Quantum Measurements Drive Quantum Communication

Archan S Majumdar

S. N. Bose National Centre for Basic Sciences

(1) Measurement incompatibility and quantum advantage in communication, D. Saha, D. Das, A. K. Das, B. Bhattacharya, A. S. Majumdar, Phys. Rev. A **107**, 062210 (2023)

(2) An operational approach to classifying measurement incompatibility, A. K. Das, S. Mukherjee, D. Saha, D. Das, A. S. Majumdar, arXiv: 2401.01236

(3) Quantum contextuality provides communication complexity advantage, S. Gupta, D. Saha, Z.-P. Xu, A. Cabello, A. S. Majumdar, Phys. Rev. Lett. **130**, 080802 (2023)

PERSPECTIVE

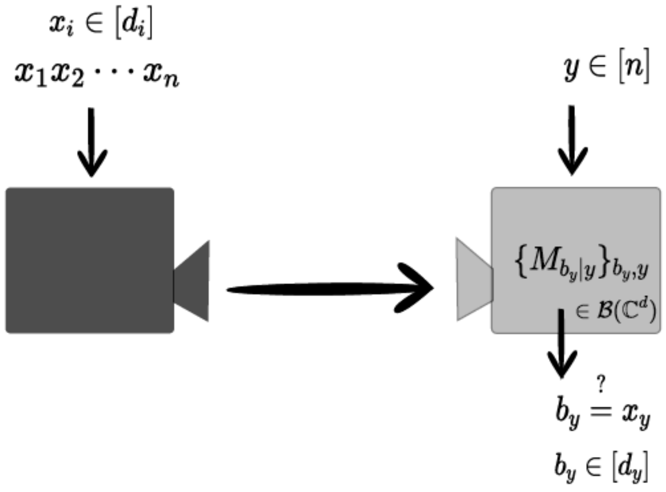
Q: *What is the fundamental (or key) feature (property) of* ***QM*** *that sets it distinctly apart from* ***classical physics*** *enabling beautiful (technologically revolutionary) information processing tasks ?*

A: ***Character of measurements: Incompatibility of measurements, Contextuality....***

Quantum entanglement is a powerful resource…..

… but there exist Quantum Communication tasks without entanglement

e.g., in prepare and measure scenarios (QKD without entanglement)



Q: What causes advantage in Quantum Communication tasks without entanglement ?

A: Measurement Incompatibility; Contextuality

(character of quantum measurements)

Outline

- What do we mean by measurement incompatibility ?
- Quantum communication tasks – RAC games
- Measurement incompatibility is necessary for Quantum Advantage in Communication
- Incompatibility in practical scenarios
- Operational witness incompatibility in DI and semi-DI protocols
- Quantum contextuality & communication complexity advantage

Measurement Incompatibility

- Incompatible measurements: Cannot be performed simultaneously on a single copy of a quantum system [e.g., position & momentum of a QM particle with arbitrary precision]

- MI differentiates QM from classical physics

- Quantum Measurement Incompatibility is at the root of fundamental quantum aspects, e.g., Bell-nonlocality, EPR steering, quantum contextuality, quantum violation of macrorealism, temporal & channel steering…..

Measurement Incompatibility

- MI is necessary but not sufficient for Bell violation [Brunner et al., PRA 97, 012129 (2018)]
- MI is both necessary and sufficient for steering [Brunner et al., PRL 113, 160402 (2014)]
- MI in communication tasks without entanglement, e.g., state discrimination [Carmeli et al., PRL 122, 130402 (2019)]
- MI both necessary and sufficient in state discrimination task in prepare and measure scenario (1-sided Device Independent protocol) [Cavalcanti et al., PRL 122, 130403 (2019)]

Q: Is there any generic link between MI and non-classical correlations ?

Ans: Yes, in prepare & measure scenarios without entanglement

Operational Witness of MI for any set of Quantum Measurements of arbitrary setting

Measurement Incompatibility

Consider general POVM

$$E_y \equiv \{M_{b_y|y}\}_{b_y} \text{ with } M_{b_y|y} \geqslant 0 \text{ for all } b_y \qquad \sum_{b_y} M_{b_y|y} = \mathbb{1}$$

$y \in [n]$: choice of measurements $\qquad b_y$: outcomes of measurements

$$[k] := \{1,\ldots,k\}$$

A set of measurements $\{E_y\}_y$ is **compatible if**

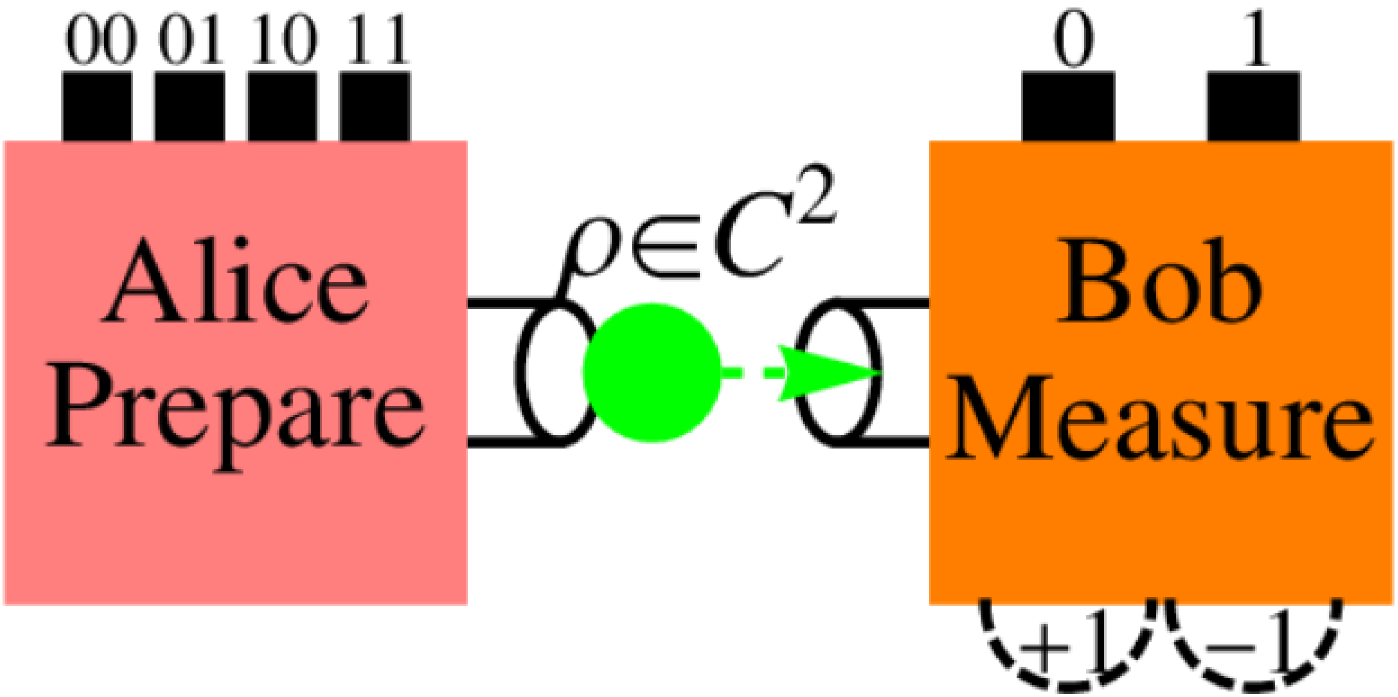
there exists a parent POVM $\{G_\kappa : G_\kappa \geqslant 0 \, \forall \kappa, \sum_\kappa G_\kappa = \mathbb{1}\}$

such that $\forall b_y, y, \quad M_{b_y|y} = \sum_\kappa P_y(b_y|\kappa) G_\kappa \quad P_y(b_y|\kappa) \geqslant 0 \; \forall y, b_y, \kappa; \; \sum_{b_y} P_y(b_y|\kappa) = 1 \; \forall y, \kappa$

Marginals of parent POVM $\{G_\kappa\}$ **give rise to individual measurement effects** $\{M_{b_y|y}\}_{b_y,y}$

Communication tasks in prepare-and-measure scenario

Random Access Code (RAC) games



(Color online) The sketch of 2 → 1 quantum random access code. Alice encodes her randomly chosen 2 classical bits a ∈ {00, 01, 10, 11} into 1 qubit ρa and sends it to Bob. To decode the required bit, Bob performs some measurement on the received qubit depending on his input bit y ∈ {0, 1} with the measurement results denoted as b ∈ {+1, −1} (which in the computational basis can be represented by b ∈ {0, 1}).

