# A mathematical foundation for self-testing: Lifting common assumptions

Pedro Baptista, Ranyiliu Chen, Jędrzej Kaniewski, David R. Lolck,
Laura Mančinska, Thor G. Nielsen, Simon Schmidt

13th Dec. 2023, HIT

arXiv: 2310.12662

# Content

Backgrounds

- Bell scenario, correlation, and self-testing
- common assumptions in self-testing

Main Result

- when we can/cannot remove those assumptions
- a special correlation without any full-rank PVM realization

A viewpoint from operator algebra

- correlation by C* algebra
- self-testing by C* algebra

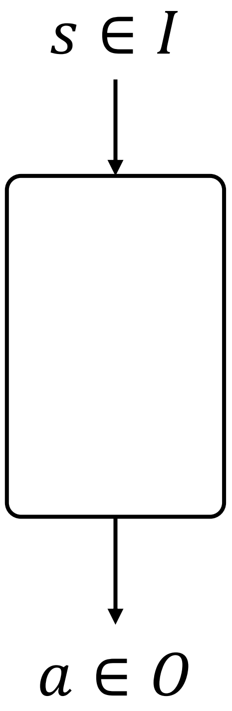
Q & A

# Background

## Bell scenario, correlation, and self-testing

# Bell scenario, correlation, and self-testing

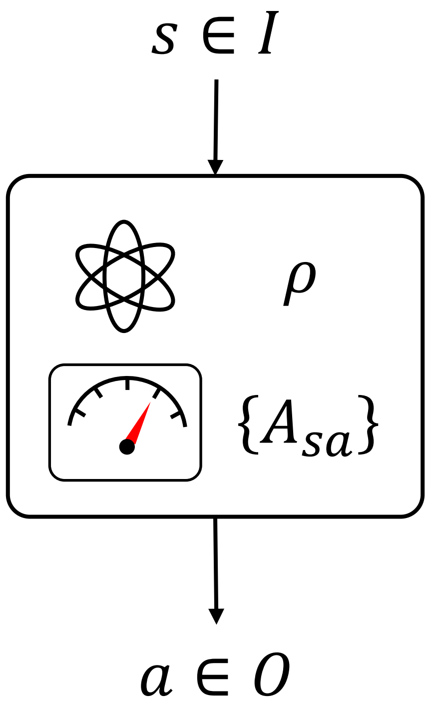
A (interactive) box:




repeat many times $\Longrightarrow p(a|s)$

# Bell scenario, correlation, and self-testing

A quantum box:

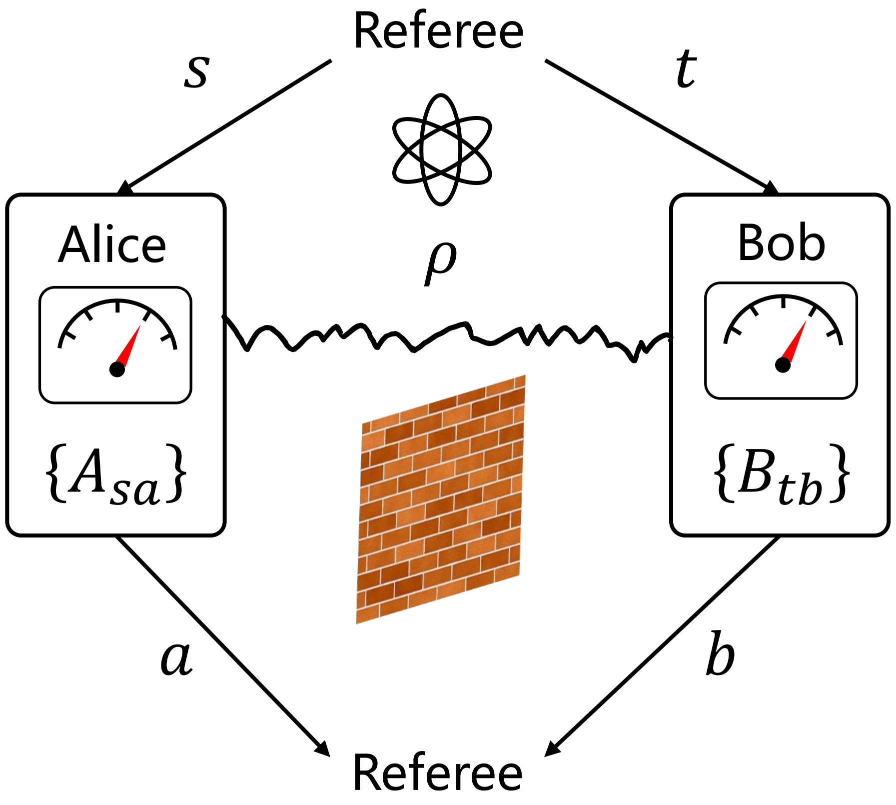



Quantum mechanism:

