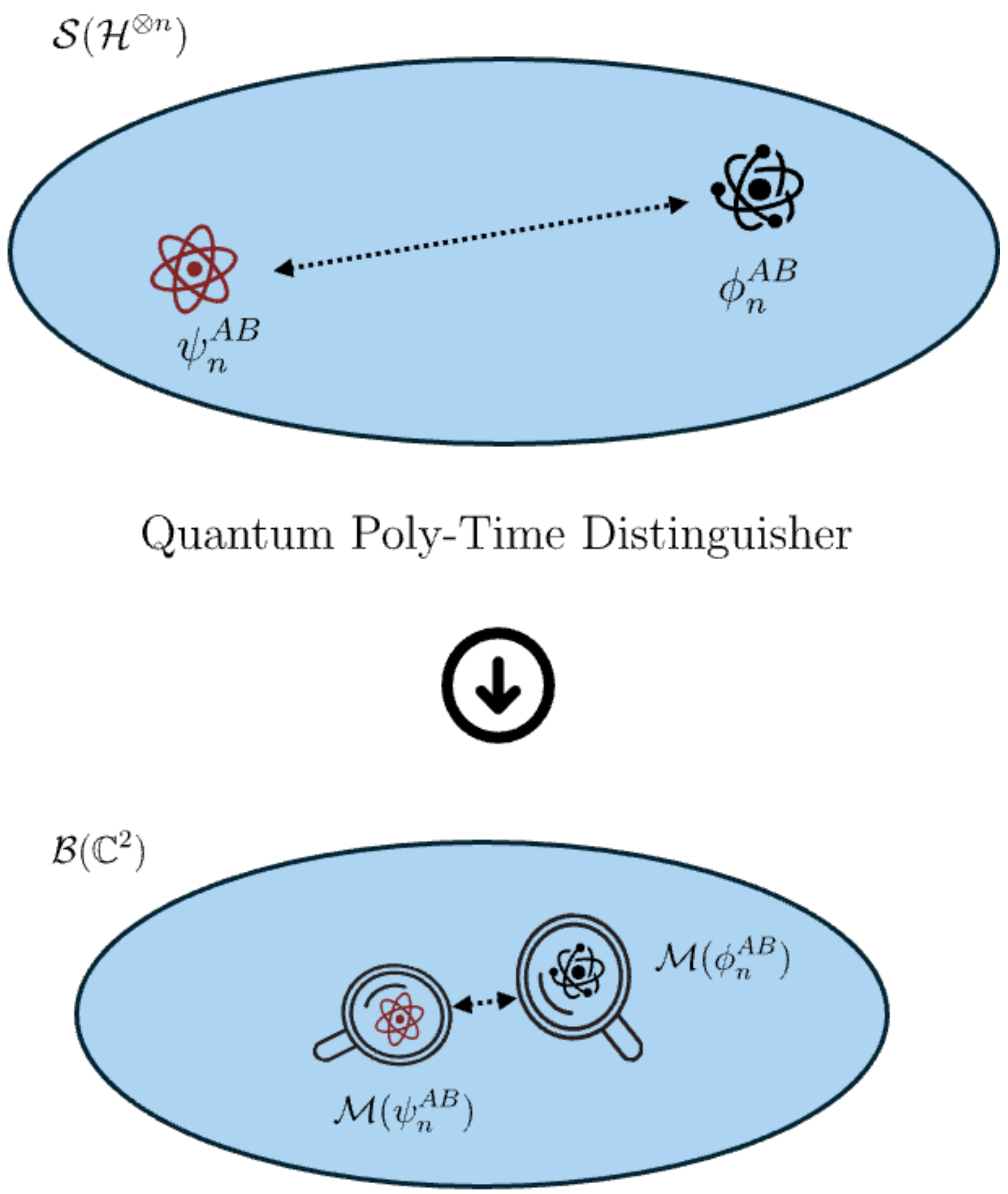
Utility of these complexity restricted divergences

- Pseudo-entangled states provide an explicit separation (assuming existence of EFI pairs [GE'24])

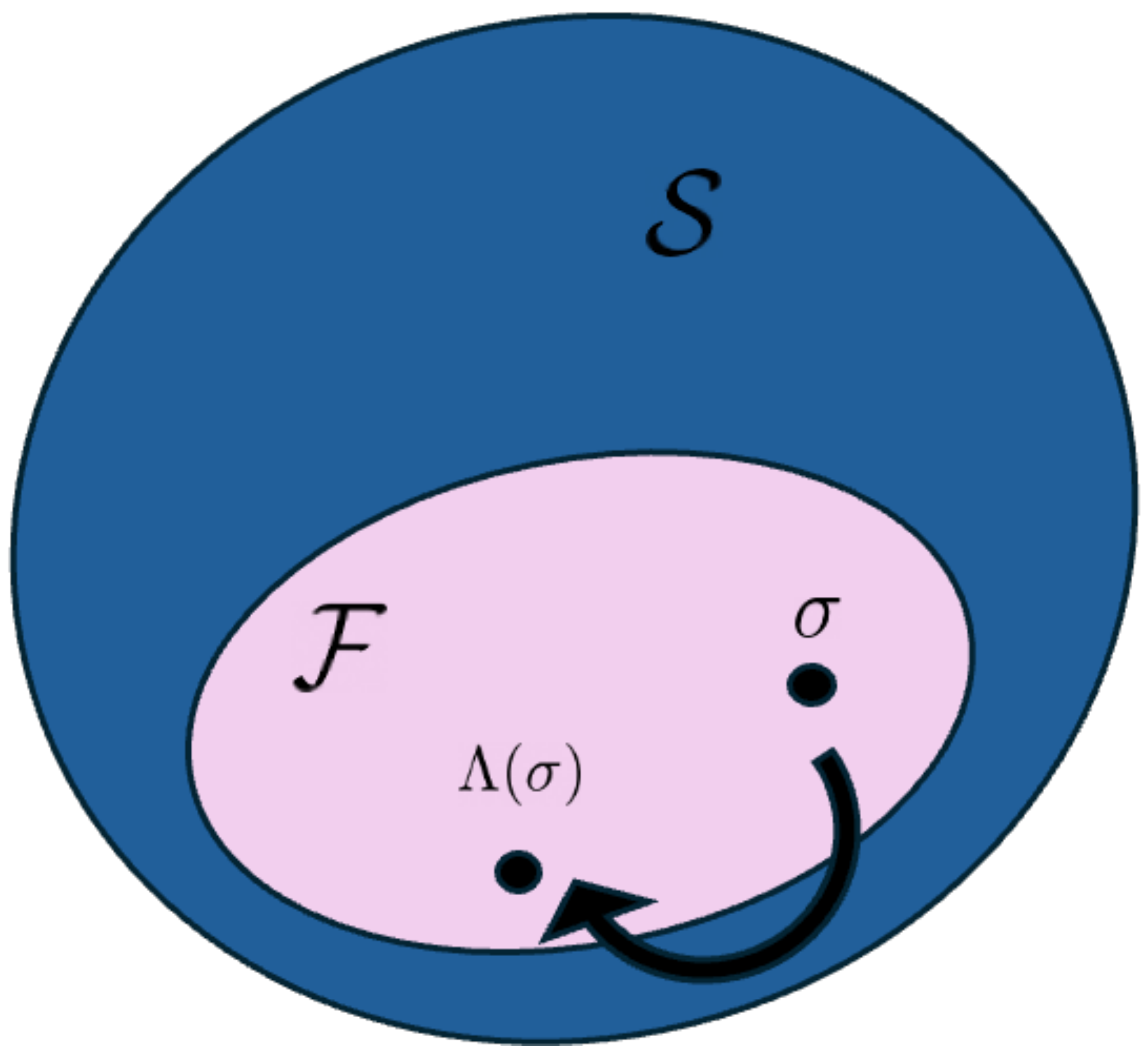
  $\exists\{\psi_n^{AB}\}_{n\in\mathbb{N}}, \{\phi_n^{AB}\}_{n\in\mathbb{N}}$ s.t. $\|\psi_n^{AB}-\phi_n^{AB}\|_1 \simeq 1,$