Acknowledgement: https://www.researchgate.net/figure/Color-online-The-sketch-of-2-1-quantum-random-access-code-Alice-encodes-her-randomly_fig1_228325435

Quantum random access codes ⟷ Non-classical temporal correlations

PHYSICAL REVIEW A **106**, 042439 (2022)

Role of nonclassical temporal correlation in powering quantum random access codes

Subhankar Bera,[1,*] Ananda G. Maity,[1,†] Shiladitya Mal,[2,3,‡] and A. S. Majumdar[1,§]
[1] *S. N. Bose National Centre for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700106, India*
[2] *Physics Division, National Center for Theoretical Sciences, Taipei 10617, Taiwan*
[3] *Department of Physics and Center for Quantum Frontiers of Research and Technology (QFort), National Cheng Kung University, Tainan 701, Taiwan*

(Received 13 May 2022; accepted 4 October 2022; published 25 October 2022)

We explore the fundamental origin of the quantum advantage behind random access code. We propose new temporal inequalities compatible with noninvasive-realist models and show that any nonzero quantum advantage of $n \mapsto 1$ random access code in the presence of shared randomness is equivalent to the violation of the corresponding temporal inequality. As a consequence of this connection, we also prove that the maximal success probability of $n \mapsto 1$ random access code can be obtained when the maximal violation of the corresponding inequality is achieved. We further show that any nonzero quantum advantage of $n \mapsto 1$ random access code, or in other words, any nonzero violation of the corresponding temporal inequality, can certify genuine randomness.

DOI: 10.1103/PhysRevA.106.042439

...... common role of measurement incompatibility

Incompatibility is necessary for quantum advantage in communication tasks

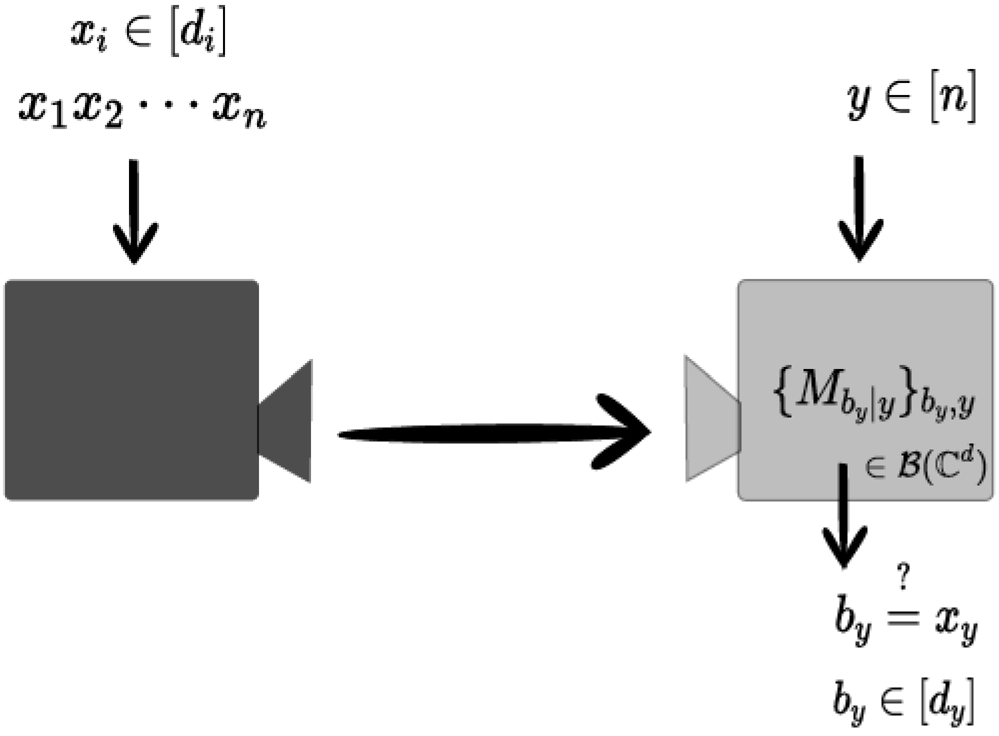
Consider communication task (general RAC) $x \in [l]$ and $y \in [n]$

Alice receives input x

She sends a d-dimensional classical or quantum system to Bob

Bob receives input y and the message

He outputs $b_y \in [d_y]$



Outcomes determined by probability $\{p(b_y|x,y)\}$

Probability distributions in RAC game *(different probabilities in different theories)*

- Classical communication using pre-shared randomness

$$p(b_y|x,y) = \sum_{m=1}^{d} \int_\lambda \pi(\lambda) p_a(m|x,\lambda) p_b(b_y|y,m,\lambda)\, d\lambda$$

encoding/decoding functions $\{p_a(m|x,\lambda)\}, \{p_b(b_y|y,m,\lambda)\}$

$$\sum_m p_a(m|x,\lambda) = \sum_{b_y} p_b(b_y|y,m,\lambda) = 1$$

- Quantum communication with pre-shared randomness

$$p(b_y|x,y) = \int_\lambda \pi(\lambda) \mathrm{Tr}\left(\rho_{x,\lambda} M_{b_y|y,\lambda}\right) d\lambda, \qquad \rho_{x,\lambda},\ M_{b_y|y,\lambda} \in \mathcal{B}(\mathbb{C}^d)$$

Quantum state sent by Alice: $\{\rho_{x,\lambda}\}$ upon input x and random variable λ

Measurement made by Bob: $\{M_{b_y|y,\lambda}\}$ for input y and random variable λ

Probability distributions in RAC game

- Quantum communication without pre-shared randomness

$$p(b_y|x,y) = \mathrm{Tr}(\rho_x M_{b_y|y}), \quad \rho_x, M_{b_y|y} \in \mathcal{B}(\mathbb{C}^d)$$

Communication scenario specified by a set of natural numbers

$l, n,$ and $\vec{d} = \{d_1, \cdots, d_n\}$ such that $x \in [l],\ y \in [n],\ b_y \in [d_y]$

Different sets of probabilities obtainable by d-dimensional communication:

- **Classical :** $\mathcal{C}_d := \{p(b_y|x,y)\}$
- **Quantum** : $\mathcal{Q}_d := \{p(b_y|x,y)\}$ (for compatible measurement set $\mathcal{Q}_d^C := \{p(b_y|x,y)\}$
- **Quantum without shared randomness**: $\overline{\mathcal{Q}}_d := \{p(b_y|x,y)\}$ or ($\overline{\mathcal{Q}}_d^C := \{p(b_y|x,y)\}$ for compatible)

Measurement incompatibility is necessary for quantum advantage (with or without shared randomness)

- **Result:** *Given any scenario specified by* $(l, n, \vec{d})$, $\overline{\mathcal{Q}}_d^C \subseteq \mathcal{Q}_d^C = \mathcal{C}_d$

Proof: 1st relation $\overline{\mathcal{Q}}_d^C \subseteq \mathcal{Q}_d^C$ follows from the definition of the two sets

Proof of 2nd relation:

Consider, Bob performs POVM measurements $\{G_\kappa\}$ (parent POVM of the set $\{M_{b_y|y,\lambda}\}$)

Frenkel-Weiner theorem [Comm. Math. Phys. 340, 563 (2015)]:

For a single quantum measurement on a d-dimensional quantum state, the set of input-output probabilities $p(\kappa|x)$ *can always be reproduced by suitable classical d-dimensional communication with shared randomness.*

Hence, $\forall \rho_{x,\lambda}$ there exists a classical strategy $\tilde{\pi}(\tilde{\lambda}), p_a(m|x,\lambda,\tilde{\lambda}), p_b(\kappa|m,\tilde{\lambda})$, such that

$$\mathrm{Tr}(\rho_{x,\lambda} G_\kappa) = \sum_{m=1}^{d} \int_{\tilde{\lambda}} \tilde{\pi}(\tilde{\lambda}) p_a(m|x,\lambda,\tilde{\lambda}) p_b(\kappa|m,\tilde{\lambda})\, d\tilde{\lambda}$$

Measurement incompatibility is necessary for quantum advantage (with or without shared randomness)

- **Proof (i)** Arbitrary probability distribution $p(b_y|x,y) \in \mathcal{Q}_d^C$ obtainable from compatible set of measurements can always be reproduced by a suitable classical strategy:

Consider arbitrary set of probability distributions arising from set of compatible measurements by Bob

$$p(b_y|x,y) \in \mathcal{Q}_d^C \qquad p(b_y|x,y) = \int_\lambda \pi(\lambda)\mathrm{Tr}\left(\rho_{x,\lambda} M_{b_y|y,\lambda}\right) d\lambda$$

There exists a parent POVM $\{G_\kappa\}$ s.t. $\forall b_y, y, \lambda, \quad M_{b_y|y,\lambda} = \sum_\kappa P_{y,\lambda}(b_y|\kappa)\, G_\kappa$

Hence, $$\int_\lambda \pi(\lambda)\mathrm{Tr}\left(\rho_{x,\lambda} M_{b_y|y,\lambda}\right) d\lambda = \sum_\kappa \int_\lambda P_{y,\lambda}(b_y|\kappa)\pi(\lambda)\mathrm{Tr}(\rho_{x,\lambda} G_\kappa)\, d\lambda$$

Now, applying Frenkel-Weiner result, $$= \sum_m \int_\lambda \int_{\tilde{\lambda}} \pi(\lambda)\tilde{\pi}(\tilde{\lambda}) p_a(m|x,\lambda,\tilde{\lambda}) \left(\sum_\kappa P_{y,\lambda}(b_y|\kappa) p_b(\kappa|m,\tilde{\lambda})\right) d\lambda\, d\tilde{\lambda}$$

$$= \sum_m \int_\lambda \int_{\tilde{\lambda}} \pi(\lambda)\tilde{\pi}(\tilde{\lambda}) p_a(m|x,\lambda,\tilde{\lambda}) p_b(b_y|y,m,\lambda,\tilde{\lambda}) d\lambda d\tilde{\lambda} \in \mathcal{C}_d$$

Thus, $\mathcal{Q}_d^C \subseteq \mathcal{C}_d$.

