A doubly composite Chernoff–Stein lemma and its applications

2510.06342 & 2510.06340

SCUOLA
NORMALE
SUPERIORE

Ludovico Lami

Scuola Normale Superiore, Pisa, Italy

European Research Council
Established by the European Commission

Introduction

Quantum hypothesis testing = Given two hypotheses concerning a quantum state, which one holds true?

Quantum hypothesis testing = Given two hypotheses concerning a quantum state, which one holds true?

Simple hypothesis: one of two known quantum states.

⤳ represented by density operators ρ, σ.

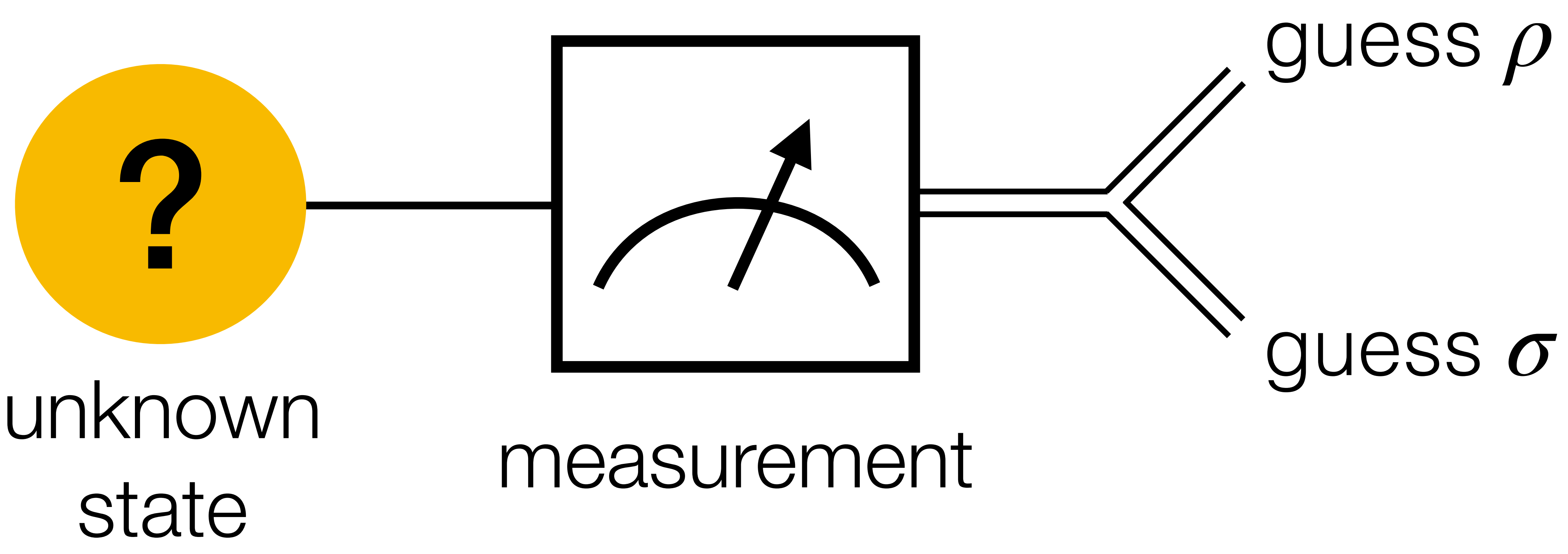
Quantum hypothesis testing = Given two hypotheses concerning a quantum state, which one holds true?

Simple hypothesis: one of two known quantum states.

⟿ represented by density operators ρ, σ.

Null hypothesis: ρ

Alternative hypothesis: σ

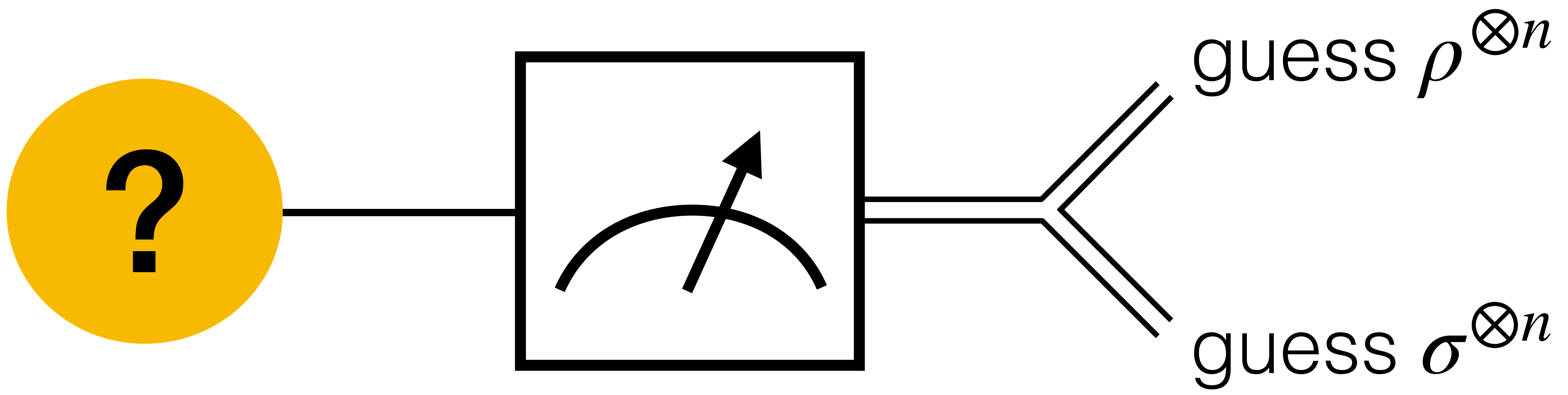


Quantum hypothesis testing = Given two hypotheses concerning a **quantum state**, which one holds true?

Simple IID hypotheses: many copies of one of two states.

Null hypothesis: $\rho^{\otimes n}$

Alternative hypothesis: $\sigma^{\otimes n}$

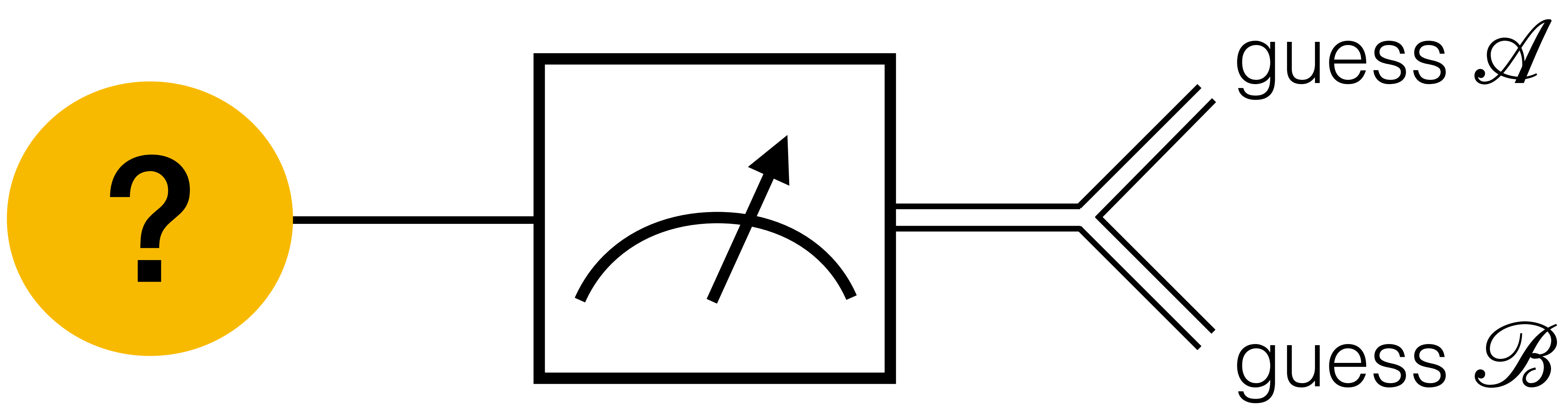


Quantum hypothesis testing = Given two hypotheses concerning a quantum state, which one holds true?

Composite hypotheses: two **sets** of quantum states.