  but $\overset{c}{\Delta}(\psi_n^{AB}, \phi_n^{AB}) \leq \mathrm{negl}(n)\,.$

- Efficient binary hypothesis testing
  - One-sided computational quantum Stein's lemma
- Resource theories
  - Entanglement cost and distillation



Resource theories



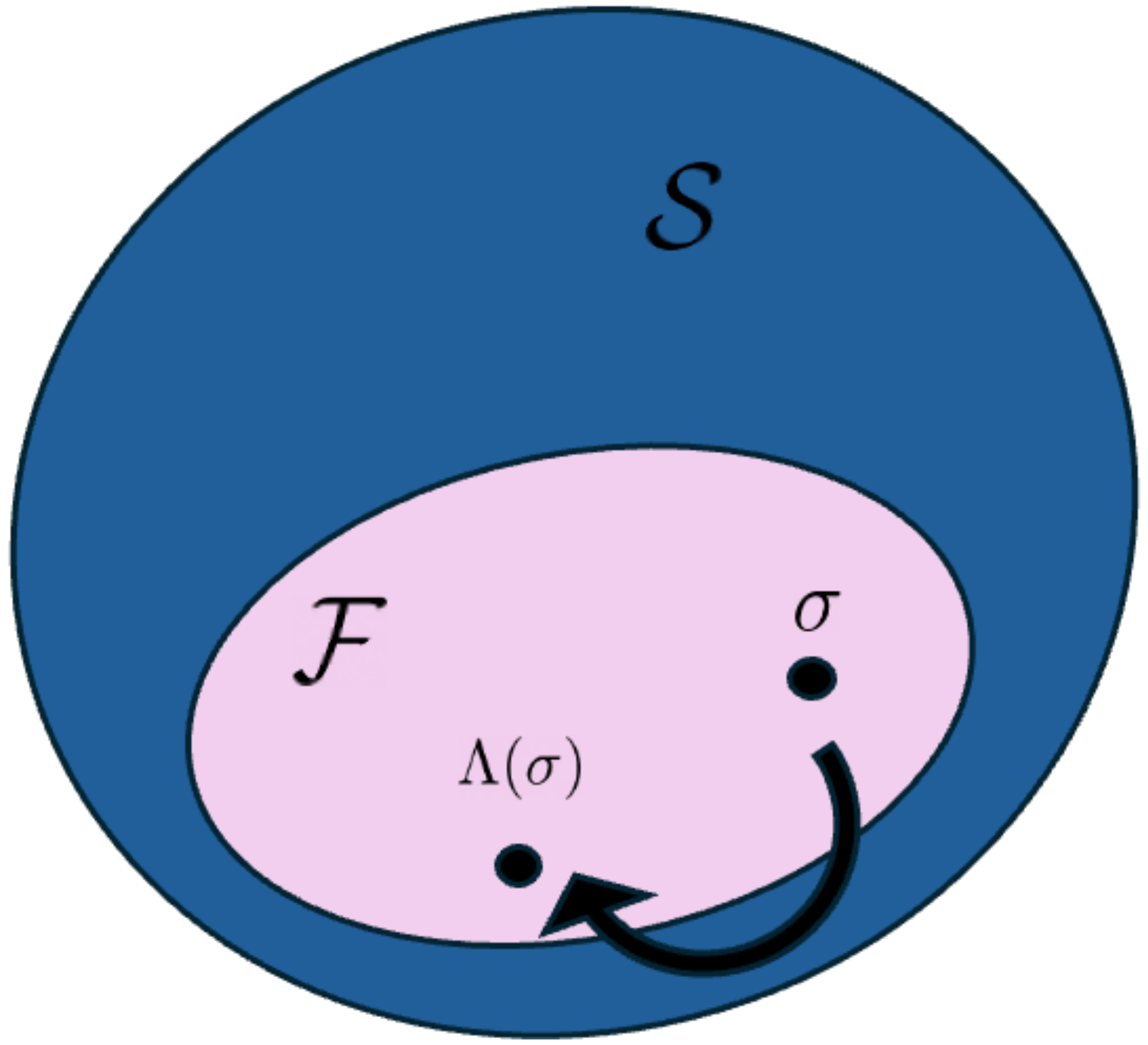
Free operation

- Resource theories: $(\mathscr{F}, \{\Lambda\})$

Resource	Free states $\mathscr{F}$	Free operations Λ
Entanglement	Separable	LOCC maps
Magic	Stabilizer	Clifford operations
Coherence	Incoherent	Incoherent maps
…	…	…

- Resource measure: $R_{rel}(\rho) := \inf_{\sigma \in \mathscr{F}} D(\rho \| \sigma)$ $\quad D(\rho \| \sigma) = \mathrm{Tr}[\rho(\log \rho - \log \sigma)]$

Computational Resource theories



Free efficient operation

- Computational entropy of resource:

$$D_{\mathscr{F}_n}(\rho) := \inf_{\sigma \in \mathscr{F}_n} D^{c\,\mathbf{M}_n^{eff}}(\rho \| \sigma)$$

- Given family of free states: $\{\mathscr{F}_n^1\}_{n\in\mathbb{N}}, \{\mathscr{F}_n^2\}_{n\in\mathbb{N}}$
- Family of free efficient operations:
  - State condition: $\Lambda(\mathscr{F}_n^1) \subset \mathscr{F}_n^2$
  - Test stability: $\Lambda^*(\mathbf{E}_n^{eff,2}) \subset \mathbf{E}_n^{eff,1}$