Proof (ii) On the other hand, any classical strategy can always be realized by a quantum strategy with compatible measurements, i.e., $\mathcal{C}_d \subseteq \mathcal{Q}_d^C$.

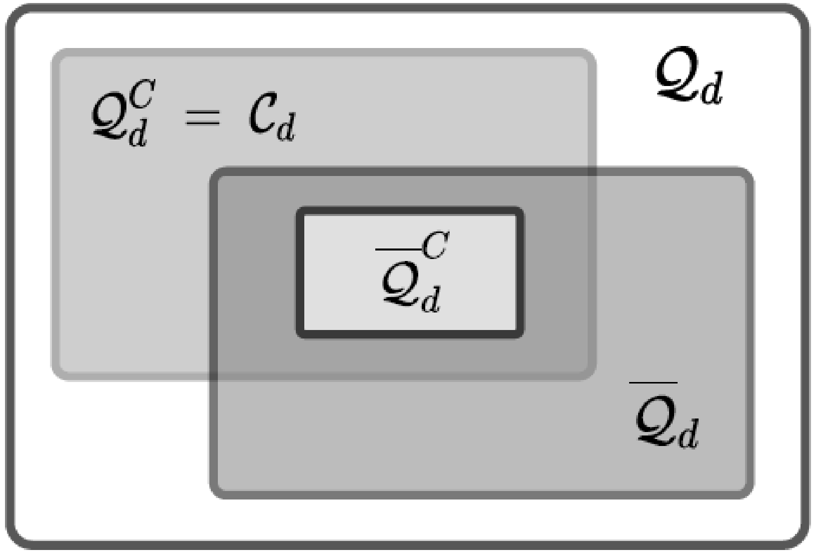
[Saha, Das,…., ASM, PRA 2023)] Hence, the sets are identical $\mathcal{Q}_d^C = \mathcal{C}_d$ □

Measurement incompatibility is necessary for quantum advantage in communication tasks

Figure of merit in any communication tasks is a function of the probabilities $p(b_y|x,y)$

Any quantum advantage in such tasks can be attained (with or without shared randomness) only if the set of measurements is incompatible.

[Saha, Das,...., ASM, PRA 2023)]



Generic relations among the various probability sets

$\overline{\mathcal{Q}}_d$ is not a subset of $\mathcal{C}_d$

$\overline{\mathcal{Q}}_d^C$ is a subset of both $\mathcal{C}_d$ and $\overline{\mathcal{Q}}_d$

$(\mathcal{C}_d \cap \overline{\mathcal{Q}}_d) \setminus \overline{\mathcal{Q}}_d^C \neq \varnothing$ $\overline{\mathcal{Q}}_d^C$ is not the intersection

Measurement incompatibility is not sufficient for quantum advantage without pre-shared randomness

[Chaves, et al., PRX Quantum 2, 030311 (2021)]

(Semi-Device-Independent) Witness of Measurement Incompatibility

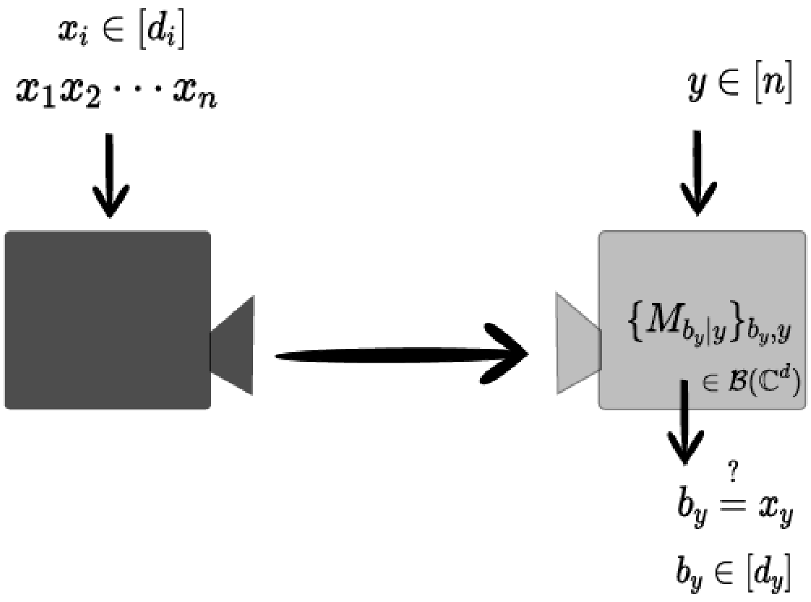
Recap of the scenario

n measurements, defined by $\{M_{b_y|y}\}$ $\quad y \in [n]$

Measurement $\quad y$ has d_y outcomes, $\quad b_y \in [d_y]$

Alice gets a string of n dits $\quad x = x_1 x_2 \cdots x_n$

randomly from the set of all possible strings $\quad x_y \in [d_y]$



Alice communicates a d-dimensional classical or quantum system encoding her information

Bob's task is to guess the y-th dit when y is chosen randomly.

[Saha, Das,…., ASM, PRA 2023)]

Incompatibility witness for any set of measurements of arbitrary settings

For the generalized RAC game, figure of merit (average success probability):

$$S(n,\vec{d},d) = \frac{1}{n\prod_y d_y}\sum_{x,y} p(b_y = x_y|x,y)$$

Result: *Given any scenario specified by $(l,n,\vec{d})$, the maximum values of any linear function of $\{p(b_y|x,y)\}$ obtained within the three different sets $\mathcal{C}_d$, $\mathcal{Q}_d^C$, and $\overline{\mathcal{Q}}_d^C$ are the same.*

maximum value over $\mathcal{C}_d$, $\mathcal{Q}_d^C$ and $\overline{\mathcal{Q}}_d^C$ are the same

$$S_c(n,\vec{d},d) = \max_{\{p(b_y|x,y)\}\in\mathcal{C}_d} S(n,\vec{d},d) = \max_{\{p(b_y|x,y)\}\in\mathcal{Q}_d^C} S(n,\vec{d},d)$$

Incompatibility witness for any set of measurements of arbitrary settings

Classical (or compatible quantum measurements) bound for

$$d \leqslant \min_y d_y$$

$$S_c(n,\vec{d},d) = \frac{1}{n\prod_y d_y}\sum\left[\left(\prod_{j=1}^{d_{\max}} C_{n_j}^{\alpha_j}\right)\max_{i=1,\cdots,d}\{n_i\}\right]$$

$$\alpha_j = k_j - \sum_{i=j+1}^{d_{\max}} n_i, \quad C_{n_j}^{\alpha_j} = \frac{\alpha_j(\alpha_j-1)\cdots(\alpha_j-n_j+1)}{n_j(n_j-1)\cdots 1}$$

In order to witness measurement incompatibility, one needs to know $S_c(n,\vec{d},d)$

Whenever a set of measurements in the scenario specified by $n,\vec{d},d$ gives

$$S(n,\vec{d},d) > S_c(n,\vec{d},d)$$

in the generalized RAC game, we can conclude that the measurements are incompatible

Incompatibility witness (limiting cases)

Dimension of the system is upper bounded by number of outcomes: $d \leqslant \min_y d_y$

Consider all measurements have same number of outcomes: $d_y = \tilde{d}$

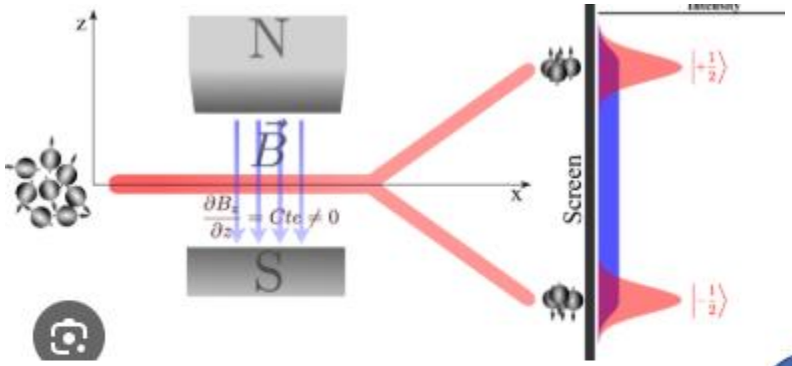
- For n = 2 (e.g., $2 \mapsto 1$ RAC): $S_c(2,\tilde{d},d) = \frac{1}{2\tilde{d}^2}\left(d + 2d\tilde{d} - d^2\right)$ *
- For n = 3 (e.g., $3 \mapsto 1$ RAC): $S_c(3,\tilde{d},d) = \frac{d}{3\tilde{d}^3}\left(d^2 - 1 + 3\tilde{d}(\tilde{d} + 1 - d)\right)$
- **Result:** Any set of three incompatible rank-1 projective measurements

  yields larger value than $S_c(n = 3, \tilde{d} = 2, d = 2) = 3/4$

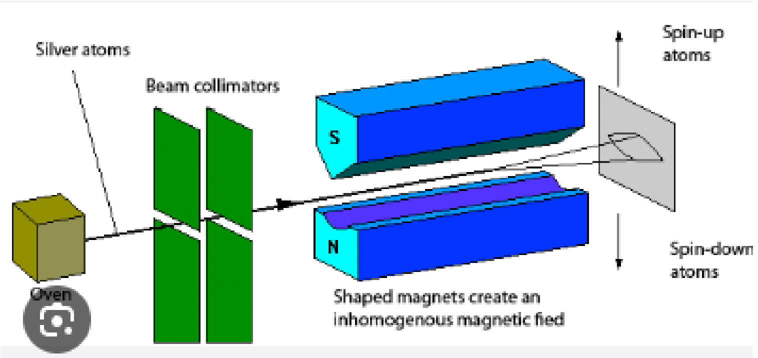
* (recovers earlier results [Heinosaari et al., EPL 130, 50001 (2020)];
[Horodecki et al., Phys. Rev. A 101, 052104 (2020)]