Null hypothesis: $\rho \in \mathscr{A}$

Alternative hypothesis: $\sigma \in \mathscr{B}$



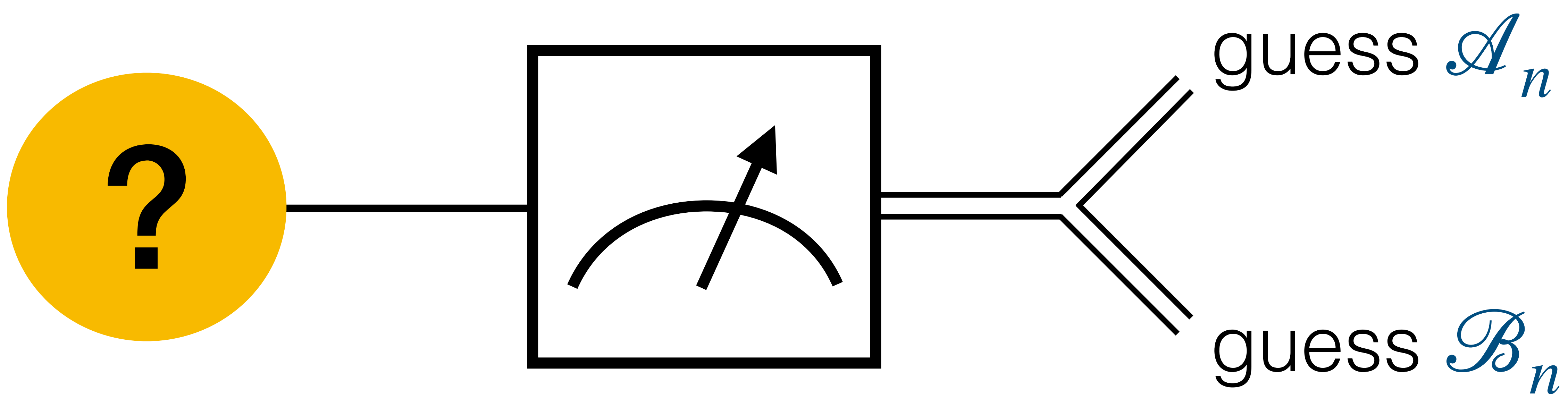
$\mathscr{A}, \mathscr{B}$: sets of states on the same quantum system.

Quantum hypothesis testing = Given two hypotheses concerning a quantum state, which one holds true?

Composite hypotheses: two sequences of sets of states, indexed by $n \in \mathbb{N}$.

Null hypothesis: $\rho_n \in \mathscr{A}_n$

Alternative hypothesis: $\sigma_n \in \mathscr{B}_n$



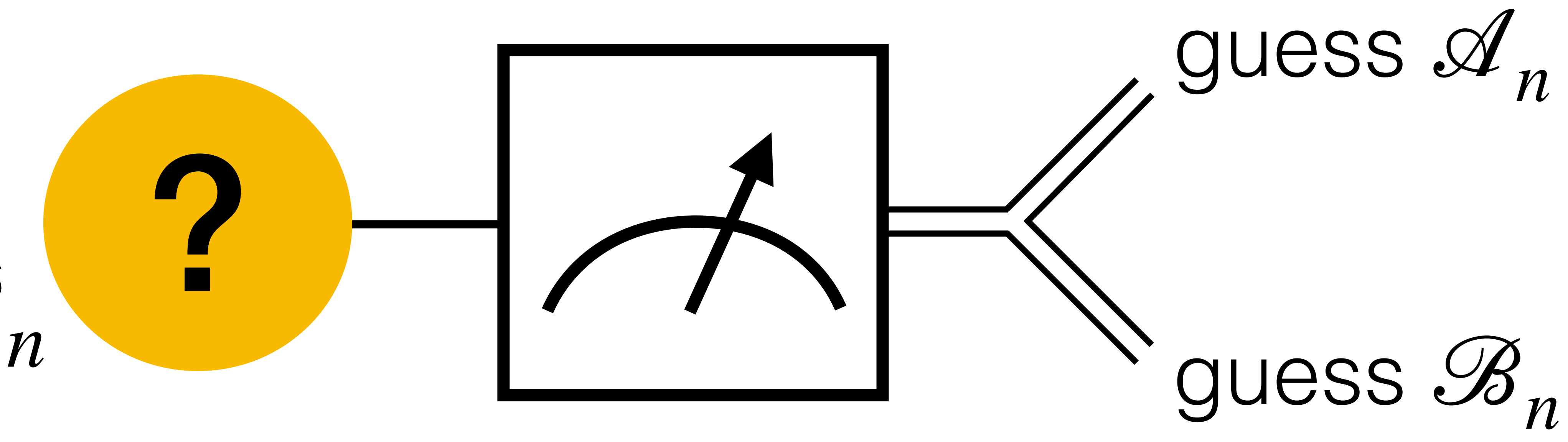
$\mathscr{A}_n, \mathscr{B}_n \subseteq \mathscr{D}\left(\mathscr{H}^{\otimes n}\right)$ sequences of sets of states on the n-copy system.

Two types of error:

- Type 1: null hypothesis correct, guessed alternative
- Type 2: alternative hypothesis correct, guessed null

Null hypothesis: $\rho_n \in \mathscr{A}_n$

Alternative hypothesis: $\sigma_n \in \mathscr{B}_n$

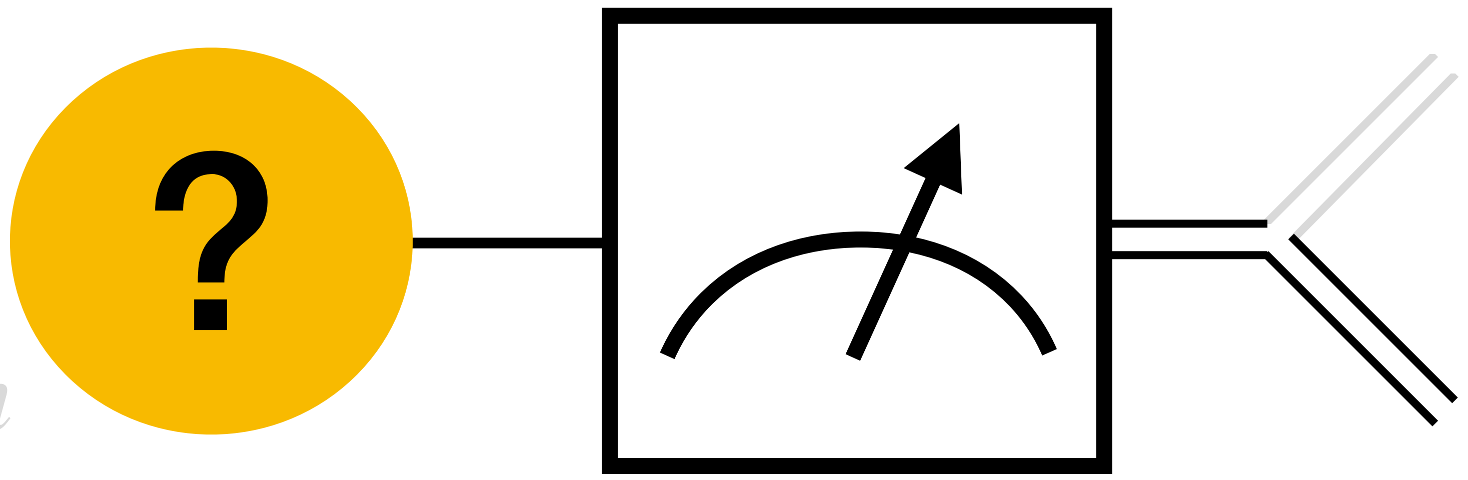


Two types of error:

- Type 1: null hypothesis correct, guessed alternative
- Type 2: alternative hypothesis correct, guessed null

Null hypothesis: $\rho_n \in \mathscr{A}_n$

Alternative hypothesis: $\sigma_n \in \mathscr{B}_n$



guess $\mathscr{A}_n$ ⇝ type 2 error

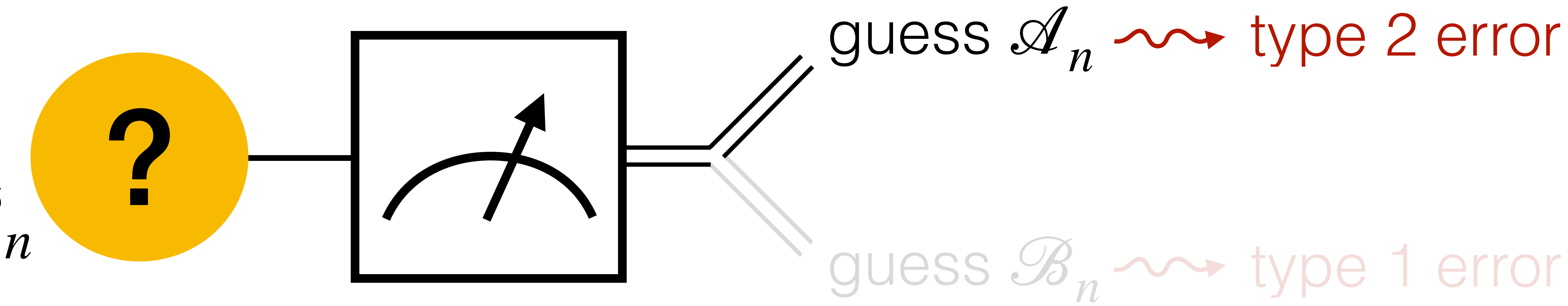
guess $\mathscr{B}_n$ ⇝ type 1 error

Two types of error:

- Type 1: null hypothesis correct, guessed alternative
- Type 2: alternative hypothesis correct, guessed null