- $\rho \in B(H), \rho \succcurlyeq 0, \mathrm{Tr}[\rho] = 1$
- $A_{sa} \in B(H), A_{sa} \succcurlyeq 0, \sum_a A_{sa} = \mathrm{id}$
- $p(a|s) = \mathrm{Tr}[A_{sa}\rho]$

# Bell scenario, correlation, and self-testing

Bell scenario:

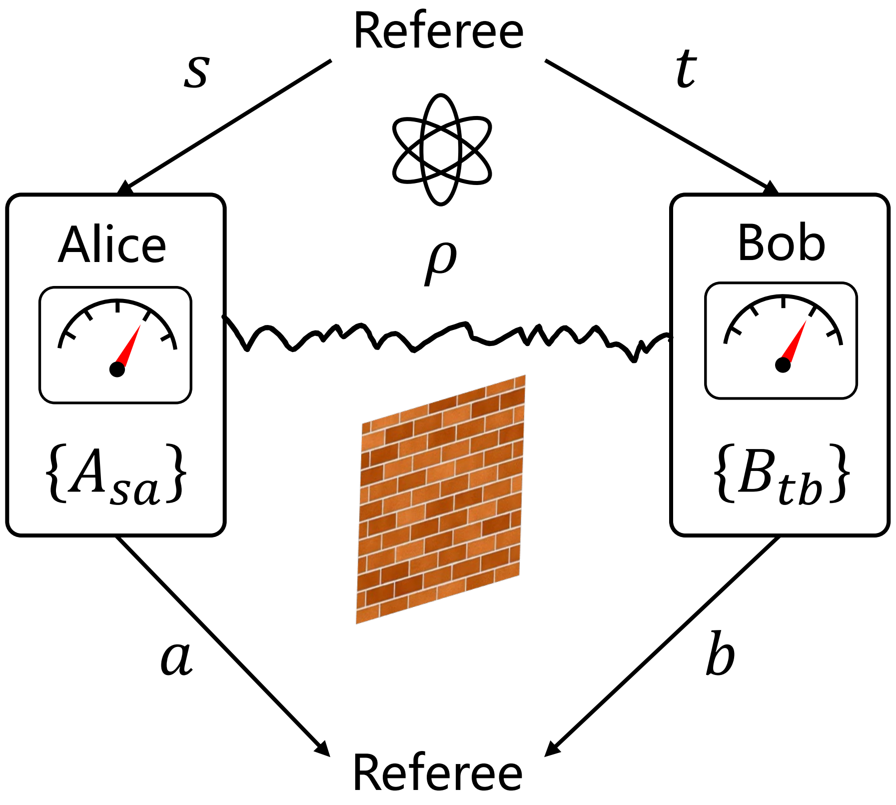



Quantum mechanism:

- $\rho \in B(H_A \otimes H_B)$

# Bell scenario, correlation, and self-testing

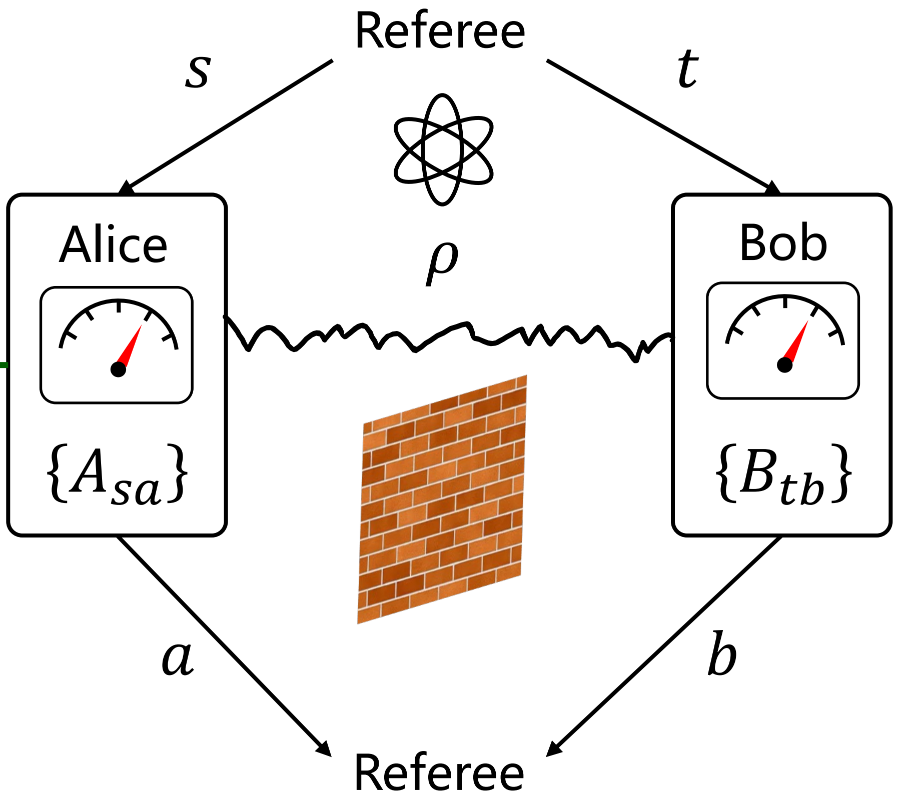
Bell scenario:




$$p(a,b|s,t) = \mathrm{Tr}[A_{sa} \otimes B_{tb} \rho]$$

# Bell scenario, correlation, and self-testing

Bell scenario:



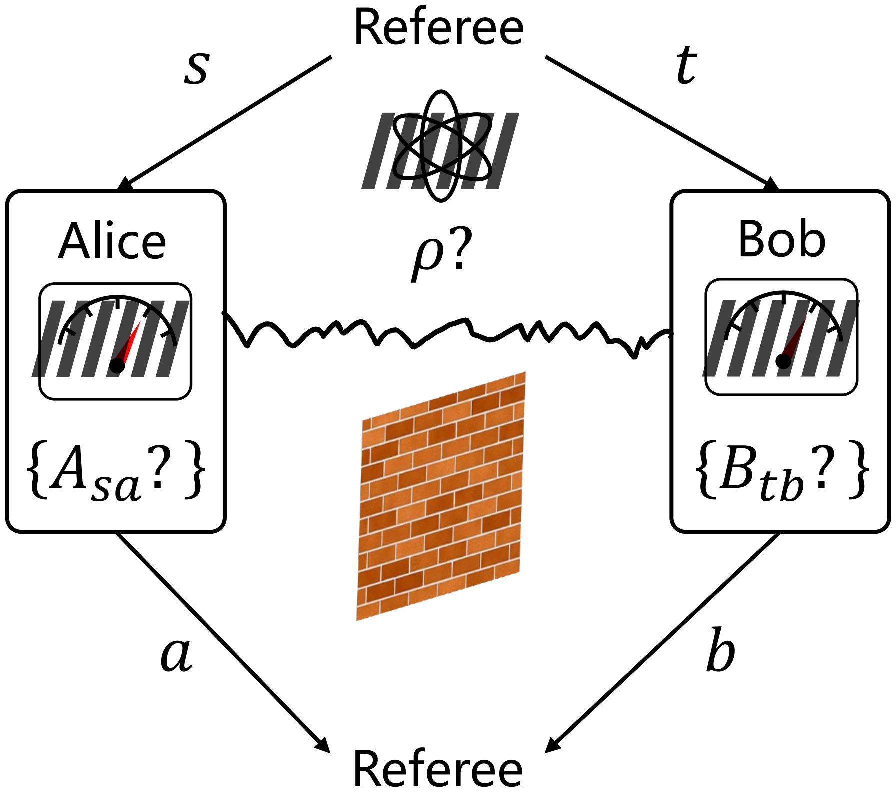

$$p(a,b|s,t) = \mathrm{Tr}[A_{sa} \otimes B_{tb} \rho]$$

strategy:

$S = (\rho, \{A_{sa}\}, \{B_{tb}\})$

It is known that some statistics (correlation) cannot be produced by classical mechanics!

# Bell scenario, correlation, and self-testing




$$p(a,b|s,t) \overset{?}{\Rightarrow} (\rho, \{A_{sa}\}, \{B_{tb}\})$$

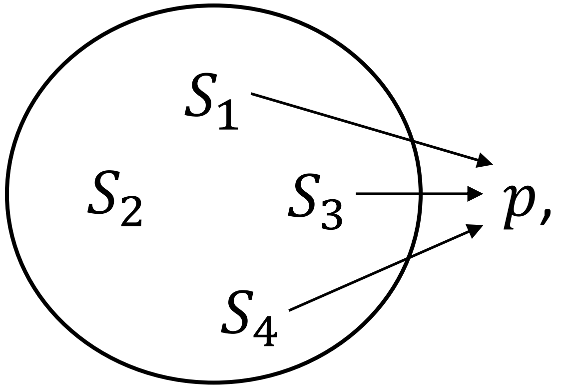
Inverse question:

Can $p(a,b|s,t)$ induce $S = (\rho, \{A_{sa}\}, \{B_{tb}\})$?