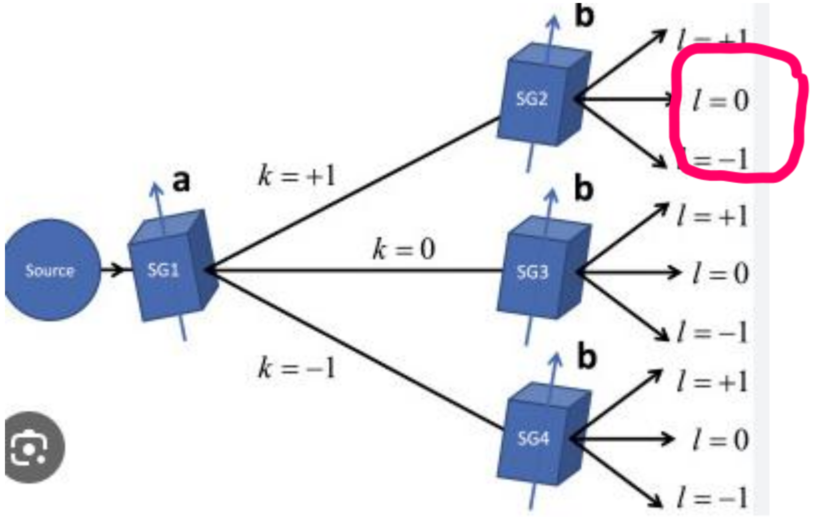
Measurement Incompatibility: Practical scenario [Das,..., Saha..., ASM, arXiv: 2401.01236]

Measurement devices are imperfect:



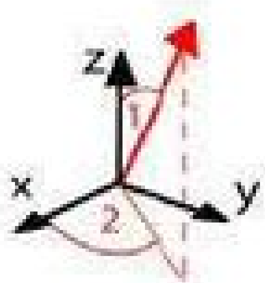
- **Coarse-graining of outcomes**

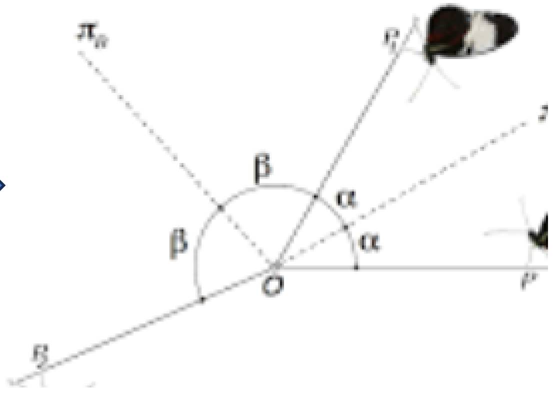




- **Convex mixing of measurements**

$$\sigma_z \rightarrow \vec{\sigma}.\hat{n} = \sigma_x n_x + \sigma_y n_y + \sigma_z n_z$$





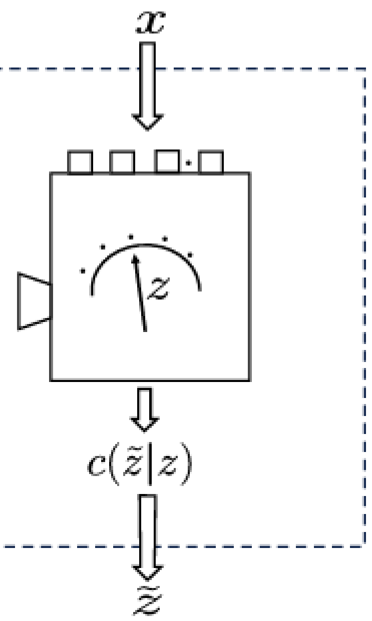
- **Environmental/device noise**

Measurement Incompatibility: Operational approach [Das,..., Saha..., ASM, arXiv: 2401.01236]

- **Coarse-graining of outcomes:**

Modified set of measurements

$$\tilde{M}_{\tilde{z}_x|x} = \sum_z c_x(\tilde{z}_x|z) M_{z|x}$$



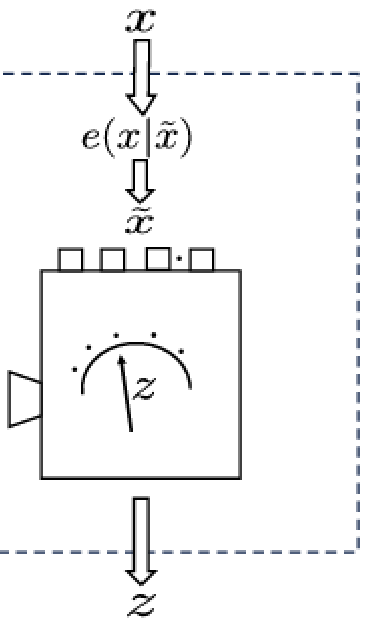
- **Convex mixing of measurements:**

$$M = \{M_z\}_z, N = \{N_z\}_z, R = \{R_z\}_z$$

$$Q_{(M,N)} = \{qM_z + (1-q)N_z\}_z$$

Even if R is incompatible with M and N separately,

R is not necessarily incompatible with $Q_{(M,N)}$



Definitions

Definition 1 (Fully incompatible measurements w.r.t. coarse-graining). *A set of measurements* $\{M_{z|x}\}$ *is fully incompatible w.r.t. coarse-graining if they remain incompatible after all possible nontrivial coarse-graining.*

Definition 2 (k-incompatible measurements w.r.t. coarse-graining). *A set of measurements* $\{M_{z|x}\}$ *is k-incompatible w.r.t. coarse-graining if they remain incompatible after all possible nontrivial coarse-graining that gives rise to at least k outcome measurements.*

Definition 3. *Three measurements M, N and R are fully incompatible w.r.t. disjoint-convex-mixing if each of the pairs, M and* $Q_{(N,R)}$*, N and* $Q_{(M,R)}$*, R and* $Q_{(M,N)}$*, are incompatible for all values of q*

Definition 4 (k-incompatible measurements w.r.t. disjoint-convex-mixing). *Given a set of n measurements, the measurements are k-incompatible w.r.t. disjoint-convex-mixing if, after taking every possible disjoint-convex-mixing that yields k number of measurements, the resulting measurements are incompatible.*

Definition 5 (Fully incompatible measurements w.r.t. disjoint-convex-mixing). *A set of n measurements is fully incompatible w.r.t. disjoint-convex-mixing if it is k-incompatible for all* $k = 2, \cdots, n$.

Theorems [Das,..., Saha..., ASM, arXiv: 2401.01236]

Theorem 1. *The following condition is necessary but not sufficient for two rank-one projective measurements of dimension ≥ 4, defined by $\{|\psi_i\rangle\}$ and $\{|\phi_j\rangle\}$, to be fully incompatible w.r.t. coarse-graining:*

$$\langle\psi_i|\phi_j\rangle \neq 0, \ \forall i, j.$$

However, the above condition is necessary and sufficient for two 3-dimensional rank-one projective measurements.

Theorem 2. *If three-qubit measurements (15) are such that $\vec{n}_i$ are in the same plane of the Bloch sphere, then they are not fully incompatible w.r.t. disjoint-convex-mixing.*

$$M_z = \frac{1}{2}\left(\mathbb{1} + (-1)^z \ \vec{n}_0 \cdot \vec{\sigma}\right)$$
$$N_z = \frac{1}{2}\left(\mathbb{1} + (-1)^z \ \vec{n}_1 \cdot \vec{\sigma}\right) \qquad z = 0, 1$$
$$R_z = \frac{1}{2}\left(\mathbb{1} + (-1)^z \ \vec{n}_2 \cdot \vec{\sigma}\right)$$

Theorem 3. *Consider three-qubit measurements (15) are such that $\vec{n}_0 = \nu_0\hat{x}$, $\vec{n}_1 = \nu_1\hat{y}$, $\vec{n}_2 = \nu_2\hat{z}$ with $0 \leqslant \nu_0, \nu_1, \nu_2 \leqslant 1$, that is, the noisy version of Pauli observables,*

$$M_z = \frac{1}{2}\left(\mathbb{1} + (-1)^z \nu_0 \sigma_x\right) = \nu_0 \left(\frac{\mathbb{1}+(-1)^z\sigma_x}{2}\right) + (1-\nu_0)\frac{\mathbb{1}}{2},$$
$$N_z = \frac{1}{2}\left(\mathbb{1} + (-1)^z \nu_1 \sigma_y\right) = \nu_1 \left(\frac{\mathbb{1}+(-1)^z\sigma_y}{2}\right) + (1-\nu_1)\frac{\mathbb{1}}{2},$$
$$R_z = \frac{1}{2}\left(\mathbb{1} + (-1)^z \nu_2 \sigma_z\right) = \nu_2 \left(\frac{\mathbb{1}+(-1)^z\sigma_z}{2}\right) + (1-\nu_2)\frac{\mathbb{1}}{2},$$

with $z = 0, 1$. These measurements are fully incompatible w.r.t. disjoint-convex-mixing if and only if

$$\min\left\{\nu_0^2 + \frac{\nu_1^2\nu_2^2}{\nu_1^2+\nu_2^2}, \nu_1^2 + \frac{\nu_0^2\nu_2^2}{\nu_0^2+\nu_2^2}, \nu_2^2 + \frac{\nu_0^2\nu_1^2}{\nu_0^2+\nu_1^2}\right\} > 1$$

