Self-testing in a prepare-measure scenario sans assuming quantum dimension

Souradeep Sasmal

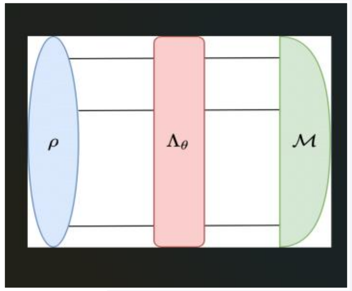
Quantum Algorithm and Resource Theory Group, IFFS, UESTC, Chengdu, China

2025-12-09

Characterisation of Quantum Devices

- **Device Dependent**

User trust the preparation and measurement devices.



Parameter Estimation,

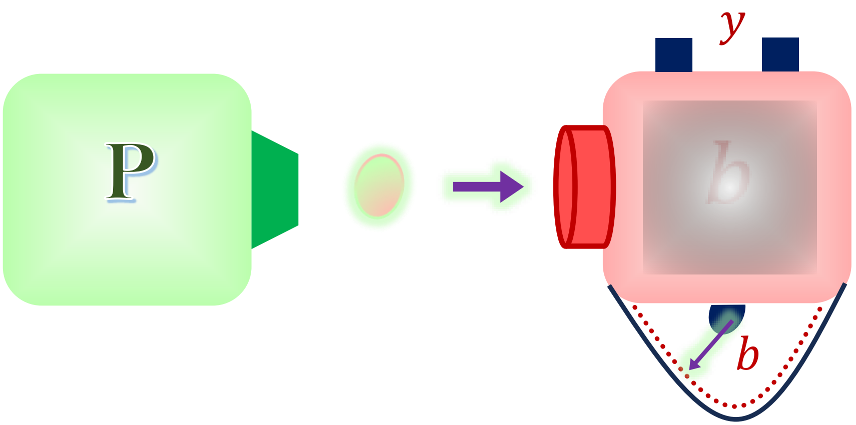
Tomography

- **Device Independent**

User does not trust the preparation or measurement devices. User can only charecterise the input-output statistics through a probability distribution $p(input|output)$