Resource	Free states	Free efficient operations Λ
Entanglement	Seperable	Efficient LOCC maps
Magic	Stabilizer	Efficient Clifford operations
Coherence	Incoherent	Efficient Incoherent maps
…		…

Computational Resource theories

- Computational entropy of resource:

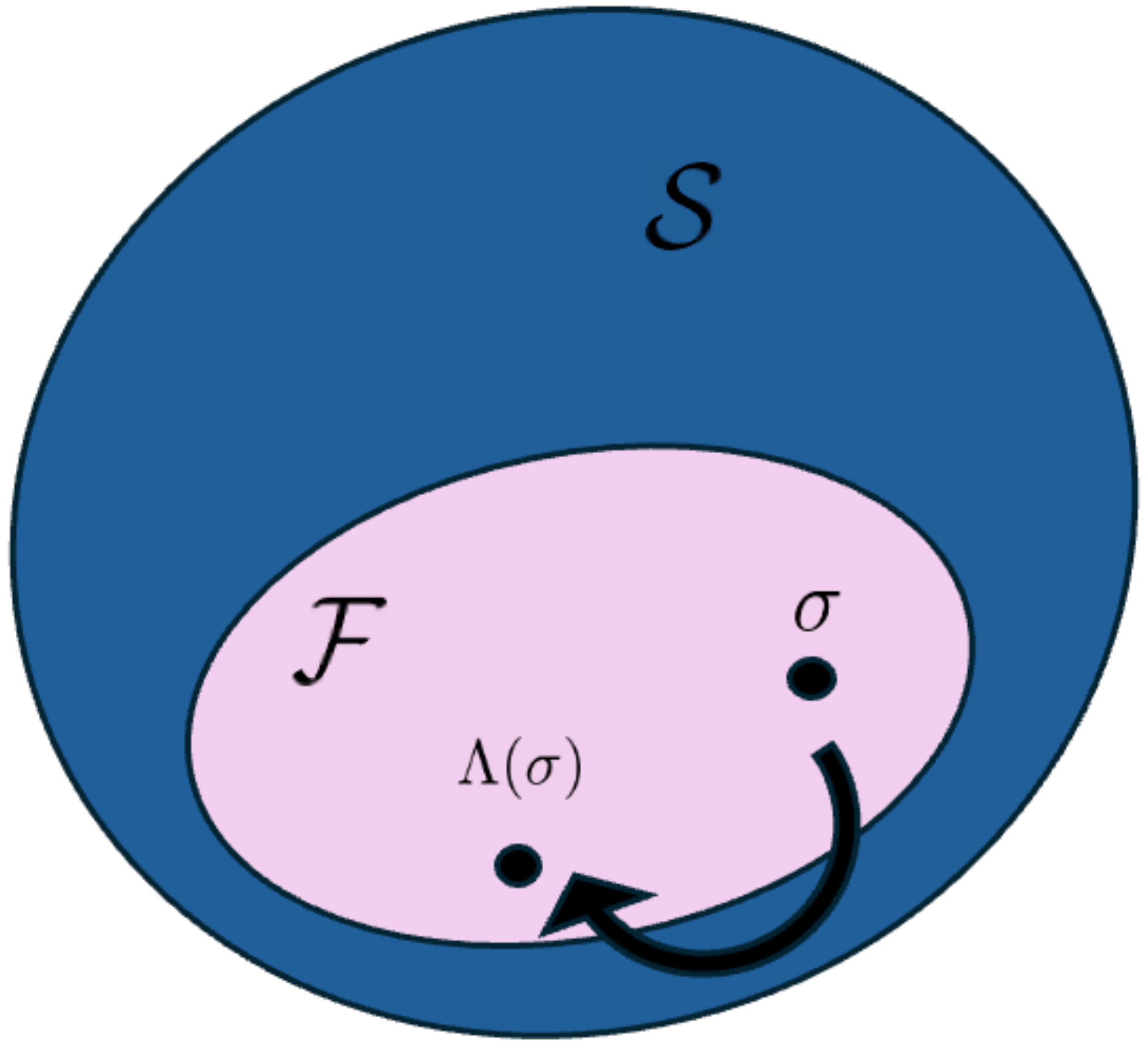
$$D_{\mathcal{F}_n}(\rho) := \inf_{\sigma \in \mathcal{F}_n} \overset{c}{D}^{\mathbf{M}_n^{eff}}(\rho \| \sigma)$$

- Properties:
  - Faithfulness: $D_{\mathcal{F}_n}(\rho) = 0 \iff \rho \in \mathcal{F}_n$,
  - Monotonicity: $D_{\mathcal{F}_n^2}(\Lambda_n(\rho)) \leq D_{\mathcal{F}_n^1}(\rho)$, for free efficient operations Λ_n

- Theorem 5.7: Asymptotic continuity bound: Let $\overset{c}{\Delta}(\rho, \sigma) \leq \epsilon$, then