Device-independent operational witness of incompatibility

Projective measurements of Alice (3-outcome rank-1 projective in $\mathbb{C}^3$:

$$|\xi\rangle_{A,a} = \frac{1}{\sqrt{3}} \sum_{j=0}^{2} \exp\left(\mathrm{i}\frac{2\pi}{3} j(\xi + \alpha_a)\right) |j\rangle_A \quad A_a \equiv \{|\xi\rangle_{A,a}\} \quad a \in \{1,2\}$$

Projective measurements of Bob: $\xi \in \{0,1,2\}, \alpha_1 = 0, \alpha_2 = \frac{1}{2}$

$$|\eta\rangle_{B,b} = \frac{1}{\sqrt{3}} \sum_{j=0}^{2} \exp\left(\mathrm{i}\frac{2\pi}{3} j(-\eta + \beta_b)\right) |j\rangle_B \quad B_b \equiv \{|\eta\rangle_{B,b}\} \quad \eta \in \{0,1,2\}, \beta_1 = \frac{1}{4}, \beta_2 = -\frac{1}{4}$$

give maximum violation of CGLMP inequality

CH functional $\quad -1 \le S \le 1,$

$$S = P(00|A_1,B_1) + P(00|A_1,B_2) + P(00|A_2,B_2) - P(00|A_2,B_1) - P(0|A_1) - P(0|B_2).$$

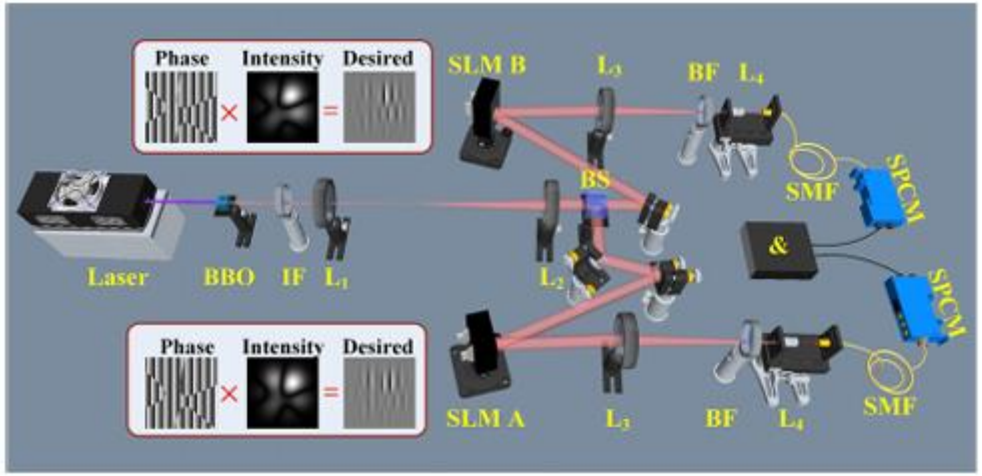
Coarse-graining of outcomes:

$(0,1) \equiv \bar{0}$ and $2 \equiv \bar{1}$ for A1 and A2; $(0,1) \equiv \bar{0}$ for B1 and B2

$$|\psi\rangle = 0.596|+1\rangle_A|-1\rangle_B + 0.529|+2\rangle_A|-2\rangle_B + 0.604|-1\rangle_A|+1\rangle_B$$

CGLMP experiment with Orbital angular momentum entanglement [Zhang et al., PRA 110, 012202 (2024)]

Possible CG choices of A_1	Possible CG choices of A_2	ΔS_T	ΔS_E	Incompatible
(0,1)	(0,1)	0.126	0.122	yes
(0,1)	(1,2)	0	0	?
(0,1)	(0,2)	0.126	0.122	yes
(1,2)	(0,1)	0.126	0.122	yes
(1,2)	(1,2)	0.126	0.122	yes
(1,2)	(0,2)	0	0	?
(0,2)	(0,1)	0	0	?
(0,2)	(1,2)	0.126	0.122	yes
(0,2)	(0,2)	0.126	0.122	yes



Semi-device-independent witness of incompatibility

RAC tasks -- $(2,\bar{d},d)$ Alice gets 2-dit string input message (x_1,x_2) with $x_1,x_2\in[\bar{d}]$,

and communicates d-dimensional system to Bob

If ant two POVMs with $\bar{d}$ *outcomes acting on* $\mathbb{C}^d$ *are jointly measureable, average success probability:*

$$P(2,\bar{d},d)\le P_{CB}(2,\bar{d},d)=\frac{1}{2}\left(1+\frac{d}{\bar{d}^2}\right)$$

Theorem 4. *Two 3-outcome rank-one projective measurements,* $M=\{|\phi_0\rangle,|\phi_1\rangle,|\phi_2\rangle\}$ *and* $N=\{|\psi_0\rangle,|\psi_1\rangle,|\psi_2\rangle\}$, *can be witnessed to be fully incompatible w.r.t. coarse-graining via RAC if and only if* $0<|\langle\phi_i|\psi_j\rangle|<\frac{4}{5}$, $\forall\ i,j=0,1,2$.

Theorem 5. *Three noisy Pauli measurements of Eq. (19) with equal noise* ($\nu=\nu_0=\nu_1=\nu_2$) *are witnessed to be fully incompatible w.r.t. disjoint-convex-mixing via RAC if and only if* $\sqrt{2/3}<\nu\leqslant 1$.

Communication without entanglement

----

*Role of Contextuality**(*)*

*** There is no probability distribution in agreement with marginal distributions corresponding to jointly measureable observables*

*(*)*Contextuality can be formulated independently of existence of incompatible measurements. [Selby et al., PRL 130, 230201 (2023)]

What is contextuality ?

Properties

- An attributive property is a constant property of an object which can be observed and measured at any time and which is not modified by the measurement.

  Example: rest mass, electric charge

- A contextual property is a property revealed only in a specific experiments or under particular conditions and characterizes the interaction of the object with the external world or a measuring apparatus. Color of the chameleon, weight, spin projection and "probability"

Applications of Contextuality….

- Quantum state discrimination

  [Schmid, Spekkens, Phys. Rev. X 8, 011015 (2018)]

- Robust self-testing

  [Bharti et al., Phys. Rev. Lett. 122, 250403 (2019)]

- Quantum computation

  [Howard et al., Nature 510, 351 (2014)]

- QKD based on Contextuality monogamy

  [J. Singh, K. Bharti, Arvind, Phys. Rev. A 95, 062333 (2017)]

- Preparation Contextuality in parity oblivious multiplexing

  [Spekkens, et al., Phys. Rev. Lett. 102, 010401 (2009);

  S. Ghorai, A. K. Pan, Phys. Rev. A 98, 032110 (2018)]

Quantum Contextuality Provides Communication Complexity Advantage

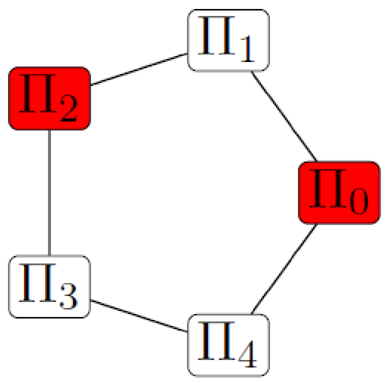
Shashank Gupta,[1] Debashis Saha,[1,2] Zhen-Peng Xu,[3,4] Adán Cabello,[5,6] and A. S. Majumdar[1]
[1]*S. N. Bose National Centre for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700106, India*
[2]*School of Physics, Indian Institute of Science Education and Research Thiruvananthapuram, Kerala 695551, India*
[3]*School of Physics and Optoelectronics Engineering, Anhui University, 230601 Hefei, People's Republic of China*
[4]*Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Straße 3, 57068 Siegen, Germany*
[5]*Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*
[6]*Instituto Carlos I de Física Teórica y Computacional, Universidad de Sevilla, E-41012 Sevilla, Spain*

(Received 30 June 2022; accepted 31 January 2023; published 24 February 2023)

Despite the conceptual importance of contextuality in quantum mechanics, there is a hitherto limited number of applications requiring contextuality but not entanglement. Here, we show that for any quantum state and observables of sufficiently small dimensions producing contextuality, there exists a communication task with quantum advantage. Conversely, any quantum advantage in this task admits a proof of contextuality whenever an additional condition holds. We further show that given any set of observables allowing for quantum state-independent contextuality, there exists a class of communication tasks wherein the difference between classical and quantum communication complexities increases as the number of inputs grows. Finally, we show how to convert each of these communication tasks into a semi-device-independent protocol for quantum key distribution.