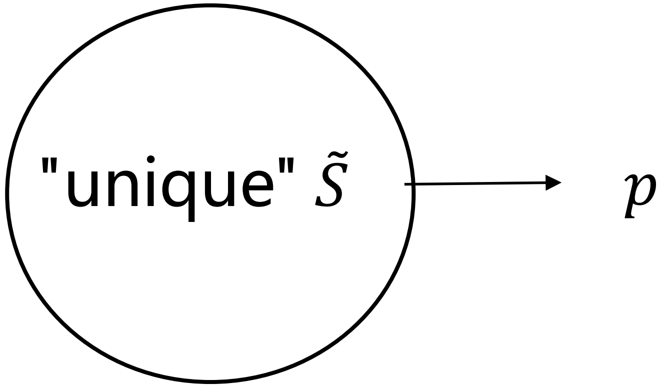
**<u>Self-testing</u>:** there is a 'unique' strategy that produces

$$p(a,b|s,t).$$

# Bell scenario, correlation, and self-testing




but we want

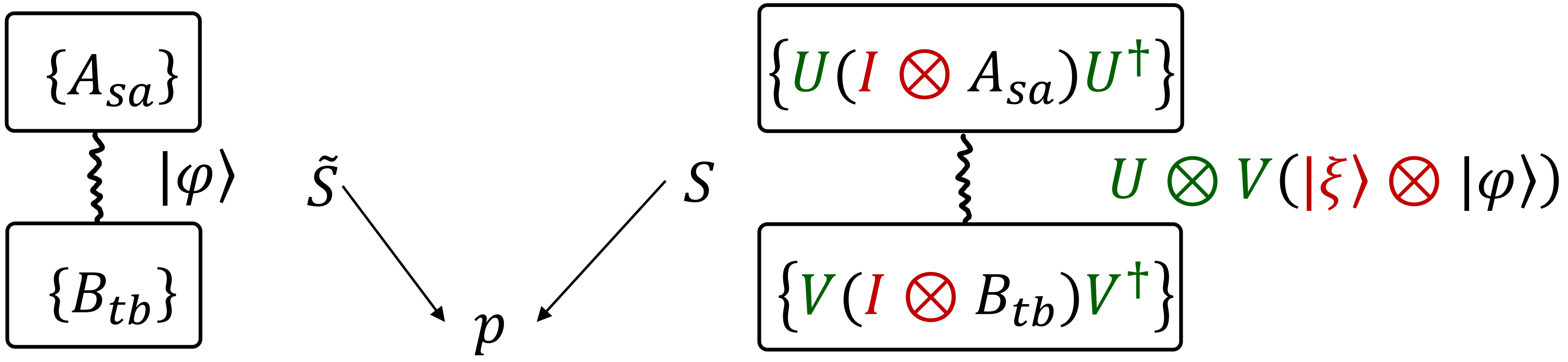



Unique up to …

# Bell scenario, correlation, and self-testing

Unique up to …

trivial auxiliary state + change of local bases:



# Bell scenario, correlation, and self-testing

Unique up to …

trivial auxiliary state + change of local bases:

$$\boxed{\{A_{sa}\}} \quad |\varphi\rangle \quad \boxed{\{B_{tb}\}}$$

$$\begin{tikzcd} \tilde{S} \arrow[dr] & \hookleftarrow & S \arrow[dl] \\ & p & \end{tikzcd}$$

$$\boxed{\{U(I \otimes A_{sa})U^{\dagger}\}} \quad U \otimes V(|\xi\rangle \otimes |\varphi\rangle) \quad \boxed{\{V(I \otimes B_{tb})V^{\dagger}\}}$$

We say $\tilde{S}$ is a local dilation of $S$, denote by $S \hookrightarrow \tilde{S}$.

# Bell scenario, correlation, and self-testing

Unique up to ...

trivial auxiliary state + change of local bases:

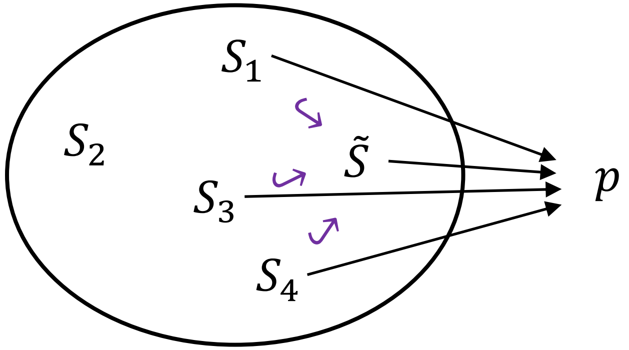
**Local dilation:** $S \hookrightarrow \tilde{S}$ if there is local isometry $V = V_A \otimes V_B$ and auxiliary state $\sigma_{\text{aux}}$ such that

$$V(A_{sa} \otimes B_{tb})\rho V^* = (\tilde{A}_{sa} \otimes \tilde{B}_{tb})\tilde{\rho} \otimes \sigma_{\text{aux}}$$

holds for all $a, b, s, t$.

# Bell scenario, correlation, and self-testing

Best one can hope for: $\tilde{S}$ is a local-dilation of any $S$ generating $p$.




**Definition (self-testing):**

A correlation $p$ is a self-test for $\tilde{S}$, if for any strategy $S$ generating $p$, there exists local isometry and auxiliary state such that $S \hookrightarrow \tilde{S}$.