Self-Testing

Self-Testing

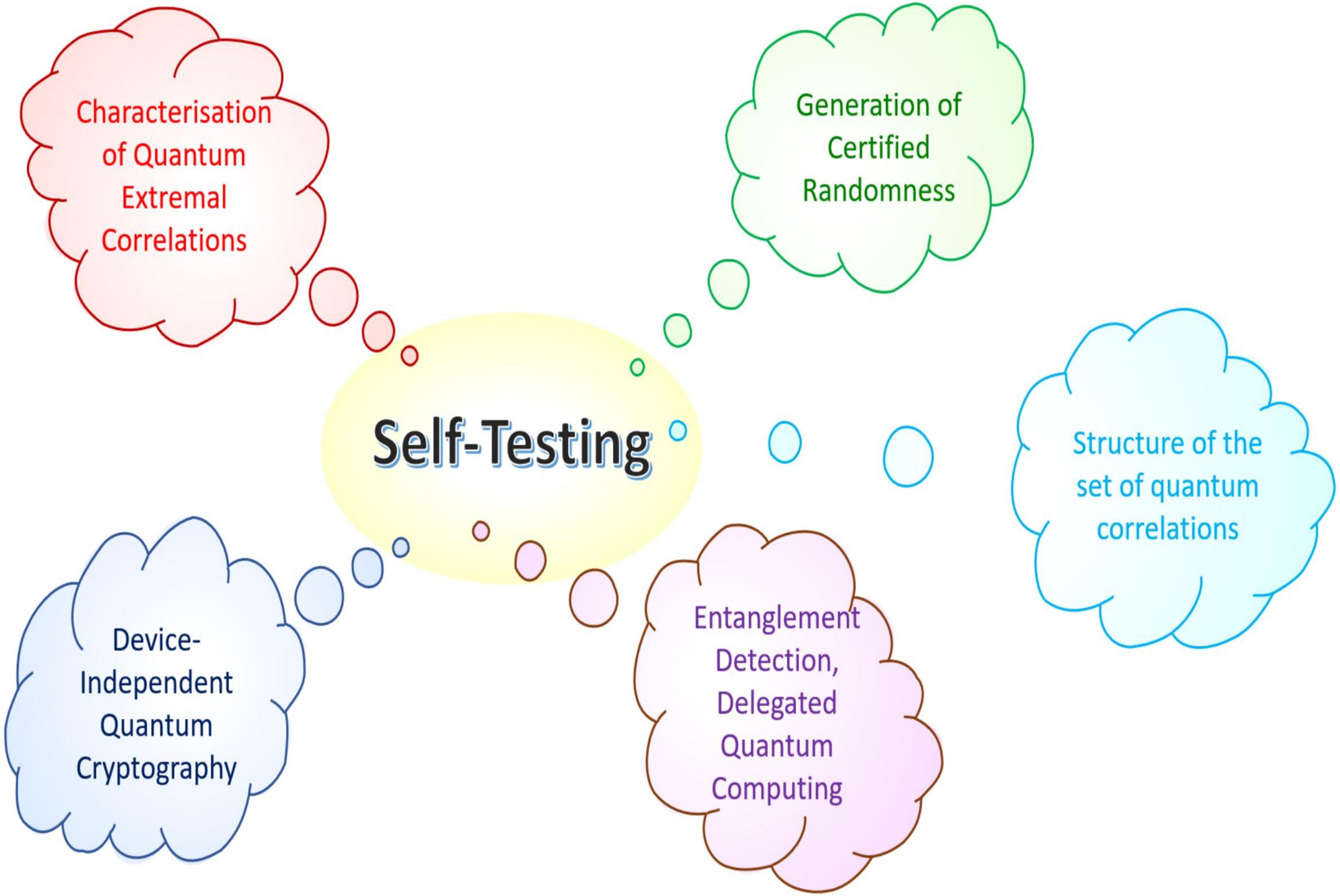


$\vec{P} \equiv \{p(b|y,P)\}$

- The ability of a classical verifier to completely characterise the working of the device by *only* considering the observed input-output statistics.
- Quantum Device: $\{\rho, \{M_{b|y}\}\}$
- A behaviour $\vec{P}_*$ self tests a quantum strategy, *iff*, that is the *only* strategy attaining $\vec{P}_*$.