DOI: 10.1103/PhysRevLett.130.080802

Contextuality witnesses



Set of events in contextuality experiment: $\{e_i\}_{i=1}^n$

Define n-vertex graph G where each event is represented by a vertex, and

Exclusive events correspond to adjacent vertices, e.g. 5-vertex graph

Event e_i is represented by projector Π_i (exclusive events ⟺ orthogonal projectors)

Contextuality witness $W = \sum_{i=1}^n w_i P(e_i), \quad w_i \geq 0$

for quantum realization Π_i and state ρ such that $\sum_{i=1}^n w_i \mathrm{tr}(\rho \Pi_i) > \alpha(G, \vec{w})$

$\alpha(G, \vec{w})$: largest value of $\sum_{i \in I} w_i$, *I* : subsets consisting of non-adjacent vertices $\vec{w} = \{w_i\}_{i=1}^n$

(Independence number)

Given W, one can find a non-contextuality inequality: Quantum value : $\sum_{i=1}^n w_i \mathrm{tr}(\rho \Pi_i)$

Upper bound for non-contextual models: $\alpha(G, \vec{w})$

State independent contextuality witness

$$\sum_{i=1}^{n} w_i \mathrm{tr}(\rho \Pi_i) > \alpha(G, \vec{w})$$

is a state independent quantum realization of contextuality witness for dimension d, if there is a quantum realization $\{\Pi_i\}_{i=1}^{n}$ of $\{e_i\}_{i=0}^{n}$ such that

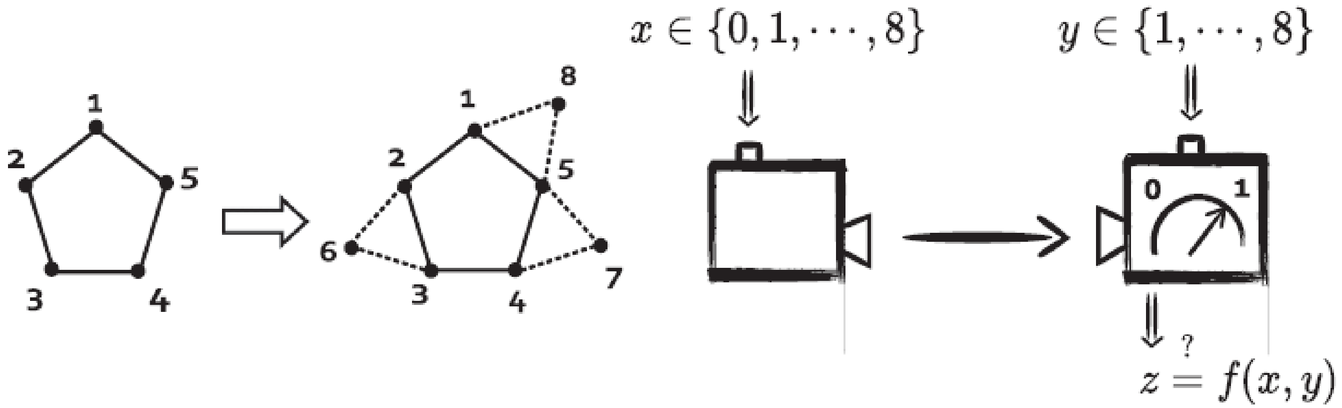
$$\sum_{i=1}^{n} w_i \mathrm{tr}(\rho \Pi_i) > \alpha(G, \vec{w})$$

holds $\forall \rho \in \mathcal{O}(\mathbb{C}^d)$ (set of quantum states in $\mathbb{C}^d$)

split all projectors into rank-1 to obtain $\{(G, \vec{w}), \{|\psi_i\rangle\langle\psi_i|\}_{i=1}^{n}, \rho\}$ satisfying witness condition

One-way communication complexity

CC: amount of communication required for tasks involving two parties



Alice, receives a random input $x \in X$

Alice sends a message (classical or quantum) to Bob. Bob receives random input $y \in Y$

[extended graph **G** ➡ $\tilde{G}$ **s.t. every vertex belongs to one clique of size 3]**

clique: every pair adjacent

Using y, and message received from Alice, Bob outputs z: Bob's guess about function f(x,y)

Figure of merit of communication task: $S = \sum_{x,y} t(x,y) p(z = f(x,y)|x,y)$, $\sum_{x,y} t(x,y) = 1$

2 benchmarks: (I) Maximum value of S with (classical or quantum) dimension d

(II) Minimum dimension required (classical or quantum) to achieve a certain value of S

Communication complexity advantage based on contextuality witness

Result: If classical system is communicated between Alice and Bob:

$$S^{(\tilde{G},\vec{w},d)} \leq S_c^{(\tilde{G},\vec{w},d)} = \frac{1}{N}\left[n + k + \sum_{x=1}^{n+k} |N_x| + \alpha(G,\vec{w}) - \delta\right]$$

$G \Rightarrow \tilde{G}$

$n \Rightarrow n + k$

δ : minimum number of improperly colored vertices of $\tilde{G}$ when d colors are used

N_x : set of vertices that are adjacent to x in $\tilde{G}$

Quantum advantage when above bound is violated

Reverse statement holds under an additional assumption:

Contextuality can be certified from communication complexity

S. Gupta, D. Saha, Z.-P. Xu, A. Cabello, A. S. Majumdar, Phys. Rev. Lett. **130**, 080802 (2023)

Increasing advantage in communication complexity

Contextuality witnesses for $\chi(G) > d_{\min}$ (equality problem)

Simplified version $S^G = \frac{1}{N}\left[\sum_{x=1}^{n} p(z=0|x, y=x) + \sum_{x=1}^{n}\sum_{y\in N_x} p(z=1|x,y)\right]$ $N = n + \sum_{x=1}^{n} |N_x|$

Minimum dimension of quantum system $Q(G)$ or classical system $C(G)$

in order to achieve $S^G = 1$

Result: $\frac{C(G^m)}{Q(G^m)} \geq \left(\frac{\chi_f(G)}{d_{\min}}\right)^m, \quad \text{for } m \in \mathbb{N}$

G^m : m times G; χ_f fractional chromatic number

$d_{\min}$: minimum dimensions in which

$\{(G, \vec{w}), \{|\psi_i\rangle\langle\psi_i|\}_{i=1}^{n}, \rho\}$ is a contextuality witness

For particular example (equality problem)

$$\frac{C(G_{N_d})}{Q(G_{N_d})} \geq \frac{1}{d}\left(\frac{2}{1.99}\right)^d$$

Gap between classical and quantum complexities can be very large !

Gap between classical and quantum communication complexities: examples

TABLE I. In order to compare the quantum advantages originated from various SI contextuality witnesses, we have taken the value of m for each set such that 200 qubits is sufficient to accomplish the respective equality problem. With respect to that, the lower bounds on the classical and quantum ratios have been obtained for various SI contextuality witnesses.

SI witness with n	$d_{\min}$	$\chi_f(G)$	$C(G^m)/Q(G^m)$ from Eq. (13) so that $d_{\min}^m \sim 200$ qubits
YO-13 [25]	3	35/11	$\geq 6 \times 10^{13}$
Peres-33 [47]	3	13/4	$\geq 4 \times 10^{13}$
CEG-18 [48]	4	9/2	$\geq 3.4 \times 10^{7}$
Pauli-240 [49]	8	15	$\geq 1.9 \times 10^{18}$
Pauli-4320 [49]	16	60	$\geq 5 \times 10^{28}$

$\chi_f(G)$ is the fractional chromatic number of G $\qquad \chi_f(G) \leq \chi(G)$

S. Gupta, D. Saha, Z.-P. Xu, A. Cabello, A. S. Majumdar, Phys. Rev. Lett. **130**, 080802 (2023)

Quantum Measurements Drive Quantum Communication (summary)

D. Saha, D. Das, A. K. Das, B. Bhattacharya, A. S. Majumdar, Phys. Rev. A **107**, 062210 (2023); S. Gupta, D. Saha, Z.-P. Xu, A. Cabello, A. S. Majumdar, Phys. Rev. Lett. **130**, 080802 (2023); A. K. Das, S. Mukherjee, D. Saha, D. Das, A. S. Majumdar, arXiv: 2401.01236.

- MI is fundamental quantum resource for non-classicality in communication tasks
- Violation of classical bound of any communication tasks is sufficient to witness measurement incompatibility
- Operational approach towards classifying incompatibility under: (i) Coarse-graining of outcomes, (ii) convex mixing of measurements, (iii) environmental noise
- Any quantum state and observables in producing contextuality $\Longleftrightarrow$ quantum advantage in communication
- As the number of inputs increases the ratio between classical and quantum complexities increases polynomially – significant for equality problems in Comp. Science applications
- **Future directions**: More efficient (optimal) MI witnesses; Witnesses for incompatible channels and instruments; applications in equality problems with more than two parties, etc.