# Background

## Assumptions in self-testing

# Assumptions in self-testing

**Definition (self-testing):**

A correlation $p$ is a self-test for $\tilde{S}$, if for any strategy $S$ generating $p$, there exists local isometry and auxiliary state such that $S \hookrightarrow \tilde{S}$.

In most of the existing results, some of these assumptions are made for $S$:

- the shared state, $\rho$, is pure, i.e., $\rho = |\varphi\rangle\langle\varphi|, |\varphi\rangle \in H_A \otimes H_B$
- the shared state is full-rank, i.e., $\mathrm{rank}(\rho_A) = \dim H_A$, $\mathrm{rank}(\rho_B) = \dim H_B$
- the measurements $\{A_{sa}\}, \{B_{tb}\}$ are PVMs, i.e., $A_{s}$

E.g., $\frac{|00\rangle+|11\rangle}{\sqrt{2}} \in \mathbb{C}^2 \otimes \mathbb{C}^2$ is full-rank, while $\frac{|00\rangle+|11\rangle}{\sqrt{2}} \in \mathbb{C}^2 \otimes \mathbb{C}^3$ is not.

# Assumptions in self-testing

**Definition (self-testing):**

A correlation $p$ is a self-test for $\tilde{S}$, if for any strategy $S$ generating $p$, there exists local isometry and auxiliary state such that $S \hookrightarrow \tilde{S}$.

In most of the existing results, some of these assumptions are made for $S$:

- the shared state, $\rho$, is pure, i.e., $\rho = |\varphi\rangle\langle\varphi|, |\varphi\rangle \in H_A \otimes H_B$
- the shared state is full-rank, i.e., $\mathrm{rank}(\rho_A) = \dim H_A$, $\mathrm{rank}(\rho_B) = \dim H_B$
- the measurements $\{A_{sa}\}, \{B_{tb}\}$ are PVMs, i.e., $A_{sa}$ and $B_{tb}$ are projections

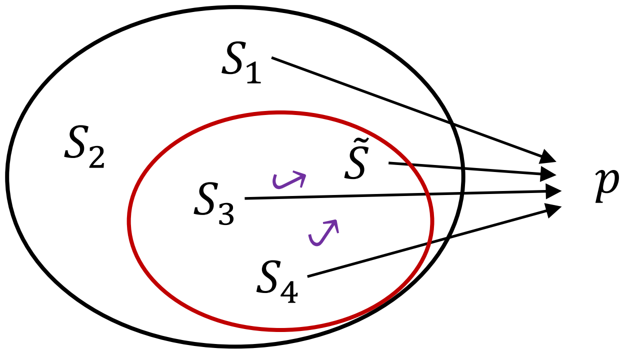
# Assumptions in self-testing

**Definition (self-testing):**

A correlation $p$ is a self-test for $\tilde{S}$, if for any strategy $S$ generating $p$, there exists local isometry and auxiliary state such that $S \hookrightarrow \tilde{S}$.

In most of the existing results, some of these assumptions are made for $S$.

Making assumptions =



# Assumptions in self-testing

Why we want to remove those assumptions?

- A purely math reason: it weakens the self-testing statements.

# Assumptions in self-testing

## Why we want to remove those assumptions?

- A purely math reason: it weakens the self-testing statements.
- Examples:

Perfectly correlated correlation:

$$p(00) + p(11) = 1$$

- If assume purity, then state must be entangled.
- But the correlation is classical!

# Assumptions in self-testing

Why we want to remove those assumptions?

- A purely math reason: it weakens the self-testing statements.
- Examples:

Perfectly correlated correlation:

$$p(00) + p(11) = 1$$

- If assume purity, then state must be entangled.
- But the correlation is classical!

In DI-RNG:

- Unpredictable by any third party
- If assume purity, then third party can never entangle a pure state, thus it is already unpredictable!

# Assumptions in self-testing

Why we want to remove those assumptions?

- A purely math reason: it weakens the self-testing statements.
- Examples
- A philosophical reason: it goes against the idea of self-testing: making **minimal** assumptions.

# Assumptions in self-testing

Why we want to remove those assumptions?

- A purely math reason: it weakens the self-testing statements.
- Examples
- A philosophical reason: it goes against the idea of self-testing: making **minimal** assumptions.

Main result: in most cases, we can remove those assumptions safely!

# Main result

## Lifting Assumptions

# Lifting Assumptions

Let $t \subseteq \{\text{pure}, \text{full rank}, \text{PVM}\}$.

**Definition ($t$-self-testing):**

A correlation $p$ is a $t$-self-test for $\tilde{S}$, if for any $t$ strategy $S$ generating $p$, there exists local isometry and auxiliary state such that $S \hookrightarrow \tilde{S}$.