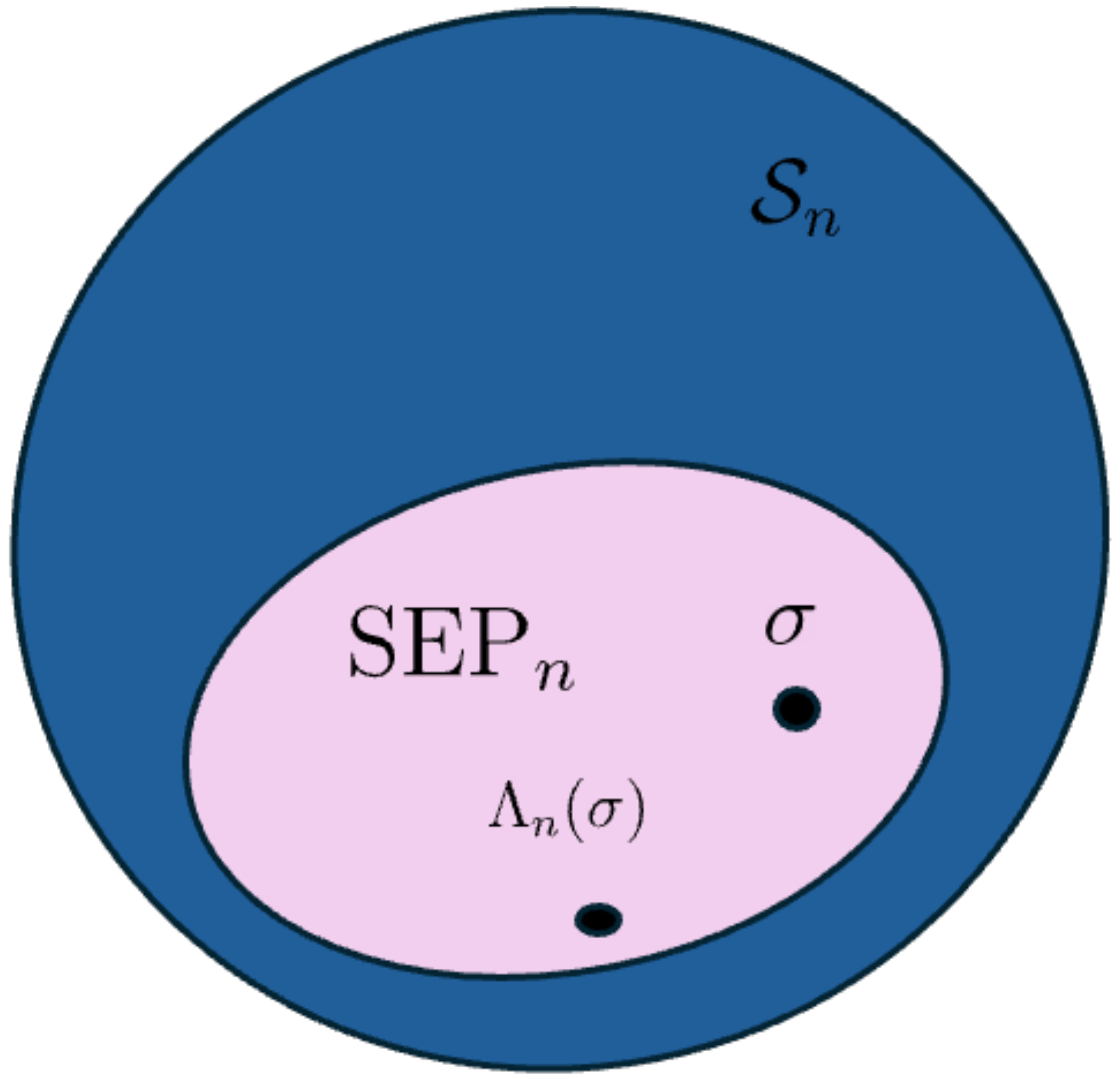
$$|\overset{c}{D}_{\mathcal{F}_n}(\rho) - \overset{c}{D}_{\mathcal{F}_n}(\sigma)| \leq (1+\epsilon)h\left(\frac{\epsilon}{1+\epsilon}\right) + \epsilon\left(\kappa + \log\frac{2}{\epsilon}\right)$$

  - $\kappa = -\log \lambda_{\min}(\sigma^*)$, for a free full rank state σ^*.
    See also [BLT'25, Corollary 14].
  - Computationally indistinguishable states have the same computational accessible resource amount!



Free efficient operation

Computational Entanglement theory



- Computational entropy of entanglement:

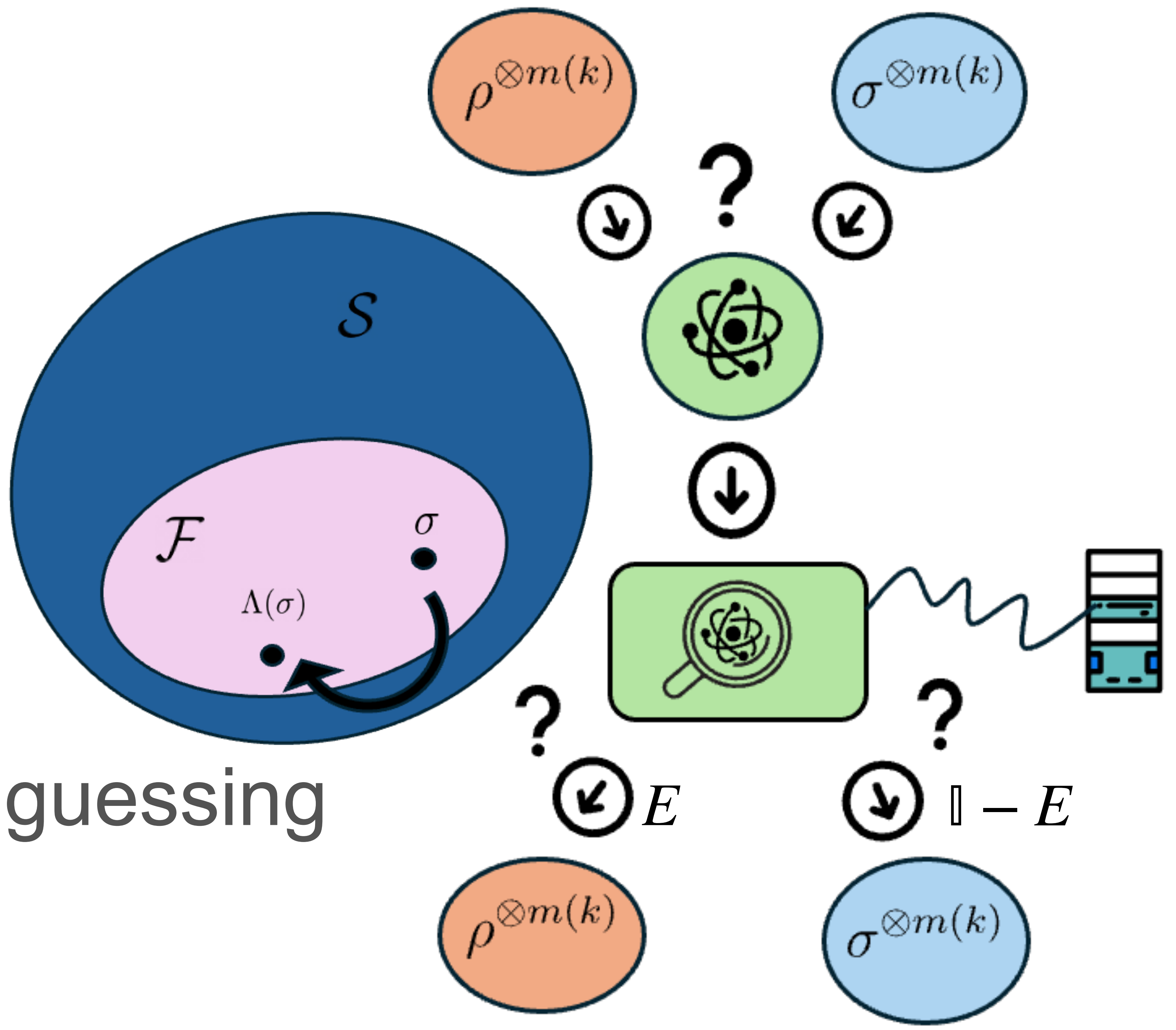
$$\overset{c}{E}_R(\rho) := \inf_{\sigma \in \mathbf{SEP}_n} \overset{c}{D}^{\mathbf{M}_n^{eff}}(\rho \| \sigma)$$

