Title: Exploring quantum correlations in causal networks

Speakers: George Moreno

Series: Quantum Foundations

Date: January 25, 2022 - 3:30 PM

URL: https://pirsa.org/22010083

Abstract: Bell's theorem is typically understood as proof that quantum theory is incompatible with local hidden variable (LHV) models. In recent years, however, LHV models have been recognized as a particular and simple case of much more general causal networks that can give rise to new and stronger forms of nonclassicality. And, since nonlocality is a resource in a variety of applications, it is thus natural to ask whether these novel forms of nonclassical behavior can also be put to use in information processing. In this seminar, I will present recent results exploring quantum correlations in several such causal scenarios, ranging from foundational questions such as freedom of choice in Bell experiments to more applied situations covering cryptography, distributed computing, and game theory.

Zoom Link: TBD

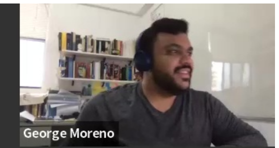
Exploring quantum correlations in causal networks

George Moreno

International Institute of Physics

January 25, 2022

marcosgeorge.mmf@gmail.com



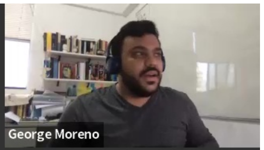
Nonclassicality

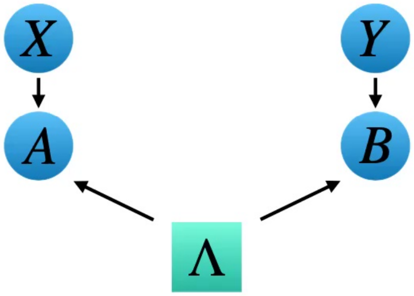
Applications

- Cryptography
- Game theory
- Communication Complexity Problems (CCP)
- Foundational questions

.
.
.

Bell Nonlocality





Distribution:

$$p(a, b|x, y)$$

Hypotheses

- Local realism:

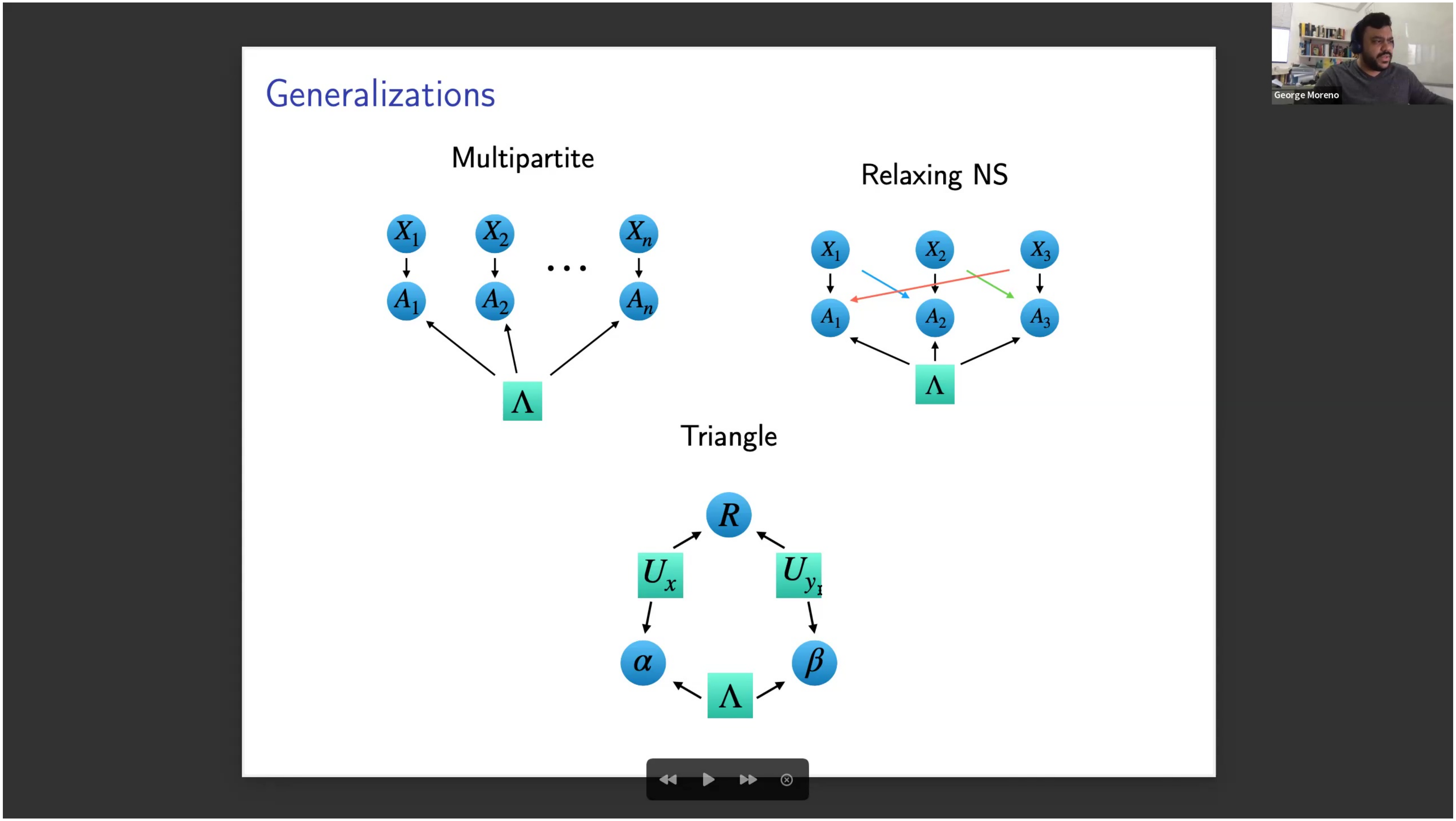
$$p(a, b|x, y) = \sum_{\lambda} p(a|x, \lambda)p(b|y, \lambda)p(\lambda)$$