Null hypothesis: $\rho_n \in \mathscr{A}_n$

Alternative hypothesis: $\sigma_n \in \mathscr{B}_n$

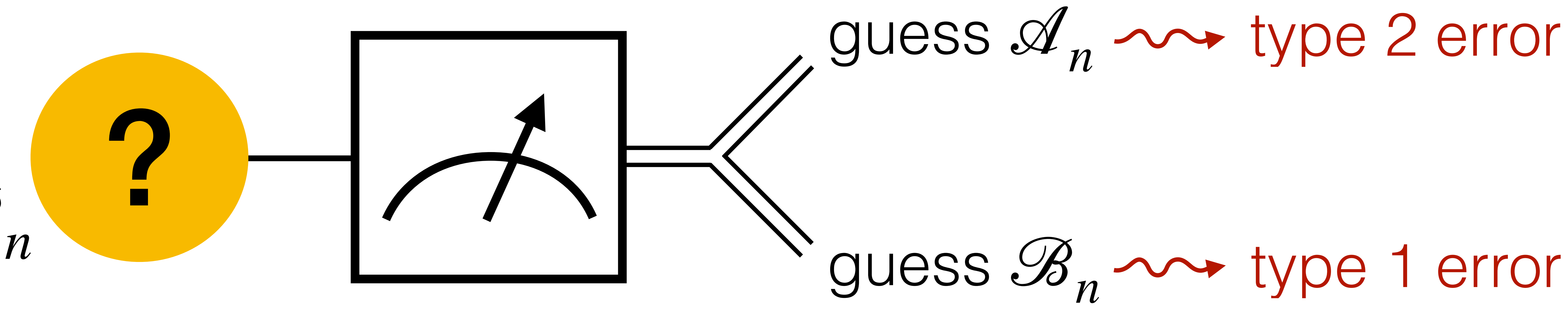


Two types of error:

- Type 1: null hypothesis correct, guessed alternative
- Type 2: alternative hypothesis correct, guessed null

Null hypothesis: $\rho_n \in \mathscr{A}_n$

Alternative hypothesis: $\sigma_n \in \mathscr{B}_n$



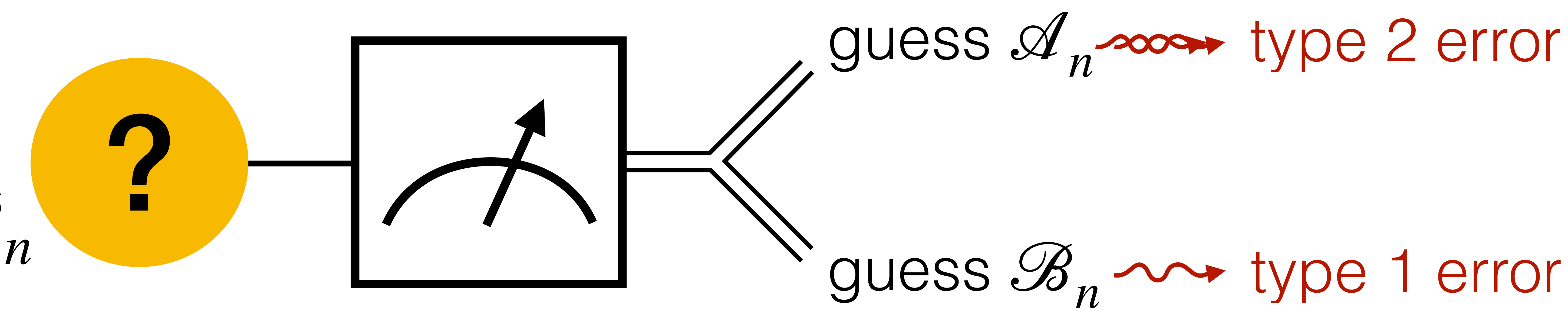
Asymmetric hypothesis testing: fix Pr{type 1} $\leq \varepsilon$, minimise Pr{type 2} as $n \to \infty$.

Two types of error:

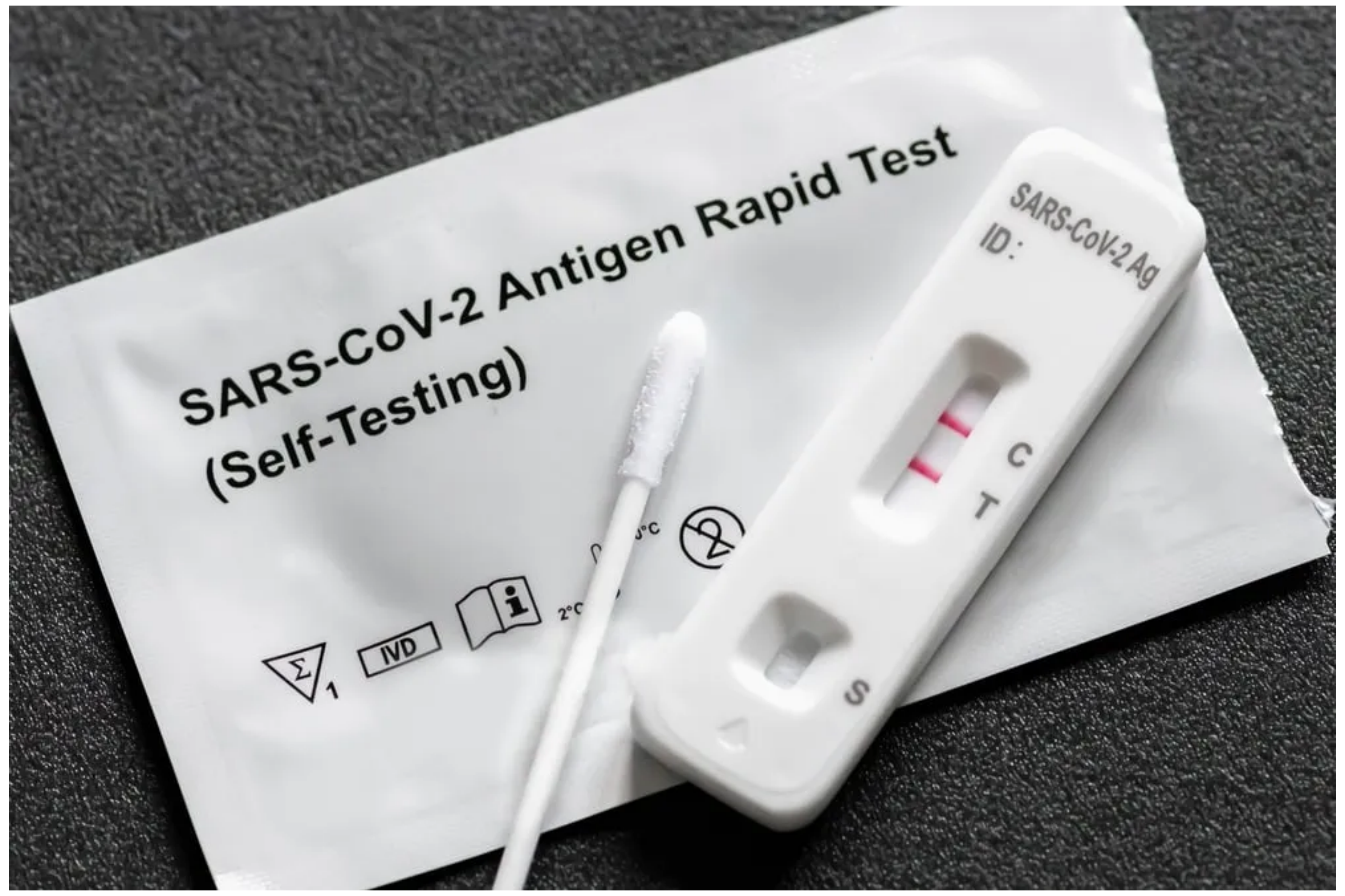
- Type 1: null hypothesis correct, guessed alternative
- Type 2: alternative hypothesis correct, guessed null

Null hypothesis: $\rho_n \in \mathscr{A}_n$

Alternative hypothesis: $\sigma_n \in \mathscr{B}_n$



Asymmetric hypothesis testing: fix Pr{type 1} $\leq \varepsilon$, minimise Pr{type 2} as $n \to \infty$.



Asymmetric hypothesis testing: fix Pr{type 1} $\leq \varepsilon$, minimise Pr{type 2} as $n \to \infty$.

Asymmetric hypothesis testing: fix Pr{type 1} $\leq \varepsilon$, minimise Pr{type 2} as $n \to \infty$.

Stein exponent:

$$\mathrm{Stein}(\mathscr{A}\|\mathscr{B}) := \lim_{\varepsilon\to 0}\lim_{n\to\infty} -\frac{1}{n}\log\min\left\{\Pr\{\text{type 2}\}\ :\ \Pr\{\text{type 1}\} \leq \varepsilon\right\}$$

$$\mathscr{A} = (\mathscr{A}_n)_n\,, \qquad \mathscr{B} = (\mathscr{B}_n)_n$$

Asymmetric hypothesis testing: fix Pr{type 1} $\leq \varepsilon$, minimise Pr{type 2} as $n \to \infty$.

Stein exponent:

$$\mathrm{Stein}(\mathscr{A}\|\mathscr{B}) := \lim_{\varepsilon\to 0}\lim_{n\to\infty} -\frac{1}{n}\log\min\left\{\Pr\{\text{type 2}\} :\ \Pr\{\text{type 1}\} \leq \varepsilon\right\}$$

$$\mathscr{A} = (\mathscr{A}_n)_n\,, \qquad \mathscr{B} = (\mathscr{B}_n)_n$$

Problem: compute $\mathrm{Stein}(\mathscr{A}\|\mathscr{B})$ for the most general sequences of sets $\mathscr{A}, \mathscr{B}$.

Asymmetric hypothesis testing: fix Pr{type 1} $\leq \varepsilon$, minimise Pr{type 2} as $n \to \infty$.