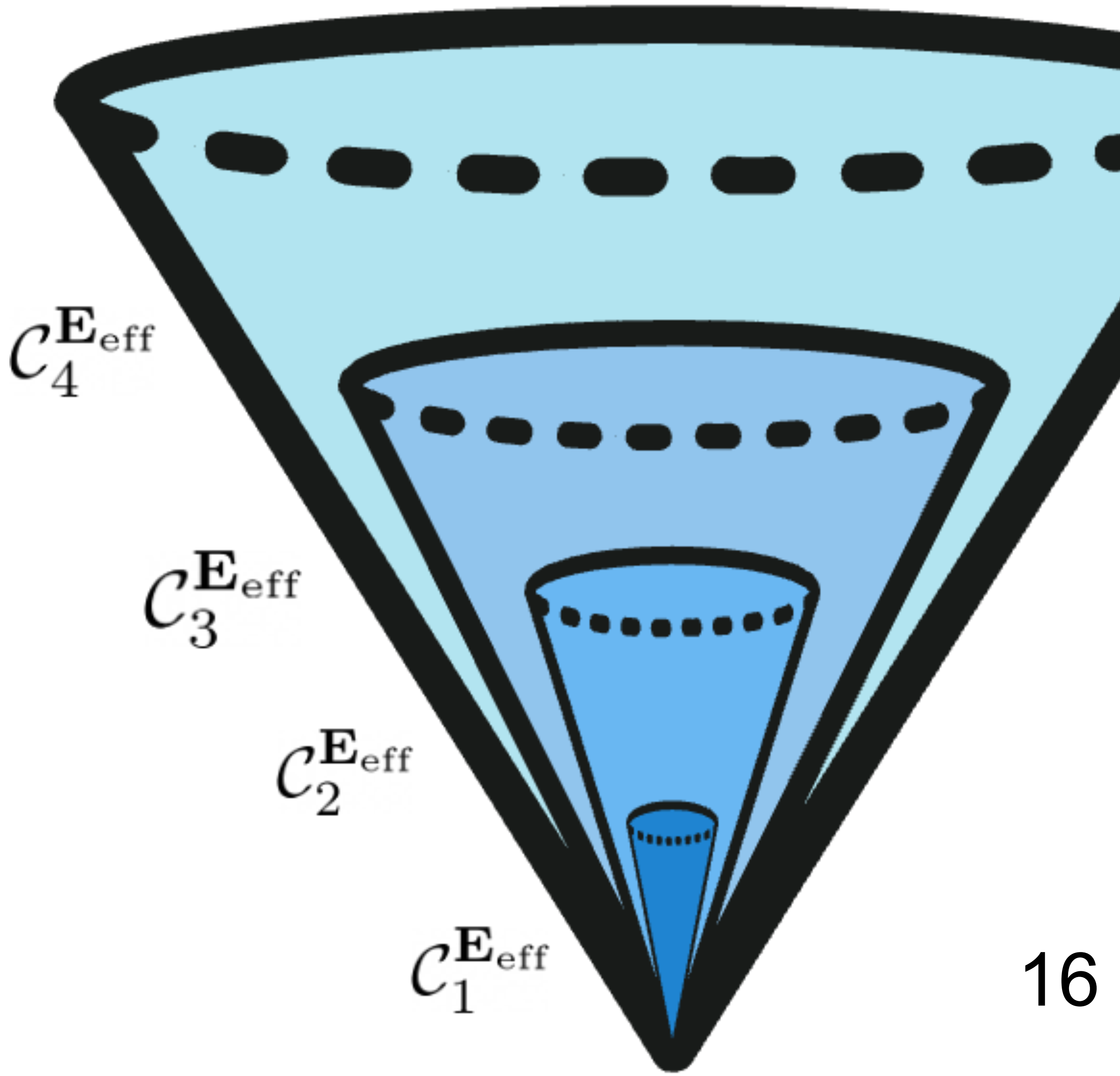
- For Bell states $\overset{c}{E}_R(\Phi^{\otimes n}) = n$ (holds under weak assumptions)
- $\overset{c}{E}_D, \overset{c}{E}_C$ are computational one-shot distillable entanglement and entanglement cost from [ABV'23, Computational Entanglement Theory]
- Lemma 5.15: For $g(\delta, n) = \mathcal{O}(\delta(n - \log \delta))$

$$\overset{c}{E}_D(\rho_{AB}^n) \leq \overset{c}{E}_R(\rho_{AB}^n) + g(\sqrt{\epsilon(n)}, n)$$
$$\overset{c}{E}_C(\rho_{AB}^n) \geq \overset{c}{E}_R(\rho_{AB}^n) - g(\sqrt{\epsilon(n)}, n)$$

Summary

- Computational Max-divergence
  - Operational Comp Min-Entropy and adversarial guessing
- Computational Measured Rényi-divergences
  - Equality for $\alpha \to \infty$
- One-sided computational Stein's Lemma
- Computational Resource theories





TELECOM Paris

IP PARIS

Inria

SORBONNE UNIVERSITÉ

WEIZMANN INSTITUTE OF SCIENCE

Thank you for your attention!

arXiv:2509.21308v1

Funded by the European Union

Bibliography

[Datta'09]: Min- and Max-Relative Entropies and a New Entanglement Monotone; Nilanjana Datta

[RKW'11]: Hilbert's projective metric in quantum information theory; David Reeb, Michael J. Kastoryano, and Michael M. Wolf

[RSB'24]: Locally-Measured Rényi Divergences; Tobias Rippchen, Sreejith Sreekumar, Mario Berta

[Johnston'12]: Norms and Cones in the Theory of Quantum Entanglement; Nathaniel Johnston (PhD Thesis)

[GC'24]: Cone-Restricted Information Theory; Ian George and Eric Chitambar

[GE'24]: Pseudo-entanglement is necessary for efi pairs; Manuel Goulão and David Elkouss.

[MRR+'25]: Computational Relative Entropy; Johannes Jakob Meyer, Asad Raza, Jacopo Rizzo, Lorenzo Leone, Sofiene Jerbi, and Jens Eisert.