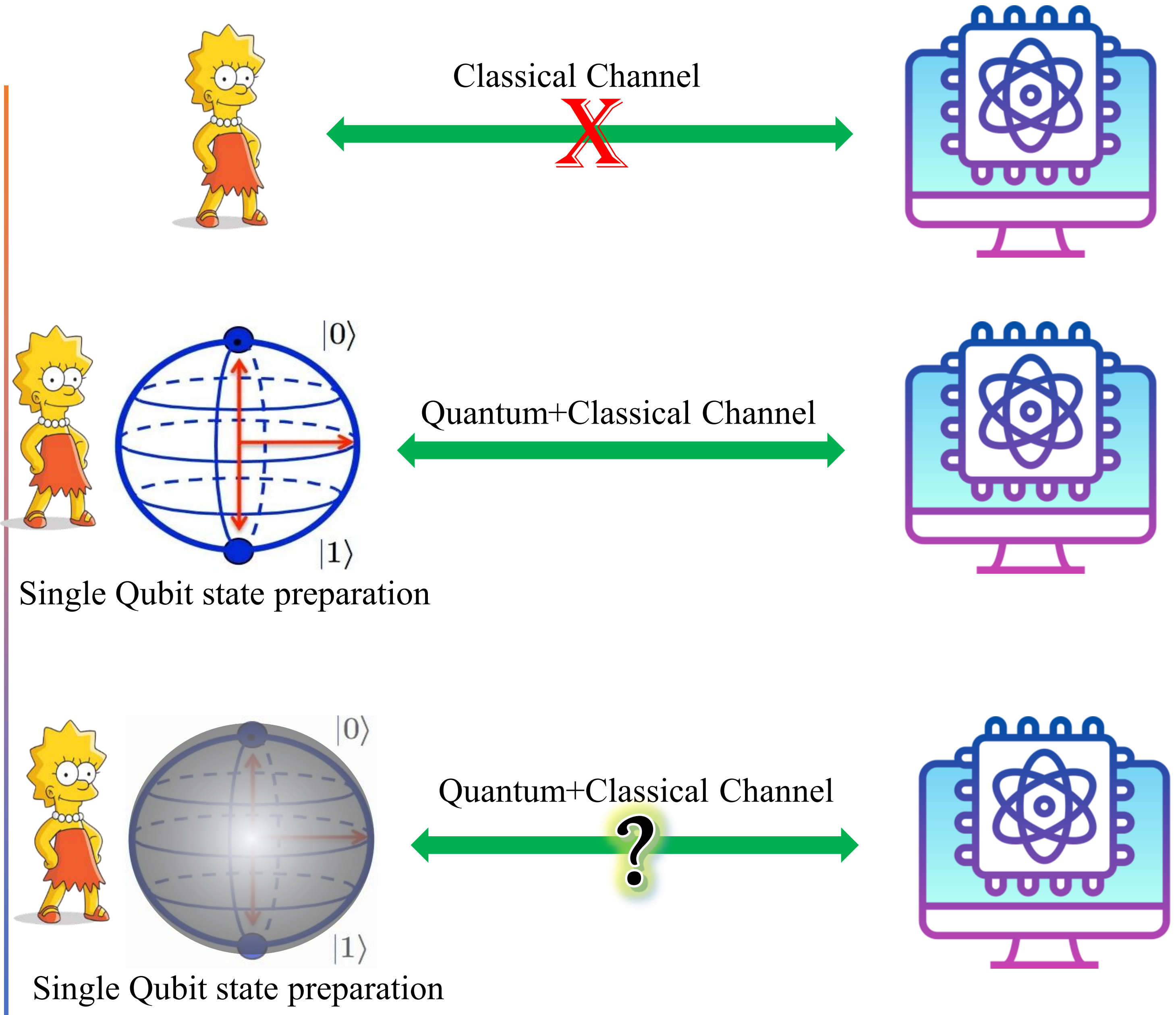
Self-Testing

Why it is important?



Why it is important?

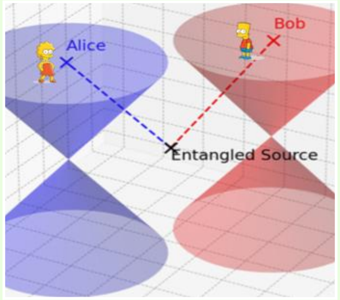
DI-VBQC



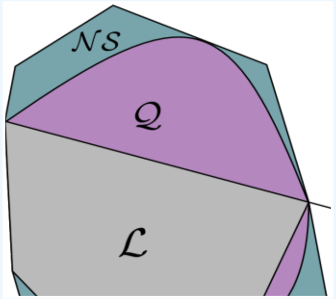
Motivation: Certification Beyond Bell Tests

- Why Prepare – Measure

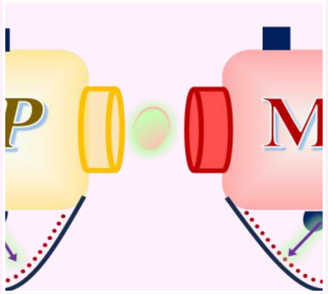
  Self-testing?



Bell Self-testing: DI, but experimentally demanding.



Geometry of Quantum Correlations

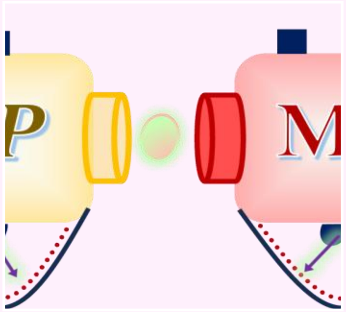


Prepare-Measure Correlations: Simpler, require upper bound on dimension.

(Contextuality, quasi-probability)