Stein exponent:

$$\mathrm{Stein}(\mathscr{A}\|\mathscr{B}) := \lim_{\varepsilon\to 0}\lim_{n\to\infty} -\frac{1}{n}\log\min\left\{\Pr\{\text{type 2}\} :\ \Pr\{\text{type 1}\} \leq \varepsilon\right\}$$

$$\mathscr{A} = (\mathscr{A}_n)_n\,, \qquad \mathscr{B} = (\mathscr{B}_n)_n$$

Problem: compute $\mathrm{Stein}(\mathscr{A}\|\mathscr{B})$ for the most general sequences of sets $\mathscr{A}, \mathscr{B}$.

Compute := find an “entropic” formula = eliminate the limit $\varepsilon \to 0$.

Asymmetric hypothesis testing: fix Pr{type 1} $\leq \varepsilon$, minimise Pr{type 2} as $n \to \infty$.

Stein exponent:

$$\mathrm{Stein}(\mathscr{A}\|\mathscr{B}) := \lim_{\varepsilon\to 0}\lim_{n\to\infty} -\frac{1}{n}\log\min\left\{\Pr\{\text{type 2}\} :\ \Pr\{\text{type 1}\} \leq \varepsilon\right\}$$

$$\mathscr{A} = (\mathscr{A}_n)_n, \qquad \mathscr{B} = (\mathscr{B}_n)_n$$

Problem: compute $\mathrm{Stein}(\mathscr{A}\|\mathscr{B})$ for the most general sequences of sets $\mathscr{A}, \mathscr{B}$.

Compute := find an "entropic" formula = eliminate the limit $\varepsilon \to 0$.

Single-letter expressions (= with no limits $\varepsilon \to 0$ or $n \to \infty$): sometimes, but unrealistic in most cases…

Hypotheses zoology:

- Simple IID: $\mathscr{A}_n = \{\rho^{\otimes n}\}$

Hypotheses zoology:

- Simple IID: $\mathscr{A}_n = \{\rho^{\otimes n}\}$
- Composite IID: $\mathscr{A}_n = \{\rho^{\otimes n} : \ \rho \in \mathscr{A}_1\} \longrightarrow \mathscr{A}_1^{\mathrm{iid}}$

Composite = more than one state

Hypotheses zoology:

- Simple IID: $\mathscr{A}_n = \{\rho^{\otimes n}\}$
- Composite IID: $\mathscr{A}_n = \{\rho^{\otimes n} : \ \rho \in \mathscr{A}_1\} \longrightarrow \mathscr{A}_1^{\text{iid}}$
- Composite, arbitrarily varying: $\mathscr{A}_n = \{\rho_1 \otimes \ldots \otimes \rho_n : \ \rho_i \in \mathscr{A}_1\} \longrightarrow \mathscr{A}_1^{\text{av}}$

Composite = more than one state

Hypotheses zoology:

- Simple IID: $\mathscr{A}_n = \{\rho^{\otimes n}\}$
- Composite IID: $\mathscr{A}_n = \{\rho^{\otimes n} :\ \rho \in \mathscr{A}_1\} \longrightarrow \mathscr{A}_1^{\text{iid}}$
- Composite, arbitrarily varying: $\mathscr{A}_n = \{\rho_1 \otimes \ldots \otimes \rho_n :\ \rho_i \in \mathscr{A}_1\} \longrightarrow \mathscr{A}_1^{\text{av}}$
- Genuinely correlated sets: extremal points are not product across the copies.

Composite = more than one state

Hypotheses zoology:

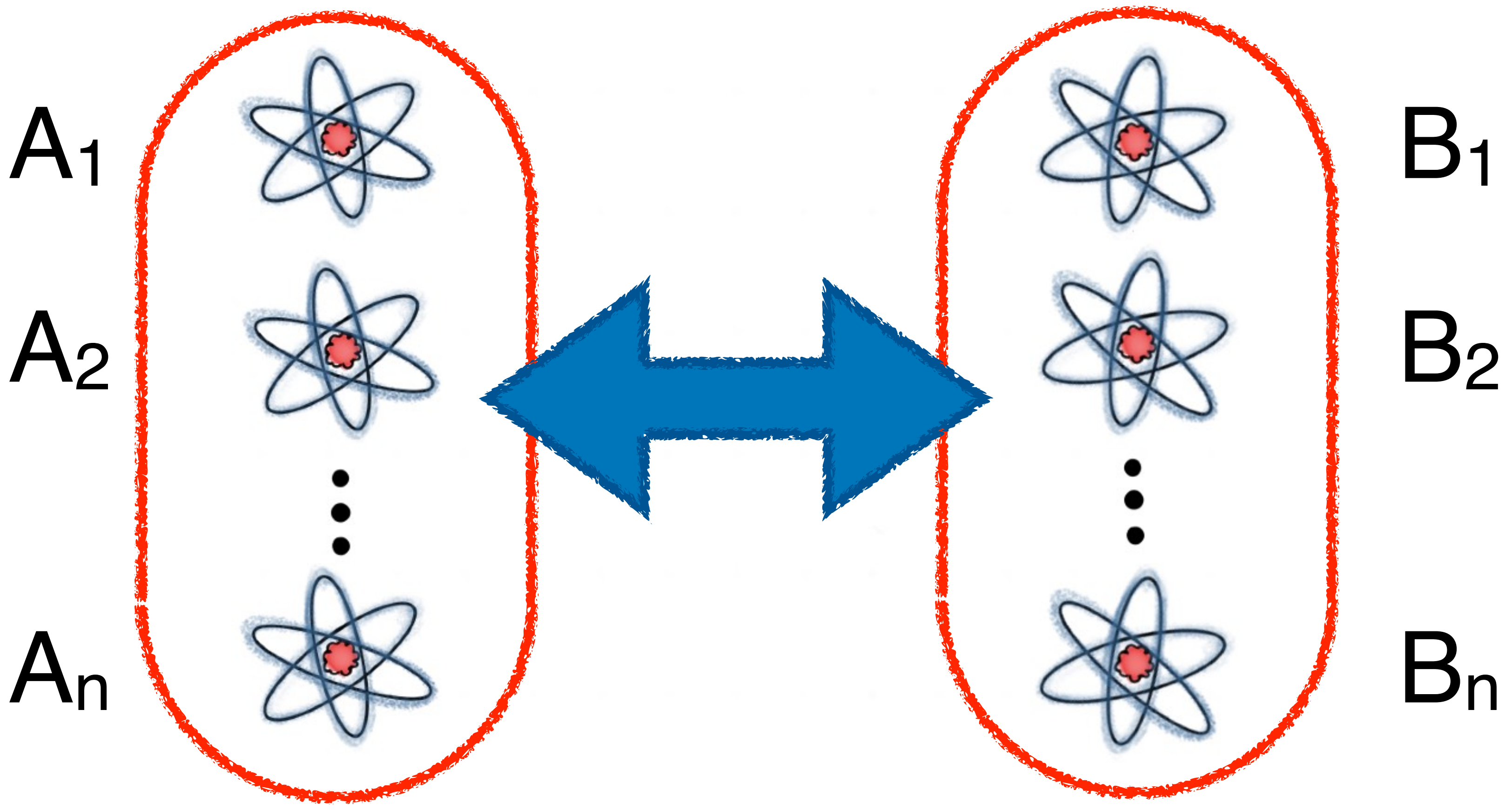
- Simple IID: $\mathscr{A}_n = \{\rho^{\otimes n}\}$
- Composite IID: $\mathscr{A}_n = \{\rho^{\otimes n} : \ \rho \in \mathscr{A}_1\} \longrightarrow \mathscr{A}_1^{\mathrm{iid}}$

Composite = more than one state

- Composite, arbitrarily varying: $\mathscr{A}_n = \{\rho_1 \otimes \ldots \otimes \rho_n : \ \rho_i \in \mathscr{A}_1\} \longrightarrow \mathscr{A}_1^{\mathrm{av}}$
- Genuinely correlated sets: extremal points are not product across the copies.
- More complicated sets…

Example of more complicated sets:

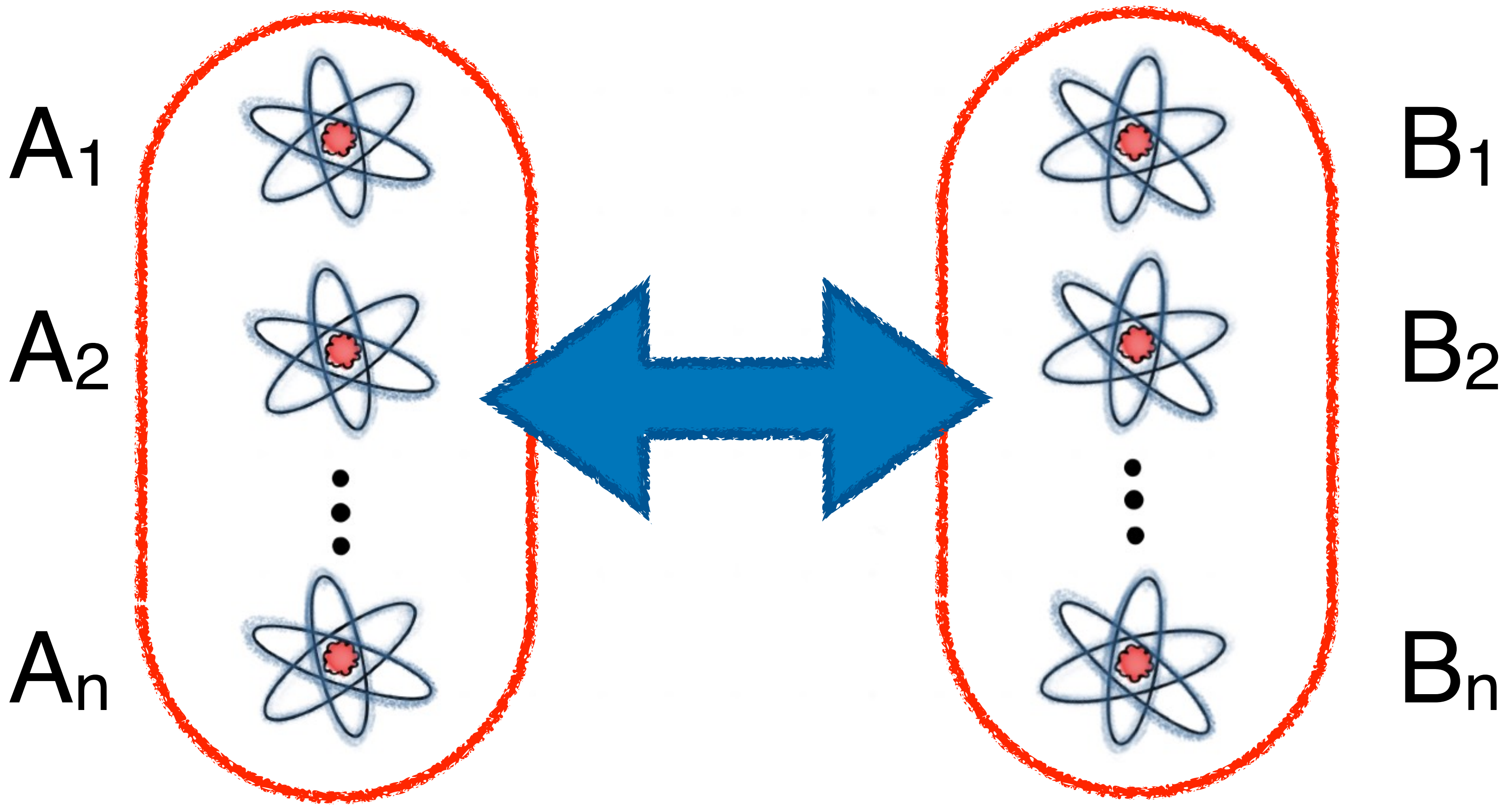
Separable states (SEP)



$$\mathrm{SEP}_n = \mathrm{SEP}_{A^n:B^n} := \mathrm{conv}\left\{\rho_{A^n} \otimes \sigma_{B^n}\right\}$$

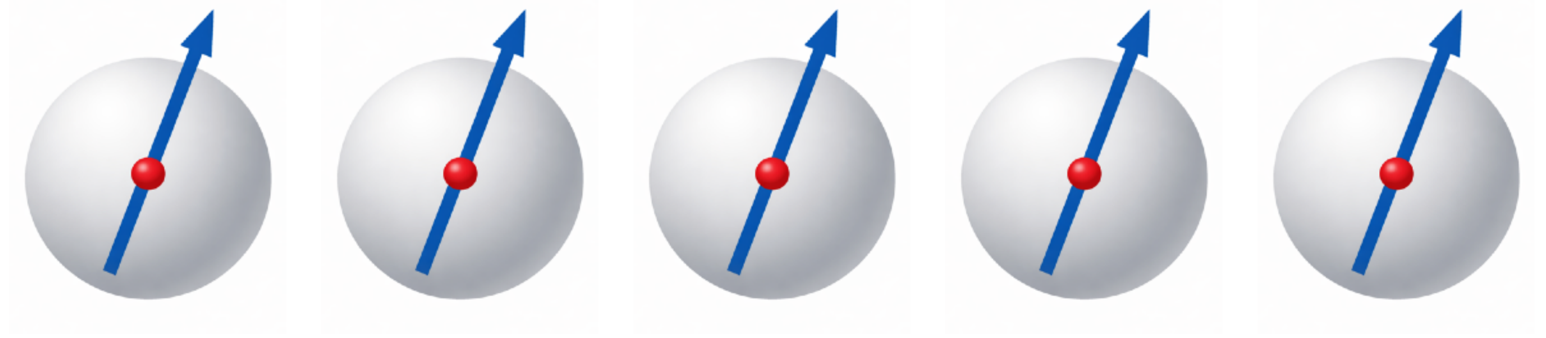
Example of more complicated sets:

Separable states (SEP)



$$\mathrm{SEP}_n = \mathrm{SEP}_{A^n:B^n} := \mathrm{conv}\left\{\rho_{A^n} \otimes \sigma_{B^n}\right\}$$

Stabiliser states (STAB)