[BLT'25]: Continuity of Entropies via Integral Representations; Mario Berta, Ludovico Lami, and Marco Tomamichel

[AA'26]: Noam Avidan and Rotem Arnon. Quantum computational unpredictability entropy and quantum leakage resilience

[AHRA'25]: Noam Avidan, Thomas A. Hahn, Joseph M. Renes, and Rotem Arnon. Fully quantum computational entropies

[KRS'09]: Robert König, Renato Renner, and Christian Schaffner. The operational meaning of min- and max-entropy

[ABV'23]: Rotem Arnon-Friedman, Zvika Brakerski, and Thomas Vidick. Computational Entanglement Theory

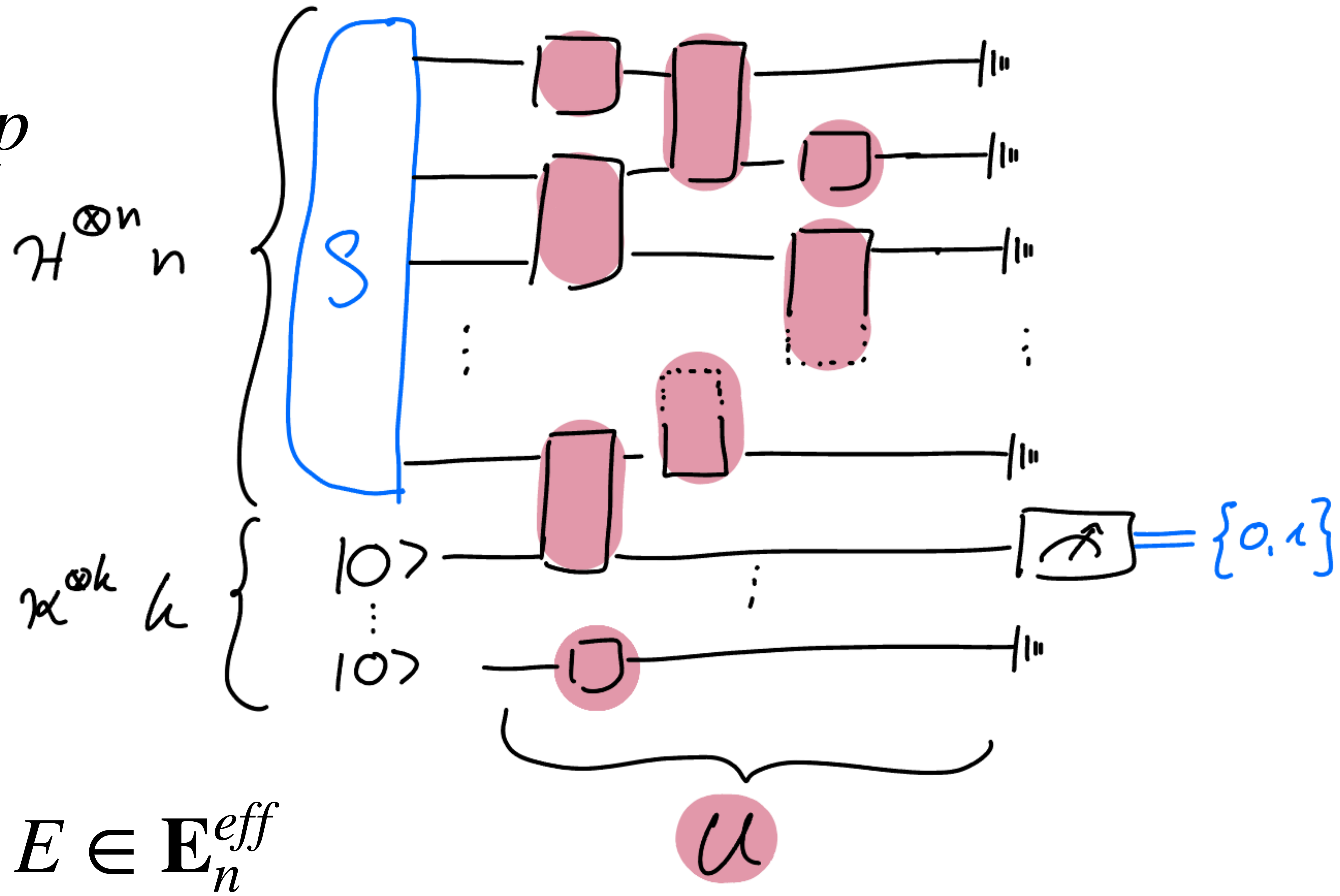
Backup slides

Efficient quantum Measurements

- Def: Efficient effect operators E
  - Given finite Gate-set $\mathscr{G}$, polynomial p

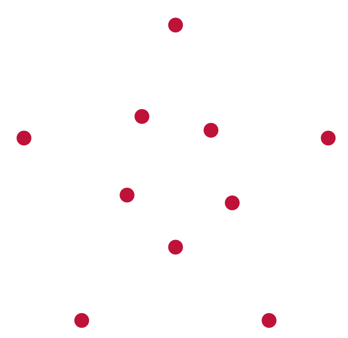
$$\mathbf{E}_n^{eff} \subset \{E \in \text{Pos}(\mathscr{H}^{\otimes n}) \,|\, 0 \leq E \leq \mathbb{I}\}$$

s.t. E or $\mathbb{I} - E$ can be implemented using at most $p(n)$ gates from $\mathscr{G}$.



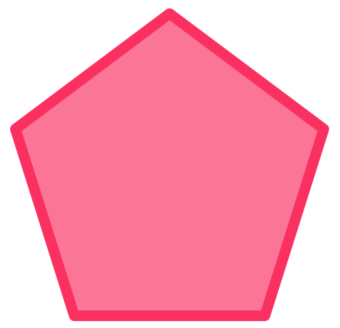
- Assumptions:
  - Complementarity: $E \in \mathbf{E}_n^{eff} \implies \mathbb{I} - E \in \mathbf{E}_n^{eff}$
  - Composition: $E_1 \in \mathbf{E}_{n_1}^{eff}, E_2 \in \mathbf{E}_{n_2}^{eff} \implies E_1 \otimes E_2 \in \mathbf{E}_{n_1+n_2}^{eff}$
  - Information completness: $\text{span}(\mathbf{E}_n^{eff}) = B(\mathscr{H}^{\otimes n})$