- Clearly, if $t \subseteq t'$, then $t$-self-test $\Longrightarrow$ $t$'-self-test.
- Removing assumption = promoting self-test
- If $t = \emptyset$, we call it an **assumption-free** self-test.

# Lifting Assumptions

**Theorem A (Main Result):**

Let $p$ be a correlation. Let $\tilde{S}$ be a 'nice' strategy for $p$.

(a) If $p$ is a {pure PVM}-self-test for $\tilde{S}$,

then $p$ is an assumption-free self-test for $\tilde{S}$.

(b) If $p$ is a {pure full-rank}-self-test for $\tilde{S}$,

then $p$ is an assumption-free self-test for $\tilde{S}$.

'nice' = pure, full-rank, PVM

# Lifting Assumptions

## Theorem A (Main Result):

$$
\begin{tikzcd}
\{\text{pure PVM}\}\text{-self-test} \arrow[dr, "\textcircled{1}"] & & \\
& \{\text{pure}\}\text{-self-test} \arrow[r, "\textcircled{3}"] & \text{assumption-free self-test} \\
\{\text{pure full-rank}\}\text{-self-test} \arrow[ur, "\textcircled{2}"'] & &
\end{tikzcd}
$$

# Lifting Assumptions

**Theorem A (Main Result):**

$$
\begin{tikzcd}
\{\text{pure PVM}\}\text{-self-test} \arrow[dr, "\textcircled{1}"] & & \\
& \{\text{pure}\}\text{-self-test} \arrow[r, "\textcircled{3}"] & \text{assumption-free self-test} \\
\{\text{pure full-rank}\}\text{-self-test} \arrow[ur, "\textcircled{2}"'] & &
\end{tikzcd}
$$

① + ③ = (a), ② + ③ = (b)

# Lifting Assumptions

**Theorem A (Main Result):**

$$
\begin{tikzcd}
& \{\text{pure PVM}\}\text{-self-test} \arrow[dr, "\textcircled{1}"] & & \\
\{\text{pure full-rank PVM}\}\text{-self-test} \arrow[ur, "?"] \arrow[dr, "?"'] & & \{\text{pure}\}\text{-self-test} \arrow[r, "\textcircled{3}"] & \text{assumption-free self-test} \\
& \{\text{pure full-rank}\}\text{-self-test} \arrow[ur, "\textcircled{2}"'] & &
\end{tikzcd}
$$

? <u>Conjecture</u>: Negative

# Lifting Assumptions

**Theorem B:**

Let $p$ be a correlation that is an assumption-free self-test for some strategy $\tilde{S}$. Then $\tilde{S}$ must be PVM on its support.

In other words, if $\tilde{S}$ is full-rank but non-projective, then it cannot be self-tested in an assumption-free way.

# Main result

## Correlation without any full-rank PVM realization

# Correlation without any full-rank PVM realization

Recall: the canonical strategy for CHSH inequality:

$$\tilde{S}_{\mathrm{CHSH}} = (|\mathrm{EPR}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \{X, Z\}, \{H := \frac{X+Z}{\sqrt{2}}, G := \frac{X-Z}{\sqrt{2}}\})$$

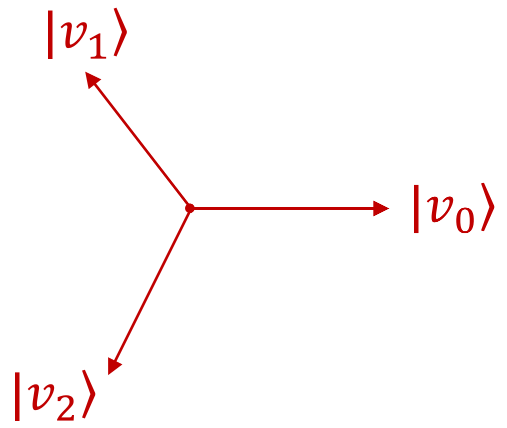
# Correlation without any full-rank PVM realization

Recall: the canonical strategy for CHSH game:

$$\tilde{S}_{\mathrm{CHSH}} = (|\mathrm{EPR}\rangle, \{X, Z\}, \{H, G\})$$

Consider the following 3-outcome non-PVM measurement $M = \{M_0, M_1, M_2\}$:

$$\begin{cases} M_0 = \frac{1}{3}(I + Z) \\ M_1 = \frac{1}{3}(I - \frac{1}{2}Z + \frac{\sqrt{3}}{2}X) \\ M_2 = \frac{1}{3}(I - \frac{1}{2}Z - \frac{\sqrt{3}}{2}X) \end{cases} \Leftrightarrow \quad M_i = \frac{2}{3}|v_i\rangle\langle v_i|$$