Motivation: Certification Beyond Bell Tests

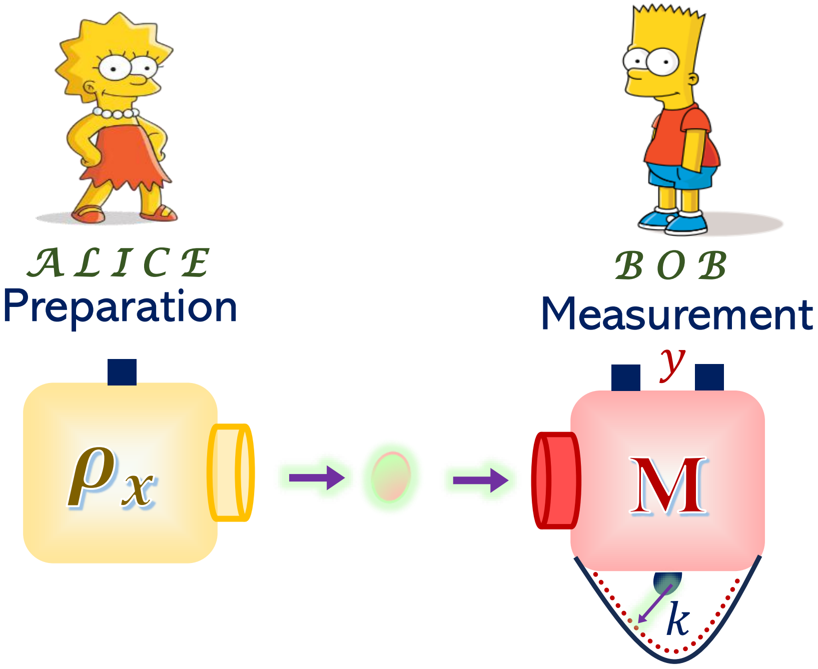
- Prevailing view:



Dimension assumption is necessary for PM self-testing.

A. Ambainis et al., arXiv:0810.2937 (2009); M. farkas et al., Phys. Rev. A 99, 032316 (2019)

The Parity-Oblivious Multiplexing Task



The $n \to 1$ POM Task

1. Alice receives an n-bit string $x^{\delta} \in \{0,1\}^n$ with $\delta \in \{0,1,\ldots,2^n-1\}$.

2. Upon the receiving the input x^{δ}, Alice uses preparation procedure $P_{x^{\delta}}$ to prepare the state and sends it to Bob.

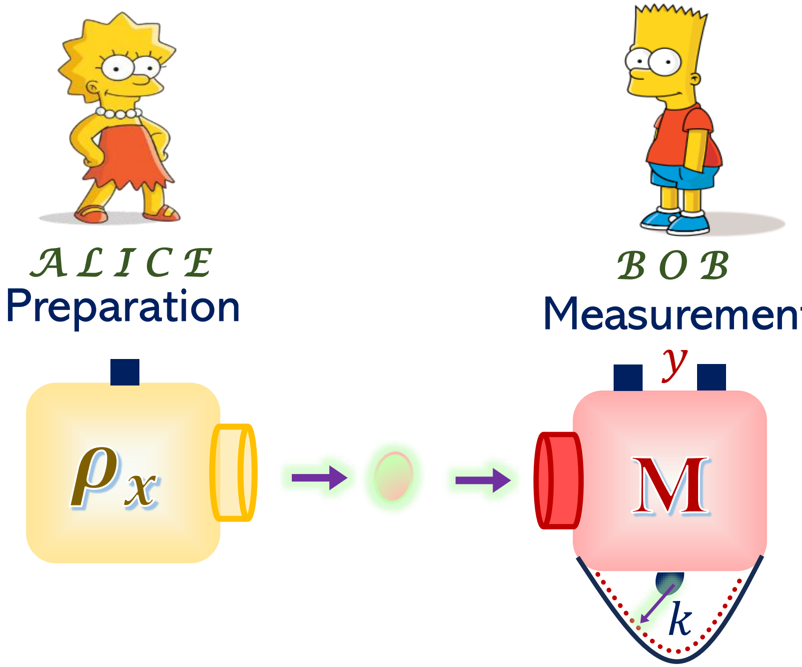
3. Bob receives index $y \in [n]$ and must output x_y.

4. The winning condition of the game is $b = x_y^{\delta}$.

5. Parity-obliviousness: Bob must learn no parity of weight

R. W. Spekkens et al., *Phys. Rev. Lett.* **102**, 010401 (2009).

The Parity-Oblivious Multiplexing Task



The $n \to 1$ POM Task

The success probability of the multiplexing task:

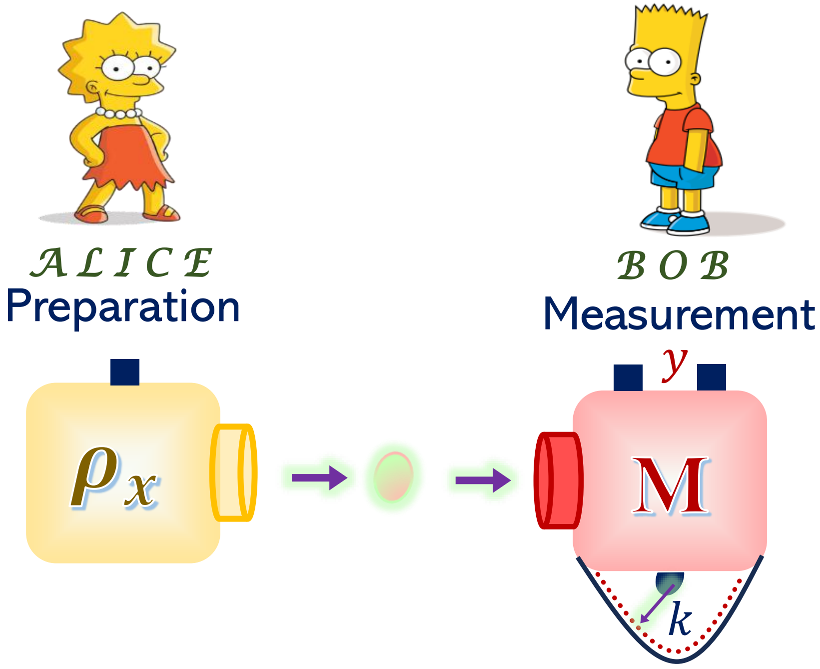
$$\mathcal{S}_n = \frac{1}{2^n n} \sum_{\substack{y \in \{1,2,3,...,n\} \\ x^\delta \in \{0,1\}^n}} p\left(b = x^\delta_y | P_{x^\delta}, B_y\right)$$

The parity-oblivious condition:

$$\forall s, y, b \sum_{x^\delta | x^\delta . s = 0} p\left(P_{x^\delta} | b, B_y\right) = \sum_{x^\delta | x^\delta . s = 1} p\left(P_{x^\delta} | b, B_y\right).$$

R. W. Spekkens et al., Phys. Rev. Lett. ***102****, 010401 (2009).*

The Parity-Oblivious Multiplexing Task



The $n \to 1$ POM Task

Parity Set:

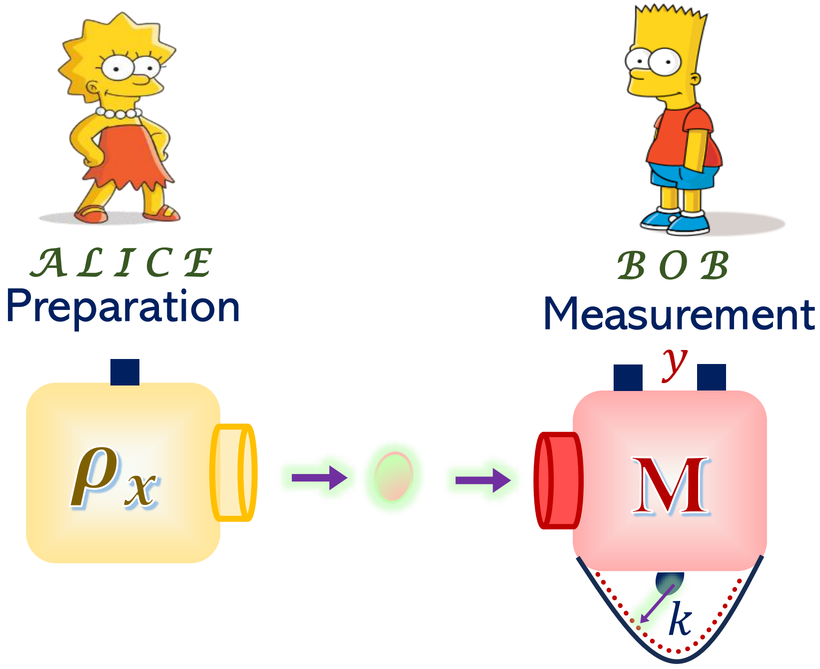
$$\mathbb{P}_n = \left\{ x^\delta \middle| x^\delta \in \{0,1\}^n, \sum_r x_r^\delta \geqslant 2 \right\} \quad \text{with} \quad r \in \{1,2,\ldots,n\}$$

For any element $s \in P_n$, the information about $x^\delta . s = \oplus_i \, x_i^\delta s_i$ must remain oblivious to Bob.

$$\forall s, y, b \quad \sum_{x^\delta | x^\delta . s = 0} p\left(P_{x^\delta} | b, B_y\right) = \sum_{x^\delta | x^\delta . s = 1} p\left(P_{x^\delta} | b, B_y\right).$$