The convex set of efficient effects is approx efficient



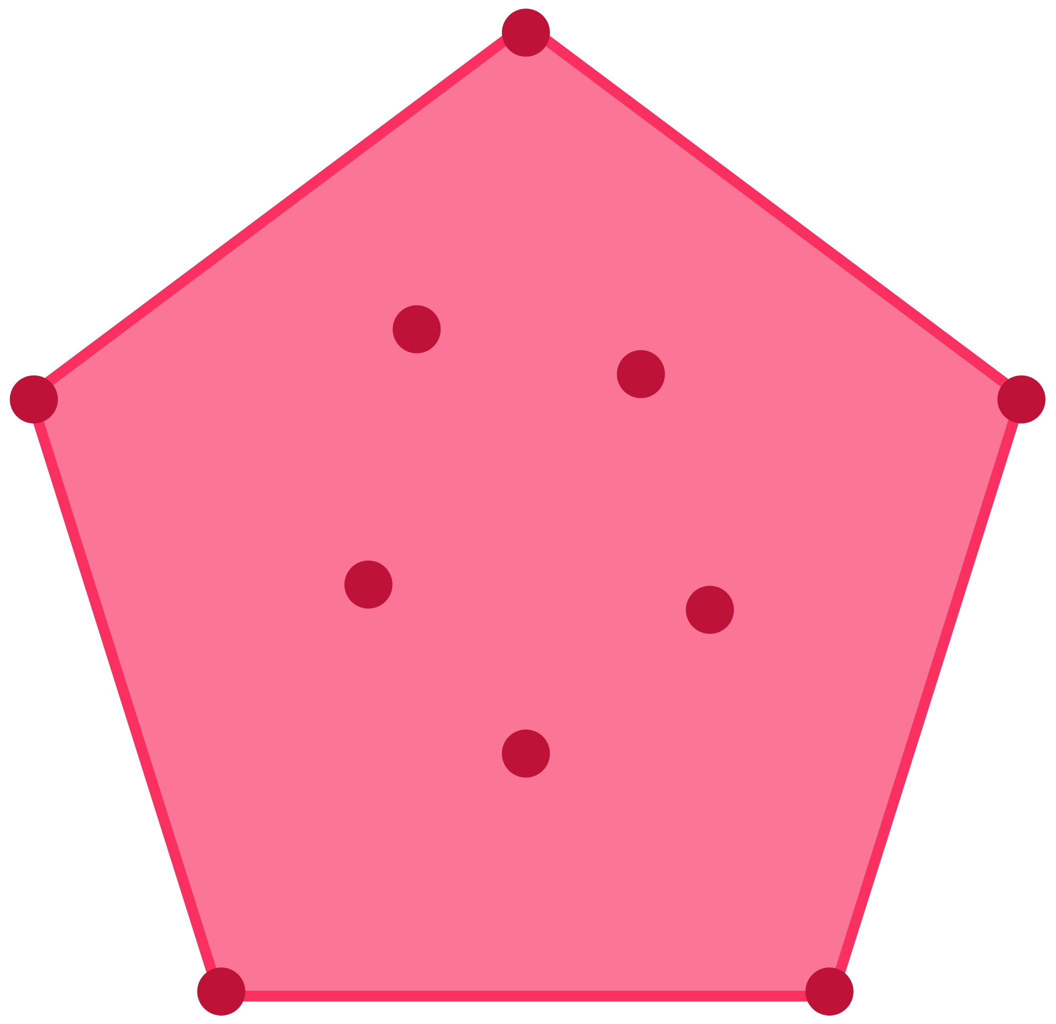
- Poly-generated set of effect operators $\{\mathbf{E}_n^{eff}\}_{n\in\mathbb{N}}$
- Its convex hull is

$$\overline{\mathbf{E}_n^{eff}} := \text{conv}(\mathbf{E}_n^{eff}) = \left\{ \sum_{i=1}^{n} \lambda_i E_i \,|\, n \in \mathbb{N}, \lambda_i \geq 0, \sum_{i=1}^{n} \lambda_i = 1, E \in \mathbf{E}_n^{eff} \right\}$$



- Proposition 3.10: (Approximability of convex closure)
For any effect operator $E \in \overline{\mathbf{E}_n^{eff}}$, there exists a subset of $k = 5\epsilon^{-2}(n \ln \dim\mathscr{H} + 1)$ effect operators $E_{j_i} \in \mathbf{E}_n^{eff}$ s.t.

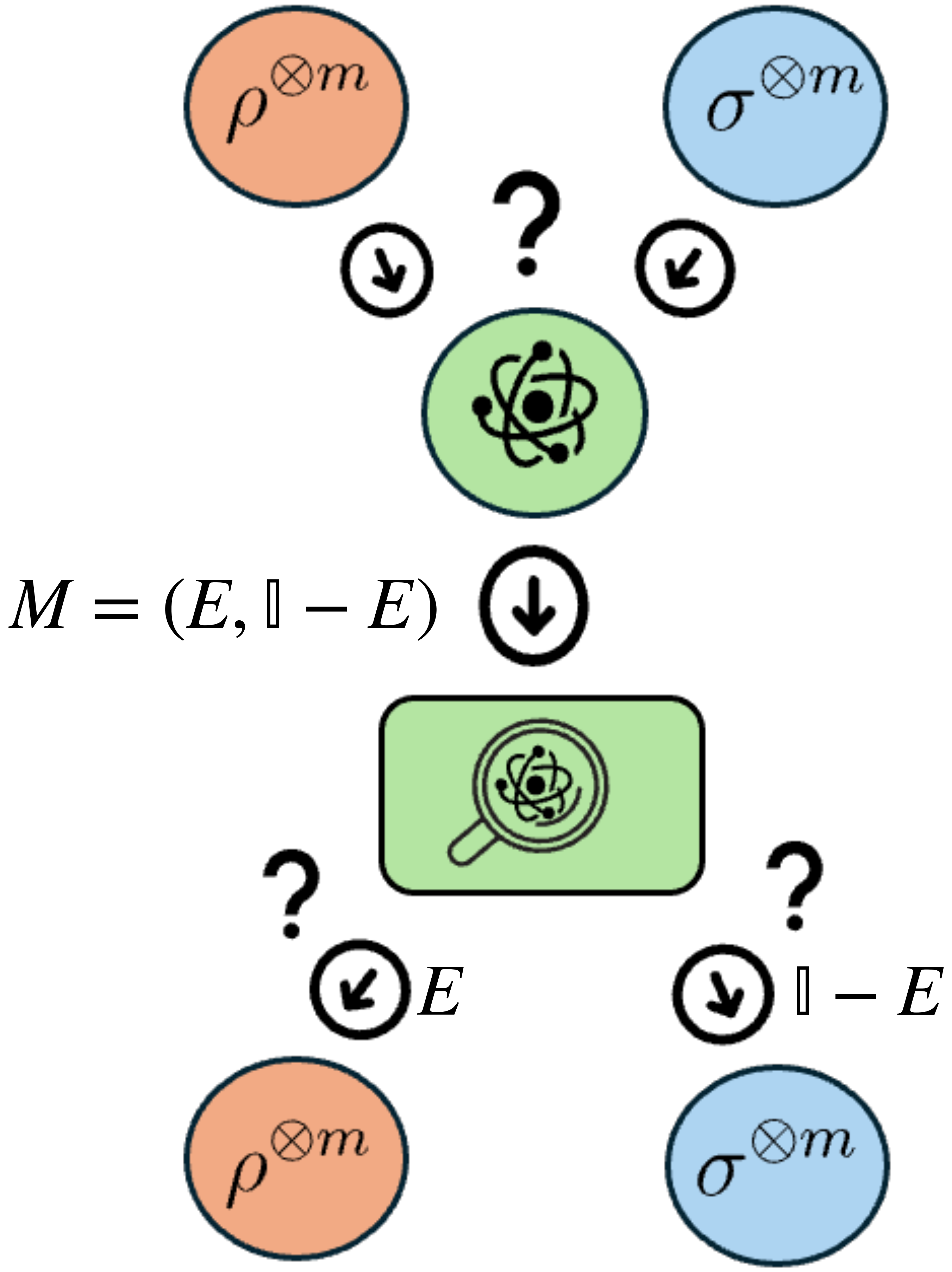
$$\left\| E - \frac{1}{k}\sum_{i=1}^{k} E_{j_i} \right\|_\infty \leq \epsilon \,.$$