THANK YOU

Semi-device-independent QKD protocol and its security using monogamy of contextuality witnesses

Semi-device-independent quantum key distribution

Protocol:

After large no. of runs Alice randomly choses some runs and publicly announces her input x

Bob verifies that the figure of merit is greater than S_c

Bob publicly announce his input y for the remaining runs

$$f(x,y) = \begin{cases} 0, & \text{if } y = x, \\ 1, & \text{if } y \in N_x, \\ 0, & \text{if } y \in \{1,\ldots,n\} \text{ and } x = 0 \end{cases}$$

Alice notes down $f(x,y)$ as the shared key

Transmission unsuccessful when $y \notin \{x, N_x\}$ or $y \in \{n+1, \ldots, n+k\}$ and x=0

S. Gupta, D. Saha, Z.-P. Xu, A. Cabello, A. S. Majumdar, Phys. Rev. Lett. **130**, 080802 (2023)

Security of QKD protocol

Monogamy between two contextuality witnesses [Ramanathan et al. PRL 109, 050404 (2012)]

$$\sum_{i=1}^{n} w_i \mathrm{tr}[\rho(\Pi_i \otimes \mathbb{1})] + \sum_{i=1}^{n} w_i \mathrm{tr}[\rho(\mathbb{1} \otimes \bar{\Pi}_i)] \leq 2\alpha(G, \vec{w})$$

Even if Eve shares arbitrary correlations with the preparation device of Alice,

$$\sum_{y=1}^{n} w_y p_B(0|x=0,y) + \sum_{y=1}^{n} w_y p_E(0|x=0,y) \leq 2\alpha(G, \vec{w})$$

Hence,

$$S_B + S_E \leq 2S_c^{(\tilde{G},\vec{w},d)}$$

Protocol is secure when Alice-Bob attain quantum advantage

$$S_B > S_c^{(\tilde{G},\vec{w},d)}$$

Key rate:

$$r = I(A:B) - I(A:E)$$

Mutual information === mutual dependence between two variables

$$\mathrm{I}(X;Y) = \sum_{y \in \mathcal{Y}} \sum_{x \in \mathcal{X}} P_{(X,Y)}(x,y) \log\left(\frac{P_{(X,Y)}(x,y)}{P_X(x)\,P_Y(y)}\right)$$

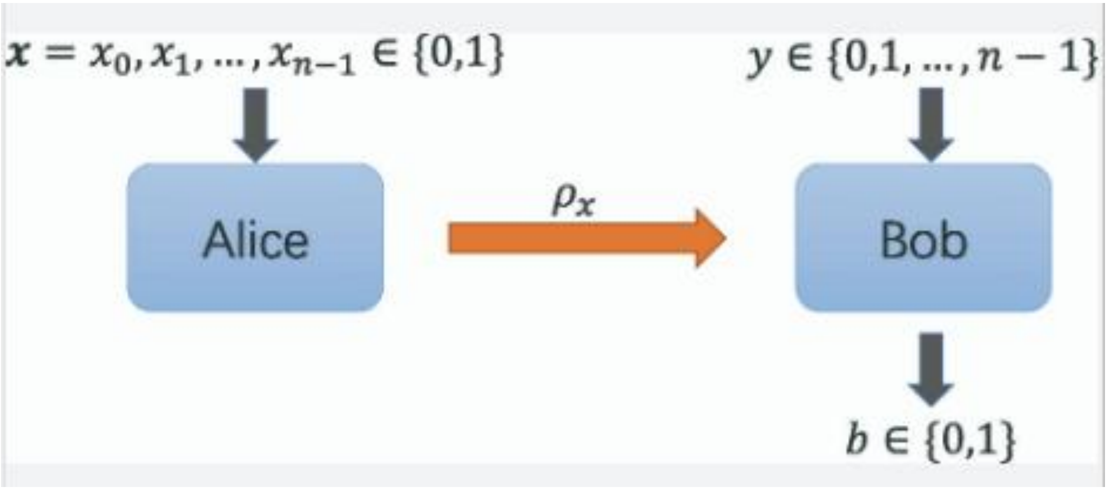
In terms of conditional and joint entropies:

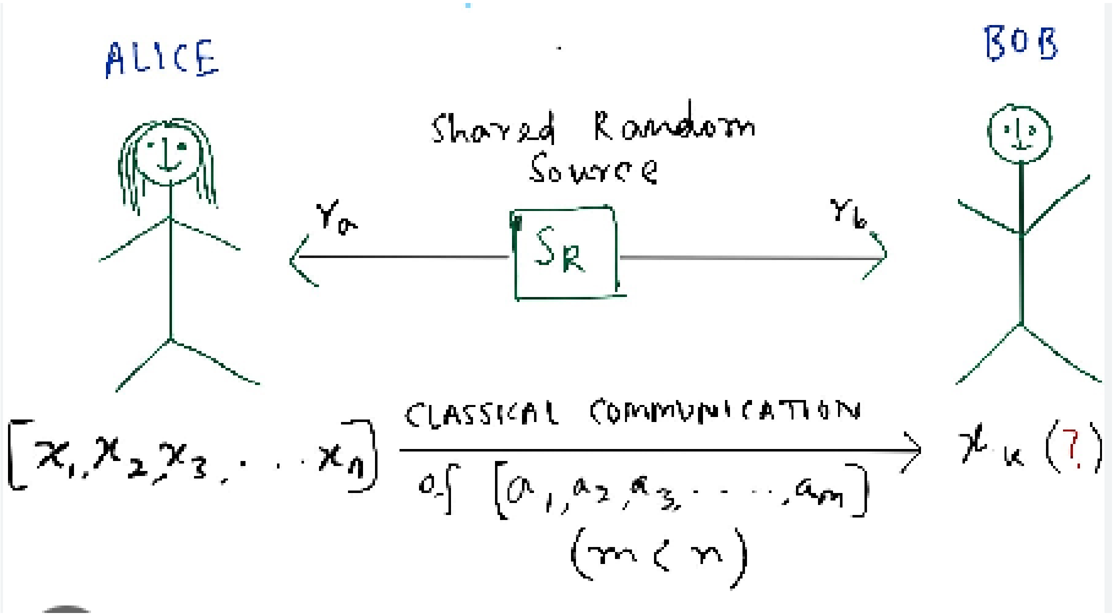
$$\mathrm{I}(X;Y) \equiv \mathrm{H}(X) - \mathrm{H}(X \mid Y)$$

$$\equiv \mathrm{H}(X,Y) - \mathrm{H}(X \mid Y) - \mathrm{H}(Y \mid X)$$

Communication tasks in prepare-and-measure scenario

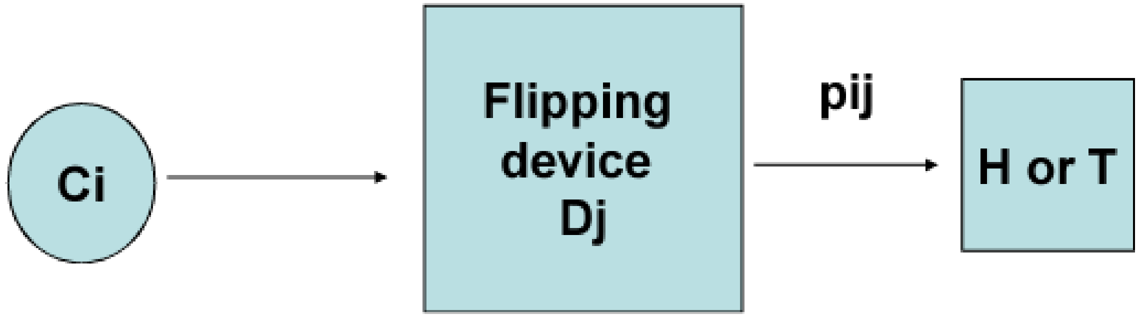
Generalized RAC games





Probability is a "contextual property" of a random experiment

The probability pij is neither a property of the coin nor the property of the flipping device Dj.It characterizes only a particular random experiment: Flipping Ci with a device Dj.



Marian Kupczynski

Experimental contexts

In QM one has conditional probabilities:

P(**A**=a)=P(**A**=a|C) where C is a context of the experiment in which A is measured

Pure state preparation: ψ vector in Hilbert space

Observable measured **A** : Â self adjoint operator

Experimental setup to measure **A:** A

E(**A**) =E(**A**|C)= E(**A**| ψ. A) =(ψ, Â ψ)

Local realism versus contextuality

- Local realism or counterfactual definiteness (CDF): measuring devices register values of physical observables existing independently whether they are measured or not.
- Contextuality: the values of contextual physical observables such as a spin projections are created in the interaction of the physical system with the measuring apparatus and they do not exist before the measurement

Bell-nonlocality produced by contextuality of spatially separated entangled systems

Quantum contextuality – simplest example [Peres-Mermin (PM) square]

Nine measurements arranged in a square

Each measurement is dichotomic: +1 or -1

$$\begin{bmatrix} A & B & C \\ a & b & c \\ \alpha & \beta & \gamma \end{bmatrix}$$

Assume 3 measurements in each row and column forms a "context"

$$\{ABC, abc, \alpha\beta\gamma, Aa\alpha, Bb\beta, Cc\gamma\}$$

$$\langle ABC \rangle \equiv \text{Prob}[ABC = +1] - \text{Prob}[ABC = -1]$$

Classical value assignment ("non-contextual"):

(there can be only an even number of

Products with assigned value +1)

$$\langle \text{PM} \rangle \equiv \langle ABC \rangle + \langle abc \rangle + \langle \alpha\beta\gamma \rangle + \langle Aa\alpha \rangle + \langle Bb\beta \rangle - \langle Cc\gamma \rangle \leq 4$$