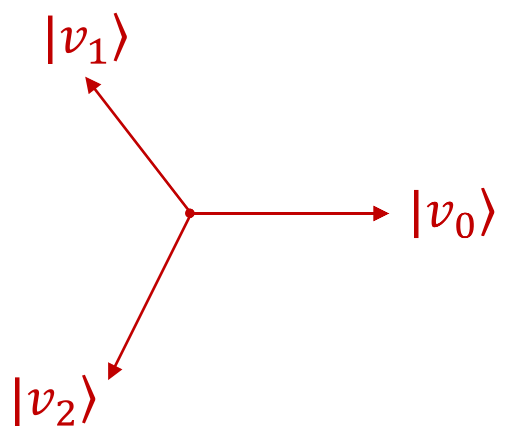
# Correlation without any full-rank PVM realization

Now, define

$$\tilde{S} = (|\mathrm{EPR}\rangle, \{X, Z\}, \{H, G, M\})$$

Consider the following 3-outcome non-PVM measurement $M = \{M_0, M_1, M_2\}$:

$$\begin{cases} M_0 = \frac{1}{3}(I + Z) \\ M_1 = \frac{1}{3}(I - \frac{1}{2}Z + \frac{\sqrt{3}}{2}X) \\ M_2 = \frac{1}{3}(I - \frac{1}{2}Z - \frac{\sqrt{3}}{2}X) \end{cases} \iff M_i = \frac{2}{3}|v_i\rangle\langle v_i|$$



# Correlation without any full-rank PVM realization

Now, define

$$\tilde{S} = (|\mathrm{EPR}\rangle, \{X, Z\}, \{H, G, M\})$$

Then $p_{\tilde{S}} \in C_q(2,3,2,3)$.

<u>Note</u>: $p_{\tilde{S}}$ cannot be an assumption-free self-test for $\tilde{S}$ by Theorem B.

# Correlation without any full-rank PVM realization

**Theorem C:**

Correlation $p_{\tilde{S}}$ satisfies the following:

(a) $p_{\tilde{S}}$ is extreme in $C_q(2,3,2,3)$.

(b) $p_{\tilde{S}}$ {pure, full-rank}-self-tests $\tilde{S}$.

(c) $p_{\tilde{S}}$ {pure, PVM}-self-tests any Naimark dilation of $\tilde{S}$.

# Correlation without any full-rank PVM realization

**Theorem C:**

Correlation $p_{\tilde{S}}$ satisfies the following:

(a) $p_{\tilde{S}}$ is extreme in $C_q(2,3,2,3)$.

(b) $p_{\tilde{S}}$ {pure, full-rank}-self-tests $\tilde{S}$.

(c) $p_{\tilde{S}}$ {pure, PVM}-self-tests any Naimark dilation of $\tilde{S}$.

**Implications:**

- In Theorem A, the condition of $\tilde{S}$ being 'nice' is crucial.
- $p_{\tilde{S}}$ admits no pure full-rank PVM realization.

# Wrap-up:

**Theorem A in short:**

If our $\tilde{S}$ is 'nice', then we may safely remove many assumptions.

**Theorem B in short:**

If our $\tilde{S}$ is not 'nice', then the best we can hope for is a self-test with assumptions (we will never get an assumption-free one).

**Theorem C in short:**

There is a correlation cannot be produced by any 'nice' strategy.

# A viewpoint from operator algebra

# Correlation by different quantum models

Fix $I, O$, let $C_q(|I|,|O|)$ be the set of all (quantum) correlation with $|I|$ inputs and $|O|$ outputs:

$$C_q(|I|,|O|) = \{p \mid p(a,b|s,t) = \mathrm{Tr}[A_{sa} \otimes B_{tb} \rho] \text{ for some } (\rho, \{A_{sa}\}, \{B_{tb}\})\}$$

$$\subseteq \mathbb{R}^{|I|^2 \times |O|^2}$$

# Correlation by different quantum models

Fix $I, O$, let $C_q(|I|, |O|)$ be the set of all (quantum) correlation with $|I|$ inputs and $|O|$ outputs.

Similarly, we can define

- $C_c(|I|, |O|)$, the set of classical correlation.
- $C_{qa}(|I|, |O|)$, (the closure of) the set of infinite dim. quantum correlation.
- $C_{qc}(|I|, |O|)$, the set of quantum commuting correlation.

Quantum commuting strategies: $p(a, b|s, t) = \langle\varphi|A_{sa}B_{tb}|\varphi\rangle, [A_{sa}, B_{tb}] = 0.$

# Correlation by different quantum models

Fix $I, O$, let $C_q(|I|, |O|)$ be the set of all (quantum) correlation with $|I|$ inputs and $|O|$ outputs.