R. W. Spekkens et al., Phys. Rev. Lett. ***102****, 010401 (2009).*

The Parity-Oblivious Multiplexing Task



The $n \rightarrow 1$ POM Task

The parity-oblivious condition:

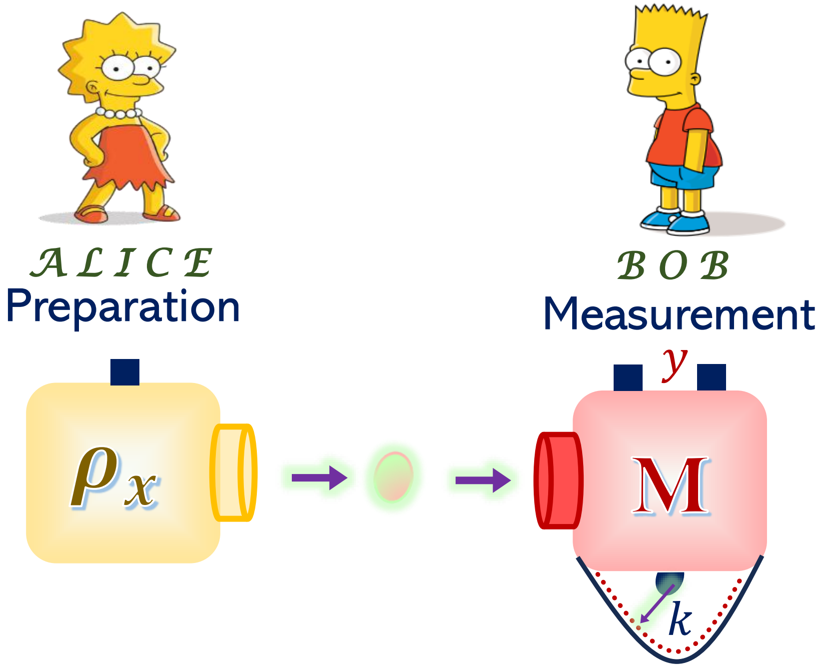
$$\forall s, y, b \quad \sum_{x^\delta | x^\delta . s = 0} p\left(P_{x^\delta} | b, B_y\right) = \sum_{x^\delta | x^\delta . s = 1} p\left(P_{x^\delta} | b, B_y\right) .$$

$$\forall s, y, b \quad \sum_{x^\delta | x^\delta . s = 0} p\left(b | P_{x^\delta}, B_y\right) = \sum_{x^\delta | x^\delta . s = 1} p\left(b | P_{x^\delta}, B_y\right)$$

Two preparation procedures $P_{x^\delta | x^\delta . s=0}$ and $P_{x^\delta | x^\delta . s=1}$ cannot be distinguished by any outcome b and any measurement B_y.

R. W. Spekkens et al., *Phys. Rev. Lett.* **102**, 010401 (2009).

The Parity-Oblivious Multiplexing Task



The $n \rightarrow 1$ POM Task

R. W. Spekkens et al., Phys. Rev. Lett. ***102****, 010401 (2009).*

The parity-oblivious condition:

$$\forall s, y, b \quad \sum_{x^\delta | x^\delta . s=0} p\left(b | P_{x^\delta}, B_y\right) = \sum_{x^\delta | x^\delta . s=1} p\left(b | P_{x^\delta}, B_y\right)$$

⇓

$$p\left(b | \rho_{00}, B_y\right) + p\left(b | \rho_{11}, B_y\right) = p\left(b | \rho_{01}, B_y\right) + p\left(b | \rho_{10}, B_y\right)$$

Preparation noncontextuality

Two preparation procedures $P_{x^\delta|x^\delta.s=0}$ and $P_{x^\delta|x^\delta.s=1}$ cannot be distinguished by any outcome b and any measurement B_y.