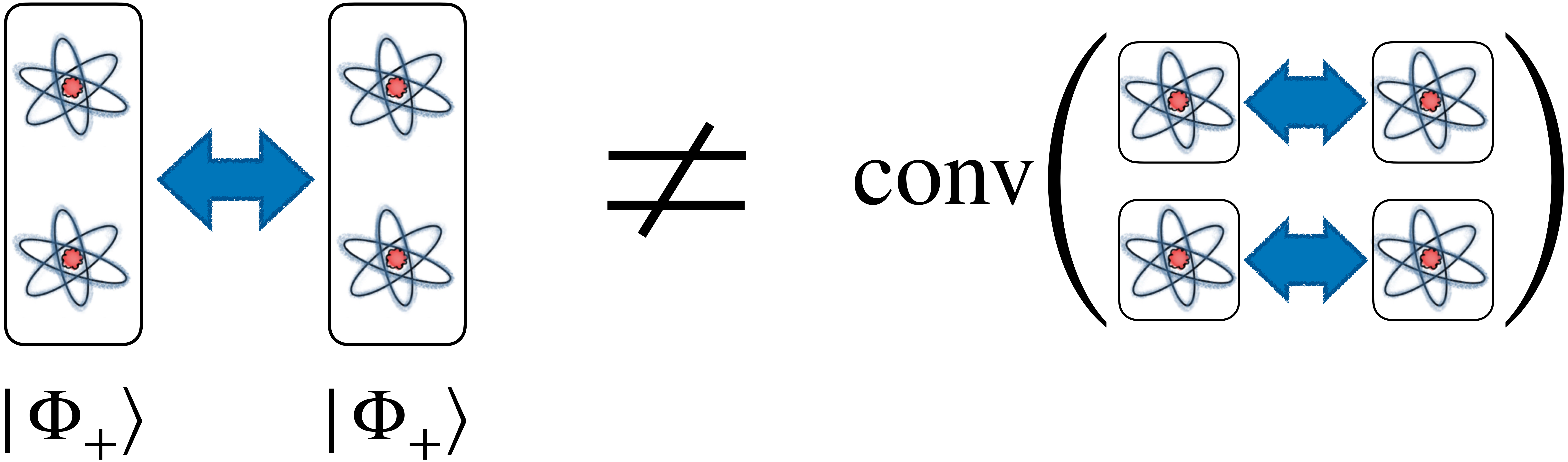


n-qubit system

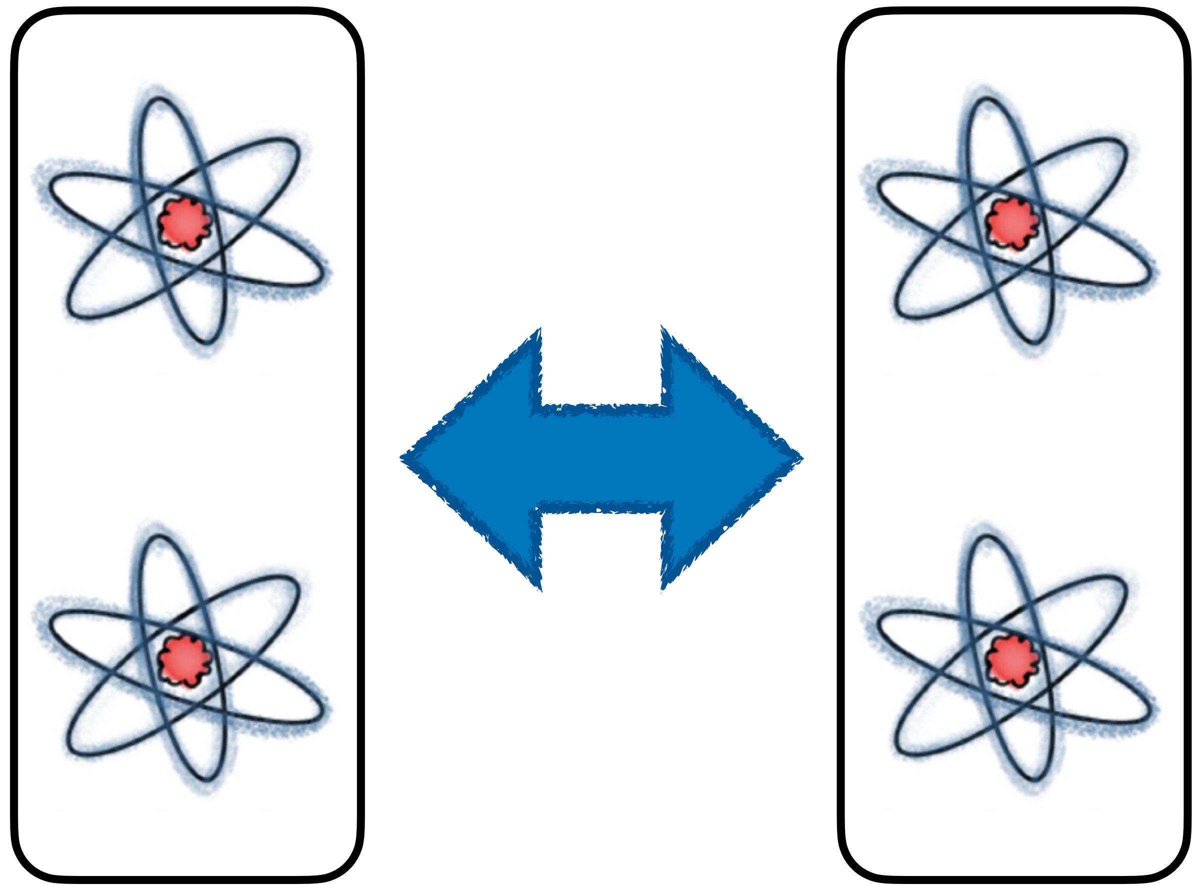
Clifford group

$$\mathrm{STAB}_n := \mathrm{conv}\left\{ C|0\rangle\langle 0|^{\otimes n} C^\dagger : \ C \in \mathscr{C}_n \right\}$$

Genuinely correlated: extremal points are <u>not</u> product across the copies.

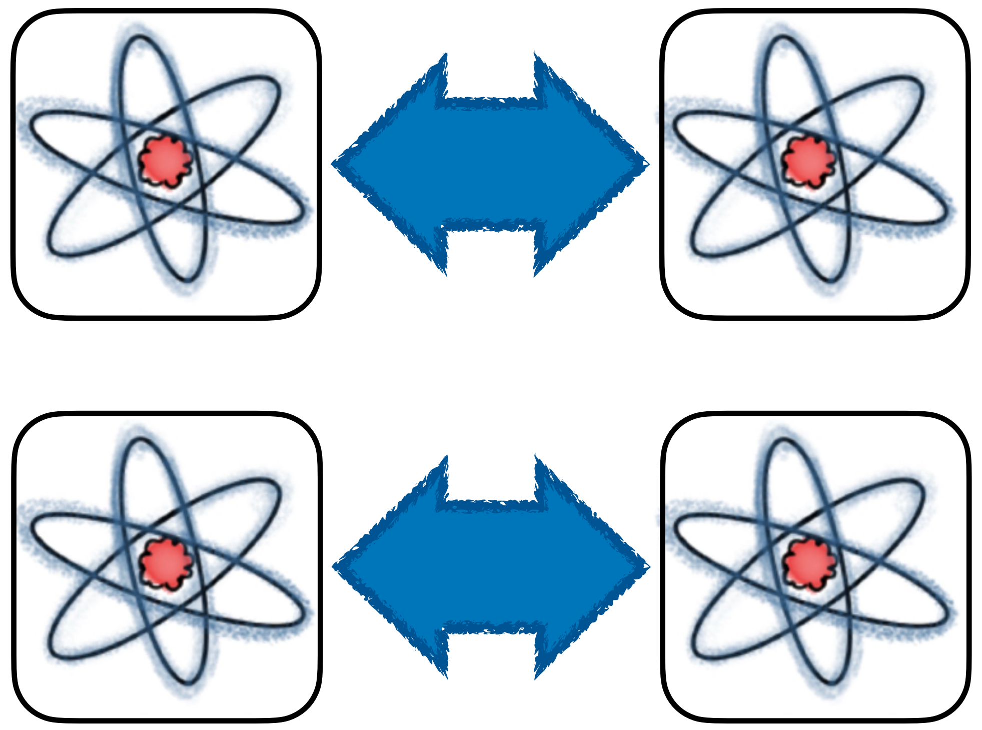


Genuinely correlated: extremal points are **not** product across the copies.



$|\Phi_+\rangle \qquad |\Phi_+\rangle$

$$\neq \quad \mathrm{conv}\Big(\Big)$$



$$\sum_i p_i \; \sigma^{(i)}_{A_1:B_1} \otimes \sigma^{(i)}_{A_2:B_2}, \qquad \sigma^{(i)}_{A_j:B_j} \in \mathrm{SEP}_1$$

Some prior results:

- Quantum Stein's lemma → simple IID vs simple IID:

$$\mathrm{Stein}\Big((\rho^{\otimes n})_n \,\|\, (\sigma^{\otimes n})_n\Big) = D(\rho\|\sigma)$$

[Hiai/Petz 1991]

Some prior results:

- Quantum Stein's lemma → simple IID vs simple IID:

$$\text{Stein}\big((\rho^{\otimes n})_n \,\|\, (\sigma^{\otimes n})_n\big) = D(\rho\|\sigma)$$

[Hiai/Petz 1991]

- Quantum Sanov theorem → composite IID/AV vs simple IID:

$$\text{Stein}\big(\mathscr{A}_1^{\text{iid}} \,\|\, (\sigma^{\otimes n})_n\big) = \inf_{\rho\in\mathscr{A}_1} D(\rho\|\sigma)$$

[Bjelaković et al. 2005]

$$\text{Stein}\big(\mathscr{A}_1^{\text{av}} \,\|\, (\sigma^{\otimes n})_n\big) = \inf_{\rho\in\text{conv}(\mathscr{A}_1)} D(\rho\|\sigma)$$

[Nötzel 2014]

Some prior results:

- Quantum Stein's lemma → simple IID vs simple IID:

$$\mathrm{Stein}\Big((\rho^{\otimes n})_n \,\|\, (\sigma^{\otimes n})_n\Big) = D(\rho\|\sigma)$$

[Hiai/Petz 1991]

- Quantum Sanov theorem → composite IID/AV vs simple IID:

$$\mathrm{Stein}\Big(\mathscr{A}_1^{\mathrm{iid}} \,\|\, (\sigma^{\otimes n})_n\Big) = \inf_{\rho\in\mathscr{A}_1} D(\rho\|\sigma)$$

[Bjelakovič et al. 2005]

$$\mathrm{Stein}\Big(\mathscr{A}_1^{\mathrm{av}} \,\|\, (\sigma^{\otimes n})_n\Big) = \inf_{\rho\in\mathrm{conv}(\mathscr{A}_1)} D(\rho\|\sigma)$$

[Nötzel 2014]

Single-letter!

Note: same formula, but $\mathscr{A}_1 \mapsto \mathrm{conv}(\mathscr{A}_1)$. Coincidence?

Some prior results:

- Generalised quantum Stein's lemma → simple IID vs SEP/STAB

$$\mathrm{Stein}\big((\rho^{\otimes n})_n \,\|\, \mathrm{SEP}\big) = D^{\infty}(\rho\|\mathrm{SEP})$$

[Brandão/Plenio 2010]
[Hayashi/Yamasaki 2024]
[L. 2024]

Some prior results:

- Generalised quantum Stein's lemma → simple IID vs SEP/STAB

$$\mathrm{Stein}\Big((\rho^{\otimes n})_n \,\|\, \mathrm{SEP}\Big) = D^{\infty}(\rho\|\mathrm{SEP})$$

[Brandão/Plenio 2010]
[Hayashi/Yamasaki 2024]
[L. 2024]

- Generalised quantum Sanov theorem → SEP/STAB vs simple IID:

$$\mathrm{Stein}\Big(\mathrm{SEP} \,\|\, (\sigma^{\otimes n})_n\Big) = D(\mathrm{SEP}\|\sigma)$$

[L./Berta/Regula 2026]

Some prior results:

- Generalised quantum Stein's lemma → simple IID vs SEP/STAB

$$\mathrm{Stein}\big((\rho^{\otimes n})_n \,\|\, \mathrm{SEP}\big) = D^\infty(\rho\|\mathrm{SEP})$$

[Brandão/Plenio 2010]
[Hayashi/Yamasaki 2024]
[L. 2024]

- Generalised quantum Sanov theorem → SEP/STAB vs simple IID:

$$\mathrm{Stein}\big(\mathrm{SEP} \,\|\, (\sigma^{\otimes n})_n\big) = D(\mathrm{SEP}\|\sigma)$$

[L./Berta/Regula 2026]

Single-letter!

Last single-letter formula you will see in this talk.