Similarly, we can define

- $C_c(|I|, |O|)$, the set of classical correlation.
- $C_{qa}(|I|, |O|)$, (the closure of) the set of infinite dim. quantum correlation.
- $C_{qc}(|I|, |O|)$, the set of quantum commuting correlation.

$$C_c \subseteq C_q \subseteq C_{qa} \subseteq C_{qc}$$

# Characterize correlation by C* algebra

Fix $I, O$, let $C_q(|I|, |O|)$ be the set of all (quantum) correlation with $|I|$ inputs and $|O|$ outputs.

Let

$$\mathcal{A} \coloneqq C^* \left\langle e_{sa} | e_{sa} = e_{sa}^2, \sum\nolimits_a e_{sa} = 1 \right\rangle$$

$$\mathcal{B} \coloneqq C^* \left\langle f_{tb} | f_{tb} = f_{tb}^2, \sum\nolimits_b f_{tb} = 1 \right\rangle$$

# Characterize correlation by C* algebra

Fix $I, O$, let $C_q(|I|, |O|)$ be the set of all (quantum) correlation with $|I|$ inputs and $|O|$ outputs.

In 2011, [1] showed that:

**Theorem (correlation by C* algebra):**

Let $p$ be a correlation in $\mathbb{R}^{|I|^2 \times |O|^2}$. Then

$$p \in C_q(|I|, |O|)$$

$$\Longleftrightarrow$$

$$\exists \text{ finite dim. } \varphi \text{ on } \mathcal{A} \otimes_{\min} \mathcal{B} \text{ s.t. } \varphi(e_{sa} \otimes f_{tb}) = p(a, b|s, t)$$

[1] M. Junge, M. Navascues, C. Palazuelos, et al. Connes' embedding problem and Tsirelson's problem. Journal of Math. Phy., 52(1):012102, Jan 2011.

# Characterize correlation by C* algebra

Fix $I, O$, let $C_{qa}(|I|,|O|)$ be (the closure of) the set of infinite dim. quantum correlation with $|I|$ inputs and $|O|$ outputs.

In 2011, [1] showed that:

**Theorem (correlation by C* algebra):**

Let $p$ be a correlation in $\mathbb{R}^{|I|^2\times|O|^2}$. Then

$$p \in C_{qa}(|I|,|O|)$$

$$\Longleftrightarrow$$

$$\exists\ \cancel{\text{finite dim.}}\ \varphi \text{ on } \mathcal{A}\otimes_{\min}\mathcal{B} \text{ s.t. } \varphi(e_{sa}\otimes f_{tb}) = p(a,b|s,t)$$

[1] M. Junge, M. Navascues, C. Palazuelos, et al. Connes' embedding problem and Tsirelson's problem. Journal of Math. Phy., 52(1):012102, Jan 2011.

# Characterize correlation by C* algebra

Fix $I, O$, let $C_{qc}(|I|,|O|)$ be the set of quantum commuting correlation with $|I|$ inputs and $|O|$ outputs.

In 2011, [1] showed that:

**Theorem (correlation by C* algebra):**

Let $p$ be a correlation in $\mathbb{R}^{|I|^2\times|O|^2}$. Then

$$p \in C_{qc}(|I|,|O|)$$

$$\Longleftrightarrow$$

$$\exists\ \cancel{\text{finite dim.}}\ \varphi \text{ on } \mathcal{A}\otimes_{\max}\mathcal{B} \text{ s.t. } \varphi(e_{sa}\otimes f_{tb}) = p(a,b|s,t)$$

[1] M. Junge, M. Navascues, C. Palazuelos, et al. Connes' embedding problem and Tsirelson's problem. Journal of Math. Phy., 52(1):012102, Jan 2011.

# Characterize self-testing by C* algebra

Fix $I, O$, let $C_q(|I|, |O|)$ be the set of all (quantum) correlation with $|I|$ inputs and $|O|$ outputs.

In 2023, [2] showed that:

**Theorem (self-testing by C* algebra):**

Let $p$ be a correlation in $\mathbb{R}^{|I|^2 \times |O|^2}$. Then

$$p \text{ is a self\_test}$$

$$\Longleftrightarrow$$

$$\exists! \text{ finite dim. } \varphi \text{ on } \mathcal{A} \otimes_{\min} \mathcal{B} \text{ s.t. } \varphi(e_{sa} \otimes f_{tb}) = p(a, b|s, t)$$

[2] C. Paddock, W. Slofstra, Y. Zhao, et al. An operator-algebraic formulation of self-testing. Annales Henri Poincaré, 2023.

# Characterize self-testing by C* algebra

Then [2] did similar generalization to other quantum models.

Future work after [2]:

- self-testing in quantum commuting model: quite unexplored
- robustness of self-testing
- geometrical properties of quantum correlation, e.g., extreme/exposed points in $C_q$

[2] C. Paddock, W. Slofstra, Y. Zhao, et al. An operator-algebraic formulation of self-testing. Annales Henri Poincaré, 2023.

# Thanks!

A mathematical foundation for self-testing:

Lifting common assumptions

arXiv: 2310.12662