Quantum example with 2 spin-1/2 particles

$$\begin{bmatrix} A & B & C \\ a & b & c \\ \alpha & \beta & \gamma \end{bmatrix} = \begin{bmatrix} \sigma_z \otimes \mathbb{1} & \mathbb{1} \otimes \sigma_z & \sigma_z \otimes \sigma_z \\ \mathbb{1} \otimes \sigma_x & \sigma_x \otimes \mathbb{1} & \sigma_x \otimes \sigma_x \\ \sigma_z \otimes \sigma_x & \sigma_x \otimes \sigma_z & \sigma_y \otimes \sigma_y \end{bmatrix}$$

$$\langle ABC \rangle = \langle \psi | ABC | \psi \rangle \qquad \langle \text{PM} \rangle = 6$$

QM violates non-contextual (classical) inequality

Quantum contextuality in practice

Implementation of PM square requires performing incompatible measurements on qubit

Non-contextuality inequalities in state-dependent scenario:

minimum dimension to witness contextuality is d = 3

(e.g., violation of KCBS inequality [Klyachko et al., PRL 101, 020403 (2008)])

Scenario defined by 5 measurements

KCBS inequality: $$\langle A_0 A_1 \rangle + \langle A_1 A_2 \rangle + \langle A_2 A_3 \rangle + \langle A_3 A_4 \rangle + \langle A_4 A_0 \rangle \geq -3$$

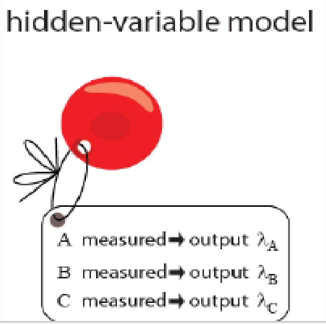
Quantum contextuality (Kochen-Specker proofs)

- Spectral decomposition says:
  observable $A = \sum_a \lambda_a \Pi_a$ where Π_a is a projector onto λ_a eigenspace.
- Consider B, C such that $\begin{cases} [A,B]=0 & \ldots\text{compatible} \\ [A,C]=0 & \ldots\text{compatible} \\ [B,C]\neq 0 & \ldots\text{incompatible} \end{cases}$

* Commuting/compatible observables can be jointly/sequentially measured without mutual disturbance: $ABAAB \rightarrow \lambda_a\lambda_b\lambda_a\lambda_a\lambda_b$ etc

* Free to measure A then decide whether to measure B or C.

- Born rule says Prob$(a|\psi) = ||\Pi_a|\psi\rangle||^2$
- Natural(?) to have a mental model whereby quantum state $|\psi\rangle$ possesses a value $v(A) \in \{\lambda_a\}$ revealed by measurement of A (irrespective of context)

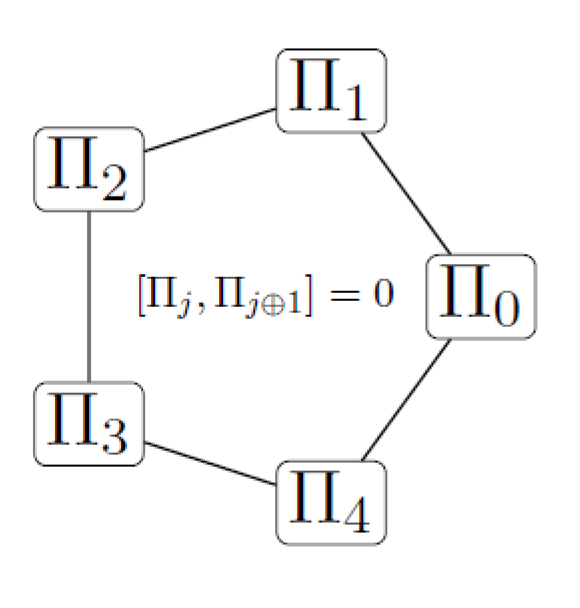


KS proof: Logical impossibility proof of value assignment

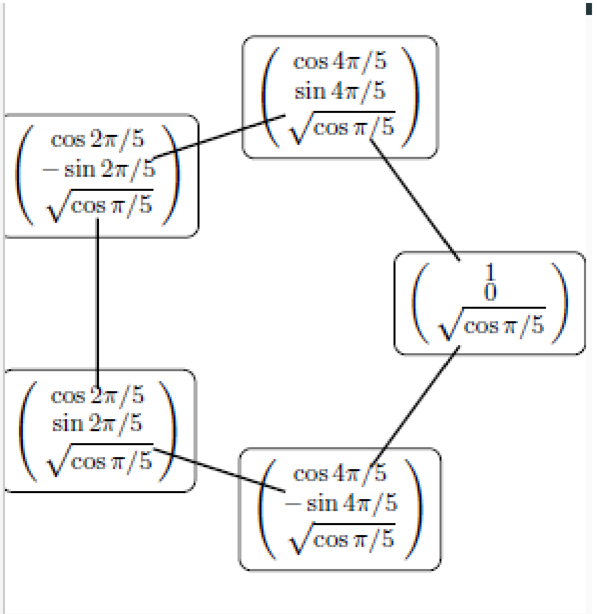
a

Acknowledgement: Mark Howard

Quantum Contextuality (state-dependent)



- $\{\Pi_i\}$ corresponds to a set of yes/no propositions
- In QM represent Π_i by projectors with $\lambda(\Pi_i) \in \{1, 0\}$
- Commuting rank-1 $\Pi_i \leftrightarrow$ mutually exclusive propositions
- Construct orthogonality/exclusivity graph Γ
- Define sum-of-projectors operator $\Sigma_\Gamma = \sum_{\Pi \in \Gamma} \Pi$



$$\langle \Sigma_\Gamma \rangle_{\max}^{\mathrm{NCHV}} = \alpha(\Gamma), \quad \langle \Sigma_\Gamma \rangle_{\max}^{\mathrm{QM}} \leq \vartheta(\Gamma)$$

$$\alpha(\Gamma) = 2, \quad \vartheta(\Gamma) = \sqrt{5} \approx 2.24$$

A. Cabello, S. Severini and A. Winter.
"(Non-)Contextuality of Physical Theories as an Axiom"
arXiv:1010.2163.

Discrimination of quantum state

Fundamental to the theory of quantum communication

<u>The question is</u>:
How can we best discriminate between a known set of states $|\psi_i\rangle$, each having been prepared with a known probability p_i ?

A general measurement (POVM) is generally the best approach

However, the "optimality of a measurement" is relative to the problem

Unambiguous state discrimination

Allow our measurement to have inconclusive results

If not inconclusive, it is always correct!

Minimum-error discrimination

Exists a necessary and sufficient condition

Optimization of Mutual information

Has only a necessary condition

In general, one does not apply the other!

(i.g. Tetrahedron states of Assignment 2)

Robust Self-Testing of Quantum Systems via Noncontextuality Inequalities

Kishor Bharti,[1] Maharshi Ray,[1] Antonios Varvitsiotis,[2] Naqueeb Ahmad Warsi,[1]
Adán Cabello,[3] and Leong-Chuan Kwek[1,4,5]
[1]*Centre for Quantum Technologies, National University of Singapore 117543, Singapore*
[2]*Department of Electrical & Computer Engineering, National University of Singapore 117583, Singapore*
[3]*Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*
[4]*MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, Singapore UMI 3654, Singapore*
[5]*National Institute of Education, Nanyang Technological University, Singapore 637616, Singapore*

(Received 8 January 2019; revised manuscript received 3 June 2019; published 26 June 2019)

Characterizing unknown quantum states and measurements is a fundamental problem in quantum information processing. In this Letter, we provide a novel scheme to self-test local quantum systems using noncontextuality inequalities. Our work leverages the graph-theoretic framework for contextuality introduced by Cabello, Severini, and Winter, combined with tools from mathematical optimization that guarantee the unicity of optimal solutions. As an application, we show that the celebrated Klyachko-Can-Binicioğlu-Shumovsky inequality and its generalization to contextuality scenarios with odd n-cycle compatibility relations admit robust self-testing.

DOI: 10.1103/PhysRevLett.122.250403

ARTICLE

doi:10.1038/nature13460

Contextuality supplies the 'magic' for quantum computation

Mark Howard[1,2], Joel Wallman[2], Victor Veitch[2,3] & Joseph Emerson[2]

Quantum computers promise dramatic advantages over their classical counterparts, but the source of the power in quantum computing has remained elusive. Here we prove a remarkable equivalence between the onset of contextuality and the possibility of universal quantum computation via 'magic state' distillation, which is the leading model for experimentally realizing a fault-tolerant quantum computer. This is a conceptually satisfying link, because contextuality, which precludes a simple 'hidden variable' model of quantum mechanics, provides one of the fundamental characterizations of uniquely quantum phenomena. Furthermore, this connection suggests a unifying paradigm for the resources of quantum information: the non-locality of quantum theory is a particular kind of contextuality, and non-locality is already known to be a critical resource for achieving advantages with quantum communication. In addition to clarifying these fundamental issues, this work advances the resource framework for quantum computation, which has a number of practical applications, such as characterizing the efficiency and trade-offs between distinct theoretical and experimental schemes for achieving robust quantum computation, and putting bounds on the overhead cost for the classical simulation of quantum algorithms.