Two equivalent experimental procedures in quantum theory are assumed to be equivalently represented in an ontological model.

$$\forall M,\ k:\ p(k|P,M) = p(k|P',M) \Rightarrow \mu_P(\lambda|\rho) = \mu_{P'}(\lambda|\rho)$$

R. W. Spekkens et al., *Phys. Rev. Lett.* **102**, 010401 (2009).

Preparation noncontextuality

$$(\mathcal{S}_n)_C \leqslant \frac{1}{2}\left(1+\frac{1}{n}\right)$$

The parity oblivious constraint on Alice's state preparation:

$$\forall s \sum_{x^\delta | x^\delta . s=0} \rho_{x^\delta} = \sum_{x^\delta | x^\delta . s=1} \rho_{x^\delta}$$

The quantum success probability

$$(\mathcal{S}_n)_Q = \frac{1}{2^n n} \sum_{\substack{y\in\{1,2,3,\ldots,n\} \\ x^\delta \in \{0,1\}^n}} \mathrm{Tr}\left[\rho_{x^\delta} \Pi_y^b\right]$$

R. W. Spekkens et al., Phys. Rev. Lett. ***102****, 010401 (2009).*

Our First Result: Dimension-independent Optimal Quantum Value

Derivation Strategy:

- No assumption on the dimension of Alice's states or Bob's measurements.
- Represent preparation as

$$\rho_x = \frac{1}{d}(I + A_x)$$

- Use parity-obliviousness to enforce constraints on the set $\{A_x\}$ as

$$\forall s \in P_n \quad \sum_{x^\delta} (-1)^{x^\delta . s} A_\delta = 0$$

- The quantum success probability becomes

$$(\mathcal{S}_n)_Q = \frac{1}{2} + \frac{1}{2^{n+1} n d} \mathrm{Tr}\left[\sum_{\delta=0}^{2^{n-1}-1} \alpha_\delta \omega_\delta \mathcal{A}_\delta \mathcal{B}_\delta\right]$$

$$\mathcal{B}_\delta = \frac{\sum_{y=1}^{n} (-1)^{x_y} B_y}{\omega_\delta}; \quad \mathcal{A}_\delta = \frac{A_\delta + A_{\overline{\delta}}}{\alpha_\delta}$$

$$\omega_\delta = \left\| \left(\sum_{y=1}^{n} (-1)^{x_y^\delta} B_y \right) \right\| ; \quad \alpha_\delta = \left\| \left(A_\delta - A_{\overline{\delta}} \right) \right\|$$

R. K. Singh et al 2025 New J. Phys. 27 114520

Our First Result: Dimension-independent Optimal Quantum Value

Optimality requires:

- Bob's observables mutually anticommute.
- Pairs of complementary preparations are orthogonal.
- The optimal quantum success probability is

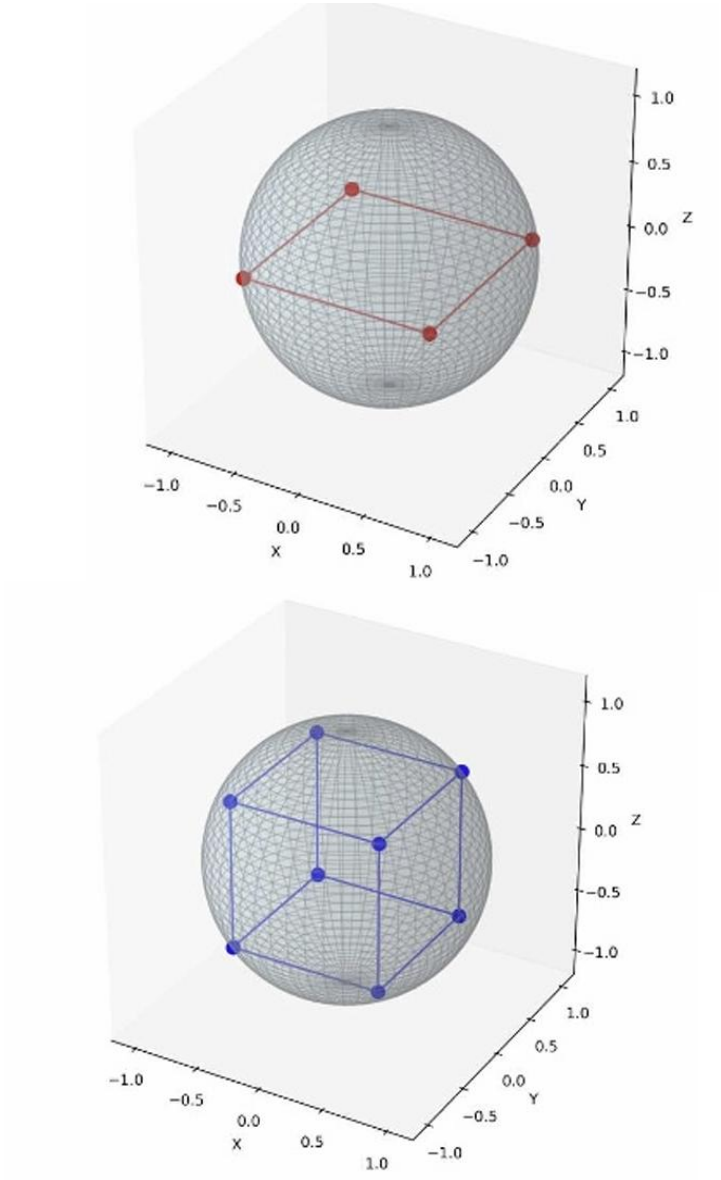
$$(\mathcal{S}_n)_Q^{\text{opt}} = \frac{1}{2}\left(1 + \frac{1}{\sqrt{n}}\right)$$