Result	Null hypothesis			Alternative hypothesis		
	Composite	Genuinely correlated	Includes SEP&STAB	Composite	Genuinely correlated	Includes SEP&STAB
Q. Stein's lemma [Hiai/Petz 1991]	N	N	N	N	N	N
Q. Sanov theorem [Bjelakovič et al. 2005], [Noetzel 2014]	Y	N	N	N	N	N
Doubly composite IID [Berta/Brandão/Hirche 2017]	Y	N	N	Y	N	N
Generalised q. Stein's lemma [Hayashi/Yamasaki 2025]	N	N	N	Y	Y	Y
Generalised q. Stein's lemma [L. 2025]	Y	Y	N	Y	Y	Y
Generalised q. Sanov theorem [L./Berta/Regula 2026]	Y	Y	Y	N	N	N
[Fang/Fawzi/Fawzi 2025]	Y	Y	N	Y	Y	N
This talk	Y	Y	Y	Y	N	N

From arXiv:2510.06340

Result	Null hypothesis			Alternative hypothesis		
	Composite	Genuinely correlated	Includes SEP&STAB	Composite	Genuinely correlated	Includes SEP&STAB
Q. Stein's lemma [Hiai/Petz 1991]	N	N	N	N	N	N
Q. Sanov theorem [Bjelakovič et al. 2005], [Noetzel 2014]	Y	N	N	N	N	N
Doubly composite IID [Berta/Brandão/Hirche 2017]	Y	N	N	Y	N	N
Generalised q. Stein's lemma [Hayashi/Yamasaki 2025]	N	N	N	Y	Y	Y
Generalised q. Stein's lemma [L. 2025]	Y	Y	N	Y	Y	Y
Generalised q. Sanov theorem [L./Berta/Regula 2026]	Y	Y	Y	N	N	N
[Fang/Fawzi/Fawzi 2025]	Y	Y	N	Y	Y	N
This talk	Y	Y	Y	Y	N	N

From arXiv:2510.06340

Results

Empirically: composite IID with base set $\mathscr{F}_1 \approx$ AV with base set $\mathrm{conv}(\mathscr{F}_1)$ (e.g. quantum Sanov theorem). Formalisation?

Empirically: composite IID with base set $\mathscr{F}_1 \approx$ AV with base set $\mathrm{conv}(\mathscr{F}_1)$ (e.g. quantum Sanov theorem). Formalisation?

Proposition. $(\mathscr{A}_n)_n$ arbitrary sequence, with $\mathscr{A}_n$ convex & closed under permutations; $\mathscr{B}_1$ closed. Then

$$\mathrm{Stein}\big(\mathscr{A} \,\|\, \mathscr{B}_1^{\mathrm{av}}\big) = \mathrm{Stein}\Big(\mathscr{A} \,\|\, \big(\mathrm{conv}(\mathscr{B}_1)\big)^{\mathrm{iid}}\Big)$$

[**L.** arXiv:2510.06340]

Empirically: composite IID with base set $\mathscr{F}_1 \approx$ AV with base set $\mathrm{conv}(\mathscr{F}_1)$ (e.g. quantum Sanov theorem). Formalisation?

Proposition. $(\mathscr{A}_n)_n$ arbitrary sequence, with $\mathscr{A}_n$ convex & closed under permutations; $\mathscr{B}_1$ closed. Then

$$\mathrm{Stein}\big(\mathscr{A} \,\|\, \mathscr{B}_1^{\mathrm{av}}\big) = \mathrm{Stein}\Big(\mathscr{A} \,\|\, \big(\mathrm{conv}(\mathscr{B}_1)\big)^{\mathrm{iid}}\Big)$$

[**L.** arXiv:2510.06340]

(And same for regularised relative entropy.)

$\Longrightarrow$ Composite IID gets us AV for free (in the alternative hypothesis).

Proof idea. Uniform combination of *k* copies of ρ_1 and *n-k* copies of ρ_2:

$$\Omega_n := \binom{n}{k}^{-1} \sum_{I \subseteq [n]:\, |I|=k} \rho_1^{\otimes I} \otimes \rho_2^{\otimes I^c}$$

Proof idea. Uniform combination of *k* copies of ρ_1 and *n-k* copies of ρ_2:

$$\Omega_n := \binom{n}{k}^{-1} \sum_{I \subseteq [n]:\, |I|=k} \rho_1^{\otimes I} \otimes \rho_2^{\otimes I^c}$$

This is the “most typical” part of

$$\left(\frac{k}{n}\rho_1 + \frac{n-k}{n}\rho_2\right)^{\otimes n}$$

Proof idea. Uniform combination of *k* copies of ρ_1 and *n-k* copies of ρ_2:

$$\Omega_n := \binom{n}{k}^{-1} \sum_{I \subseteq [n]:\, |I|=k} \rho_1^{\otimes I} \otimes \rho_2^{\otimes I^c}$$

This is the "most typical" part of

$$\left(\frac{k}{n}\rho_1 + \frac{n-k}{n}\rho_2\right)^{\otimes n}$$

And indeed, one can compare the two:

$$\Omega_n \leq (n+1)\left(\frac{k}{n}\rho_1 + \frac{n-k}{n}\rho_2\right)^{\otimes n}$$

Proof idea. Uniform combination of k copies of ρ_1 and n-k copies of ρ_2:

$$\Omega_n := \binom{n}{k}^{-1} \sum_{I \subseteq [n]:\, |I|=k} \rho_1^{\otimes I} \otimes \rho_2^{\otimes I^c}$$

This is the “most typical” part of

$$\left(\frac{k}{n}\rho_1 + \frac{n-k}{n}\rho_2\right)^{\otimes n}$$

And indeed, one can compare the two:

$$\Omega_n \leq (n+1)\left(\frac{k}{n}\rho_1 + \frac{n-k}{n}\rho_2\right)^{\otimes n}$$

$\Longrightarrow$ If one can exclude (via a test) the RHS, one can also exclude the LHS.

Proof idea. Uniform combination of *k* copies of ρ_1 and *n-k* copies of ρ_2:

$$\Omega_n := \binom{n}{k}^{-1} \sum_{I \subseteq [n]:\, |I|=k} \rho_1^{\otimes I} \otimes \rho_2^{\otimes I^c}$$

AV + permutational symmetry

This is the "most typical" part of

$$\left(\frac{k}{n}\rho_1 + \frac{n-k}{n}\rho_2\right)^{\otimes n}$$

composite IID

And indeed, one can compare the two:

$$\Omega_n \leq (n+1)\left(\frac{k}{n}\rho_1 + \frac{n-k}{n}\rho_2\right)^{\otimes n}$$

$\Longrightarrow$ If one can exclude (via a test) the RHS, one can also exclude the LHS.

Proof idea. Uniform combination of *k* copies of ρ_1 and *n-k* copies of ρ_2:

$$\Omega_n := \binom{n}{k}^{-1} \sum_{I\subseteq[n]:\,|I|=k} \rho_1^{\otimes I} \otimes \rho_2^{\otimes I^c}$$

AV + permutational symmetry

This is the "most typical" part of

$$\left(\frac{k}{n}\rho_1 + \frac{n-k}{n}\rho_2\right)^{\otimes n}$$

composite IID

And indeed, one can compare the two:

$$\Omega_n \leq (n+1)\left(\frac{k}{n}\rho_1 + \frac{n-k}{n}\rho_2\right)^{\otimes n}$$

$\Longrightarrow$ If one can exclude (via a test) the RHS, one can also exclude the LHS.

(+ discretisation procedure…)

Next: what happens to the generalised quantum Sanov theorem if the alternative hypothesis is composite IID (or AV)?

Next: what happens to the generalised quantum Sanov theorem if the alternative hypothesis is composite IID (or AV)?

Theorem (Generalised quantum Sanov theorem revisited). *Null hypothesis* $\mathcal{A} = \mathrm{SEP}$ *or* $\mathcal{A} = \mathrm{STAB}$*;* $\mathcal{B}_1$ *closed set of states. Then*

$$\mathrm{Stein}\big(\mathcal{A}\,\big\|\,\mathcal{B}_1^{\mathrm{iid}}\big) = \min_{\mu\in\mathcal{P}(\mathcal{B}_1)} \lim_{n\to\infty} \frac{1}{n} \inf_{\rho_n\in\mathcal{A}_n} D\left(\rho_n \,\middle\|\, \int_{\mathcal{B}_1} \mathrm{d}\mu(\sigma_1)\, \sigma_1^{\otimes n}\right),$$

where $\mathcal{P}(\mathcal{B}_1)$ *denotes the set of all probability measures on* $\mathcal{B}_1$*.*

[**L.** arXiv:2510.06340]

Next: what happens to the generalised quantum Sanov theorem if the alternative hypothesis is composite IID (or AV)?

Theorem (Generalised quantum Sanov theorem revisited). *Null hypothesis* $\mathcal{A} = \mathrm{SEP}$ *or* $\mathcal{A} = \mathrm{STAB}$*;* $\mathcal{B}_1$ *closed set of states. Then*

$$\mathrm{Stein}\big(\mathcal{A}\,\big\|\,\mathcal{B}_1^{\mathrm{iid}}\big) = \min_{\mu\in\mathcal{P}(\mathcal{B}_1)} \lim_{n\to\infty} \frac{1}{n} \inf_{\rho_n\in\mathcal{A}_n} D\left(\rho_n \,\middle\|\, \int_{\mathcal{B}_1} \mathrm{d}\mu(\sigma_1)\, \sigma_1^{\otimes n}\right),$$

where $\mathcal{P}(\mathcal{B}_1)$ *denotes the set of all probability measures on* $\mathcal{B}_1$*.*

[**L.** arXiv:2510.06340]

Regularised, not single-letter :-(

Next: what happens to the generalised quantum Sanov theorem if the alternative hypothesis is composite IID (or AV)?