Operational significance in hypothesis testing

- Task: State discrimination (hypothesis testing)
- Binary measurement $M = (E, \mathbb{1} - E)$
  - Type-I-error: $\alpha_n(M) = \mathrm{Tr}[\rho^{\otimes n}(\mathbb{1} - E_n)]$
  - Type-II-error: $\beta_n(M) = \mathrm{Tr}[\sigma^{\otimes n} E_n]$
- Asymmetric optimal type-II-error:
  - $\beta_n^\epsilon(\mathbf{M}) := \min_{M \in \mathbf{M}} \{\beta_n(M) \,|\, \alpha_n(M) \leq \epsilon\}$
- Steins Exponent:

$$\xi(\rho, \sigma; \mathbf{M}) := \lim_{\epsilon \to 0} \limsup_{n \to \infty} \frac{-1}{n} \log \beta_n^\epsilon(\mathbf{M})$$



Operational significance in hypothesis testing

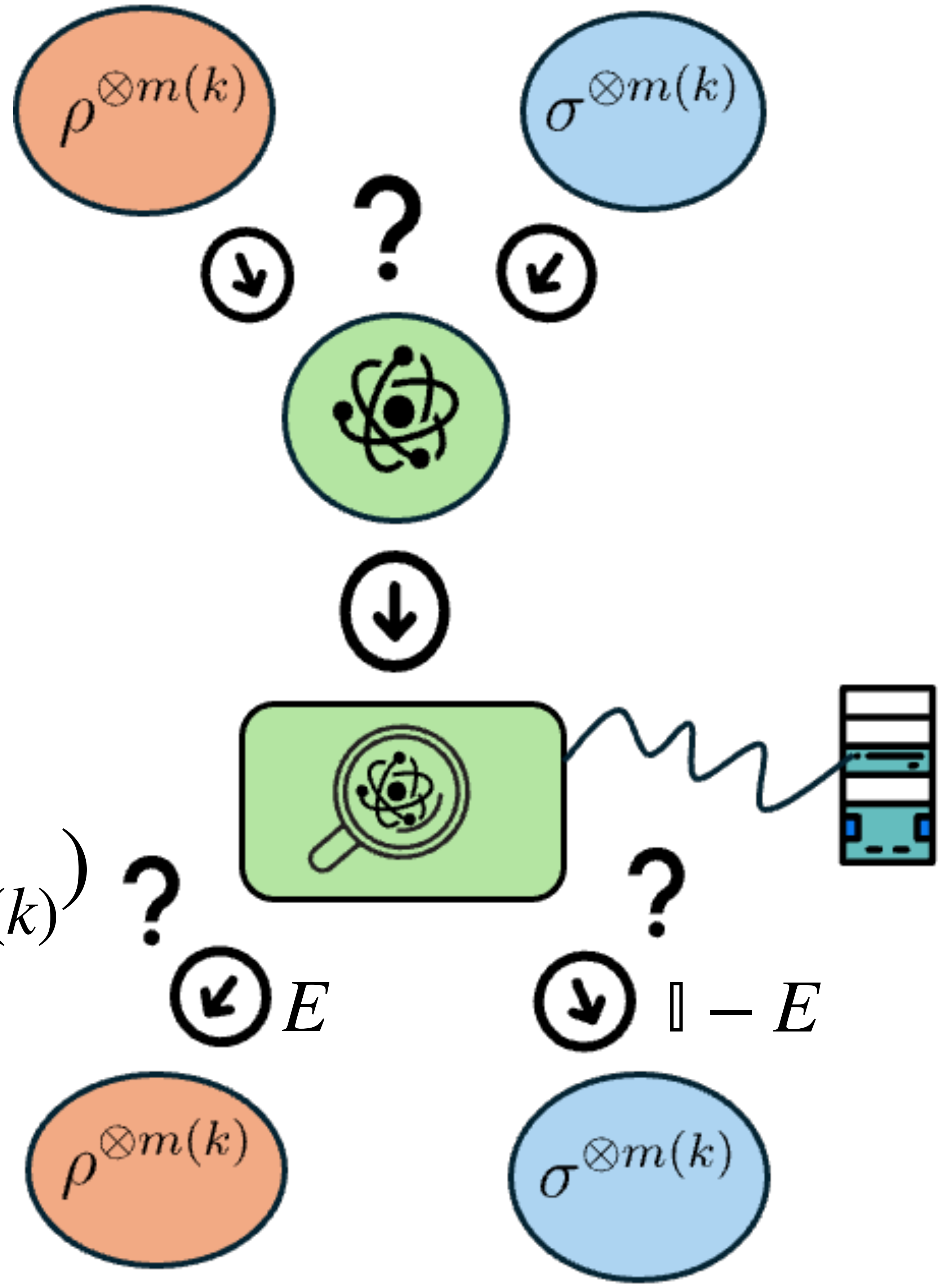
- Task: Computationally constrained state discrimination
  - $\rho_k^{m(k)}$ vs. $\sigma_k^{m(k)}$ using $M = (E_{k\cdot m(k)}, \mathbb{I} - E_{k\cdot m(k)}) \in \overline{\mathbf{M}}^{\mathit{eff}}_{k\cdot m(k)}$
- Computational Steins Exponent:

$$\xi(\{\rho_k\}, \{\sigma_k\}; \{\mathbf{M}^{\mathit{eff}}_{k\cdot m(k)}\}) := \lim_{\epsilon\to 0} \limsup_{k\to\infty} \frac{-1}{m(k)} \log \beta^{\epsilon}_{m(k)}(\mathbf{M}^{\mathit{eff}}_{k\cdot m(k)})$$

- Theorem 5.2: One-Sided Computational Steins Lemma

$$\xi(\{\rho_k\}, \{\sigma_k\}; \{\mathbf{M}^{\mathit{eff}}_{k\cdot m(k)}\}) \leq \overset{c}{D}{}^{\mathrm{reg}}(\{\rho_k\}, \{\sigma_k\})$$

$$\overset{c}{D}{}^{\mathrm{reg}}(\{\rho_k\}, \{\sigma_k\}) := \limsup_{k\to\infty} \frac{1}{m(k)} \overset{c}{D}{}^{\mathbf{M}^{\mathit{eff}}_{k\cdot m(k)}}(\rho_k^{\otimes m(k)} \| \sigma_k^{\otimes m(k)})$$



Compare [MRR+25]