Alice's optimal preparation:

$$\rho_{x^\delta} = \frac{1}{d}\left(\mathbb{1}_d + \frac{\sum_{y=1}^{n}(-1)^{x_y^\delta} B_y}{\sqrt{n}}\right)$$

R. K. Singh et al 2025 New J. Phys. 27 114520

Self-testing Implications



R. K. Singh et al 2025 New J. Phys. 27 114520

- Requirement of n mutually anti-commuting observables constrains the minimal Hilbert space dimension : $d^* = 2^m,\ m = \left\lfloor \frac{1}{2}(n-1) \right\rfloor$.

- Alice must prepare quantum states of at least the same dimension, If the prepared states lie in a smaller-dimensional Hilbert space, then regardless of Bob's measurements, the success probability cannot attain its optimal value.

- Alice's 2^n preparations correspond to vertices of an n-dimensional hypercube in the Clifford Bloch sphere:

Self-testing : Formal Statement

Theorem 1. *Let a quantum strategy* $\{\rho_{x^\delta}, B_y \in \mathscr{L}(\mathcal{H}^d)\}$, *achieve maximum quantum success probability in the n-bit POM task, where* $\mathcal{H}^d$ *is an unknown finite-dimensional Hilbert space. Then, this strategy self-tests the reference preparations and measurements* $\{\rho'_{x^\delta}, B'_y \in \mathscr{L}(\mathcal{H}^{d'})\}$, *upto unitary freedom and complex conjugation, where* $\mathcal{H}^{d'}$ *is of known dimension, if there exists a unitary operation* $U: \mathcal{H}^d \rightarrow \mathcal{H}^{d'}$ *such that*

$$\exists U : \mathcal{H}^d \rightarrow \mathcal{H}^{d'} \otimes \mathcal{H}^J \text{ s.t. } \quad (i) \;\; U B_y U^\dagger = B'_y \otimes \mathbb{1}_J, \quad (ii) \;\; U \rho_{x^\delta} U^\dagger = \rho'_{x^\delta} \otimes \frac{\mathbb{1}_J}{J}.$$

- Hence, the physical strategy is equivalent to a known finite-dimensional quantum realisation.

- This gives a **full self-test** (up to unitary and complex conjugation).

R. K. Singh et al 2025 New J. Phys. 27 114520

Conceptual Significance & Applications

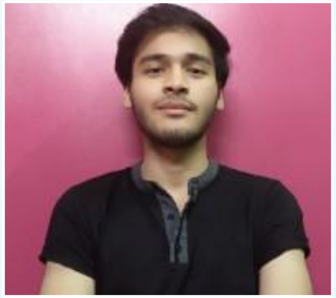
- Breaks the perceived barrier that PM self-testing needs dimension restrictions.
- Dimension witness: n mutually anticommuting observables imply a minimal system dimension.
- Recycling a quantum resource
- Single-device randomness expansion: Optimal POM violation gives a bound on min-entropy via EAT; Allows practical randomness expansion without entanglement and without dimension assumptions.
- Verifiable blind quantum computing
- Parameter Estimation, Sensing

R. K. Singh et al 2025 New J. Phys. 27 114520

Acknowledgements

- Collaborators

Ritesh Kumar Singh, IITH



Sameer Nautiyal, IITH

Alok K. Pan, IITH

R. K. Singh et al 2025 New J. Phys. 27 114520


Thank You