Theorem (Generalised quantum Sanov theorem revisited). *Null hypothesis* $\mathcal{A} = \mathrm{SEP}$ *or* $\mathcal{A} = \mathrm{STAB}$*;* $\mathcal{B}_1$ *closed set of states. Then*

$$\mathrm{Stein}\left(\mathcal{A} \,\middle\|\, \mathcal{B}_1^{\mathrm{iid}}\right) = \min_{\mu \in \mathcal{P}(\mathcal{B}_1)} \lim_{n\to\infty} \frac{1}{n} \inf_{\rho_n \in \mathcal{A}_n} D\left(\rho_n \,\middle\|\, \int_{\mathcal{B}_1} \mathrm{d}\mu(\sigma_1)\, \sigma_1^{\otimes n}\right),$$

where $\mathcal{P}(\mathcal{B}_1)$ *denotes the set of all probability measures on* $\mathcal{B}_1$*.*

[**L.** arXiv:2510.06340]

Regularised, not single-letter :-(

Best we can hope for, even when $\mathscr{A}_n = \{\rho^{\otimes n}\}$ and $\mathscr{B}_1 = \{\sigma_1, \sigma_2\}$!

[Mosonyi/Szilágyi/Weiner 2022]

Next: what happens to the generalised quantum Sanov theorem if the alternative hypothesis is composite IID (or AV)?

Theorem (Generalised quantum Sanov theorem revisited). *Null hypothesis* $\mathcal{A} = \mathrm{SEP}$ *or* $\mathcal{A} = \mathrm{STAB}$*;* $\mathcal{B}_1$ *closed set of states. Then*

$$\mathrm{Stein}\big(\mathcal{A}\,\big\|\,\mathcal{B}_1^{\mathrm{iid}}\big) = \min_{\mu\in\mathcal{P}(\mathcal{B}_1)} \lim_{n\to\infty} \frac{1}{n} \inf_{\rho_n\in\mathcal{A}_n} D\left(\rho_n \,\middle\|\, \int_{\mathcal{B}_1} \mathrm{d}\mu(\sigma_1)\, \sigma_1^{\otimes n}\right),$$

where $\mathcal{P}(\mathcal{B}_1)$ *denotes the set of all probability measures on* $\mathcal{B}_1$*.*

[**L.** arXiv:2510.06340]

Regularised, not single-letter :-(

Best we can hope for, even when $\mathscr{A}_n = \{\rho^{\otimes n}\}$ and $\mathscr{B}_1 = \{\sigma_1, \sigma_2\}$! [Mosonyi/Szilágyi/Weiner 2022]

⟶ improved formula for composite IID vs composite IID/AV! [Berta/Brandão/Hirche 2021]

Proof technique:

1. measure with the “right” measurement (chosen via minimax);
2. lift classical result for achievability;
3. weak converse by relaxing hypothesis testing relative entropy to Umegaki.

Proof technique:

1. measure with the “right” measurement (chosen via minimax);
2. lift classical result for achievability;
3. weak converse by relaxing hypothesis testing relative entropy to Umegaki.

Broadly analogous to [Berta/Brandão/Hirche 2021] and [L./Berta/Regula 2026], but:

Proof technique:

1. measure with the "right" measurement (chosen via minimax);
2. lift classical result for achievability;
3. weak converse by relaxing hypothesis testing relative entropy to Umegaki.

Broadly analogous to [Berta/Brandão/Hirche 2021] and [L./Berta/Regula 2026], but:

We need a classical result that was
not there! Need to go

Proof technique:

1. measure with the "right" measurement (chosen
2. lift classical result for achievability;
3. weak converse by relaxing hypothesis testing r

Broadly analogous to [Berta/Brandão/Hirche 2021] ar

We need a classical result that was
not there! Need to go

Classical setting. Sequence $(\mathscr{F}_n)_n$ of sets of *n*-symbol probability distributions.

Assume that:

- $\exists$ full-support distribution $P_0 \in \mathscr{F}_1$.
- $\mathscr{F}_n$ closed under P_0-depolarising channel action
- ($\mathscr{F}_n$ closed under permutations)

Classical setting. Sequence $(\mathscr{F}_n)_n$ of sets of *n*-symbol probability distributions.

Assume that:

- $\exists$ full-support distribution $P_0 \in \mathscr{F}_1$.
- $\mathscr{F}_n$ closed under P_0-depolarising channel action
- ($\mathscr{F}_n$ closed under permutations)

(replace each symbol with one drawn from P_0 with probability δ, independently)

Then: sequences whose type has large relative entropy distance from $\mathscr{F}$ have exponentially small probability of coming from a probability distribution from $\mathscr{F}$.

Then: sequences whose type has large relative entropy distance from $\mathscr{F}$ have exponentially small probability of coming from a probability distribution from $\mathscr{F}$.

Meta-lemma. $(\mathscr{F}_n)_n$ as before, V an n-type, $Q_n \in \mathscr{F}_n$. Then

$$\Pr_{x^n \sim Q_n}\{x^n \text{ has type } V\} \leq \exp\left[-D(V^{\otimes n} \| \mathscr{F}_n) + o(n)\right]$$

[**L.** arXiv:2510.06342]

Then: sequences whose type has large relative entropy distance from $\mathscr{F}$ have exponentially small probability of coming from a probability distribution from $\mathscr{F}$.

probability distribution such that $nV(x)$ is an integer $\forall\, x$

Meta-lemma. $(\mathscr{F}_n)_n$ as before, V an n-type, $Q_n \in \mathscr{F}_n$. Then

$$\Pr_{x^n \sim Q_n}\{x^n \text{ has type } V\} \leq \exp\left[-D(V^{\otimes n} \| \mathscr{F}_n) + o(n)\right]$$

$\forall\, x$, symbol x appears in x^n exactly $nV(x)$ times

[**L.** arXiv:2510.06342]

Then: sequences whose type has large relative entropy distance from $\mathscr{F}$ have exponentially small probability of coming from a probability distribution from $\mathscr{F}$.

probability distribution such that $nV(x)$ is an integer $\forall\, x$

Meta-lemma. $(\mathscr{F}_n)_n$ as before, V an n-type, $Q_n \in \mathscr{F}_n$. Then

$$\Pr_{x^n \sim Q_n}\{x^n \text{ has type } V\} \leq \exp\left[-D(V^{\otimes n} \| \mathscr{F}_n) + o(n)\right]$$

$\forall\, x$, symbol x appears in x^n exactly $nV(x)$ times

[**L.** arXiv:2510.06342]

Proved via simpler variation of the blurring technique, called symbol-by-symbol blurring.

Then: sequences whose type has large relative entropy distance from $\mathscr{F}$ have exponentially small probability of coming from a probability distribution from $\mathscr{F}$.

probability distribution such that $nV(x)$ is an integer $\forall\, x$

Meta-lemma. $(\mathscr{F}_n)_n$ as before, V an n-type, $Q_n \in \mathscr{F}_n$. Then

$$\Pr_{x^n \sim Q_n}\{x^n \text{ has type } V\} \leq \exp\left[-D(V^{\otimes n} \| \mathscr{F}_n) + o(n)\right]$$

$\forall\, x$, symbol x appears in x^n exactly $nV(x)$ times

[**L.** arXiv:2510.06342]

Proved via simpler variation of the blurring technique, called symbol-by-symbol blurring.

$\Longrightarrow$ nice classical Chernoff-Stein lemma that we can then lift to quantum!

$\Longrightarrow$ Classical constrained de Finetti reduction theorem: if $Q_n \in \mathscr{F}_n$ perm. symm.,

$$Q_n \leq \int \mathrm{d}P \, \exp\left[-D(P^{\otimes n} \| \mathscr{F}_n) + o(n)\right] \, P^{\otimes n}$$

see also [Duan/Severini/Winter 2016],
[Lancien/Winter 2017]

$\Longrightarrow$ Classical constrained de Finetti reduction theorem: if $Q_n \in \mathscr{F}_n$ perm. symm.,

$$Q_n \leq \int \mathrm{d}P \, \exp\left[-D(P^{\otimes n} \| \mathscr{F}_n) + o(n)\right] \, P^{\otimes n}$$

see also [Duan/Severini/Winter 2016], [Lancien/Winter 2017]

Conjecture. For all permutationally symmetric separable states $\sigma_{A^nB^n}$,

$$\sigma_{A^nB^n} \leq \int \mathrm{d}\omega_{AB} \, \exp\left[-nD^{\infty}(\omega \| \mathrm{SEP}) + o(n)\right] \omega_{AB}^{\otimes n}$$

Summary

- Regularised formulas for Stein exponents of very general hypotheses vs composite IID/AV
- $\Longrightarrow$ Generalised quantum Sanov theorem "revisited"
- Alternative hypothesis: AV = composite IID + convex hull
- We need better classical results!
- Meta-lemma as a new unifying framework for dealing with (classical?) problems

Summary

- Regularised formulas for Stein exponents of very general hypotheses vs composite IID/AV
- $\Longrightarrow$ Generalised quantum Sanov theorem "revisited"
- Alternative hypothesis: AV = composite IID + convex hull
- We need better classical results!
- Meta-lemma as a new unifying framework for dealing with (classical?) problems

Thank you!