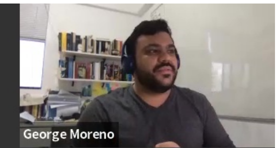
- Measurement independence

$$p(x, y, \lambda) = p(x, y)p(\lambda)$$

$\implies$ Set of correlations bounded by linear inequalities:

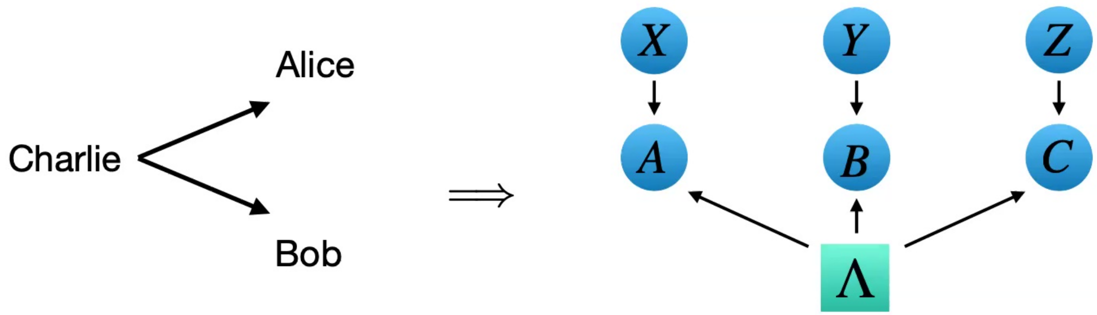
$$CHSH = E_{x=0,y=0} + E_{x=0,y=1} + E_{x=1,y=0} - E_{x=1,y=1} \leq 2$$


George Moreno
Generalizations
Multipartite
X_1 X_2 X_n
A_1 A_2 A_n
Λ
Relaxing NS
X_1 X_2 X_3
A_1 A_2 A_3
Λ
Triangle
R
U_x U_y
α β
Λ



Relaxing NS condition and secret sharing

Secret Sharing



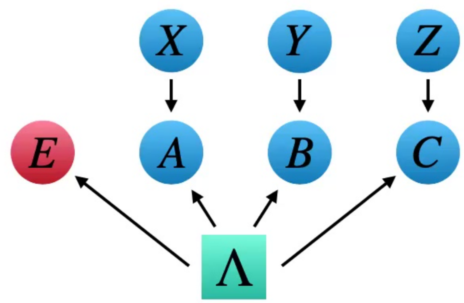
Each participant has a bit

- Charlie $\rightarrow c$
- Alice $\rightarrow a$
- Bob $\rightarrow b$

Such that, for some x^*, y^*, and z^*,

$$c = a \oplus b$$

Usual attack

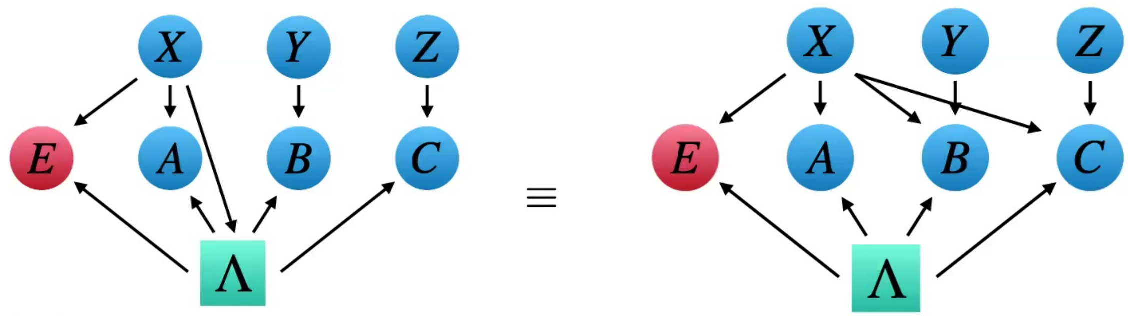


Eavesdropper goal → maximize $p(e = c|x^*, y^*, z^*)$

Solution:

- $p(a, b, c|x, y, z) = \text{tr}\left[(M_x^a \otimes M_y^b \otimes M_z^c)\rho\right]$
- $\rho = |GHZ\rangle\langle GHZ|$
- $M_{x=0}^0 - M_{x=0}^1 = M_{y=0}^0 - M_{y=0}^1 = M_{z=0}^0 - M_{z=0}^1 = \sigma_x$
- $M_{x=1}^0 - M_{x=1}^1 = M_{y=1}^0 - M_{y=1}^1 = M_{z=1}^0 - M_{z=1}^1 = \sigma_y$

Special attack



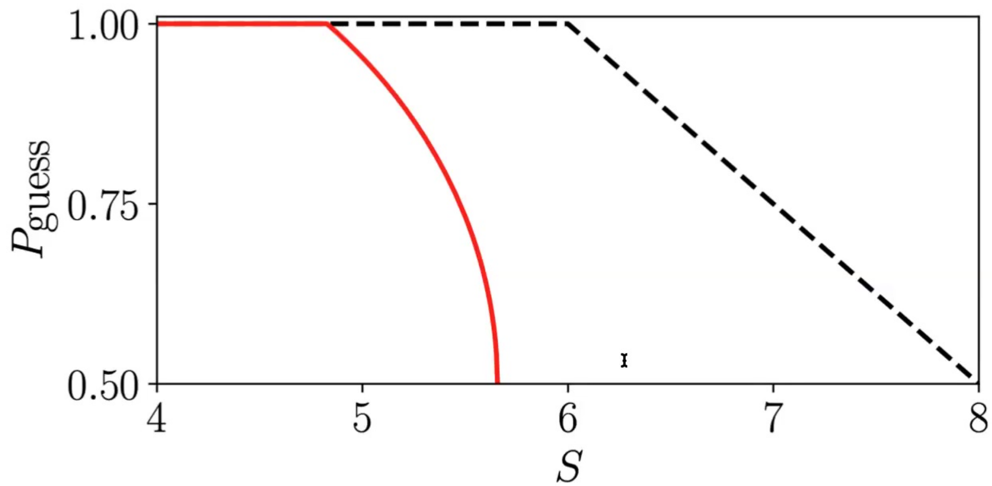
Solution:

$$S = 4\sqrt{2} \implies \text{security}$$

in which

$$S = p_A(0|0)\,CHSH_{00} - p_A(1|0)\,CHSH_{10} + p_A(0|1)\,CHSH'_{01} - p(1|1)\,CHSH'_{11}$$

Using the NPA relaxation, we observe that the result is robust



Phys. Rev. A **101**, 052339 (2020)

Relaxing NS condition and Game Theory

Bayesian games with advisor $\longleftrightarrow$ Bell nonlocality

Bayesian games

Player 2

Player 1	C	D
C	(-2,-2)	(0,-3)
D	(-3,0)	(-1,-1)

Elements of the game:

- N players
- Type $\Theta = \times_{i=1}^{n} \Theta_i$
- Actions $A = \times_{i=1}^{n} A_i$
- Payoff functions $\{u_i\}$ such that $u_i : \Theta \times A \mapsto \mathbb{R}$

How a correlation mediated by some variable Λ can affect a game (CCD)?

$$U_i = \sum_{\vec{a},\vec{\theta},\lambda} \left(\Pi_{i=1}^{n} p(a_i|\theta_i, \lambda)\right) p(\lambda) p(\vec{\theta}) u_i(\vec{\theta}, \vec{a})$$

$\Longrightarrow$ nonlocality may lead to new average payoffs.

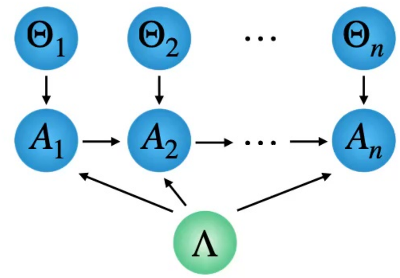
Multistage games

Elements of the game:

Bayesian game

$+$

History $\vec{h} = (h_1, \ldots, h_n)$



A better way of setting correlations (ECD):

$$U_i = \sum_{\vec{a},\vec{\theta},\lambda} \left(\Pi_{i=1}^{n} p(a_i|h_i,\theta_i,\lambda)\right) p(\lambda) p(\vec{\theta}) u_i(\vec{\theta},\vec{a})$$

We found scenarios in which

- QECD beats QCCD
- QCCD beats ECD
- QCCD ties with QECD that beats ECD

Phys. Rev. A **102**, 042412 (2020)

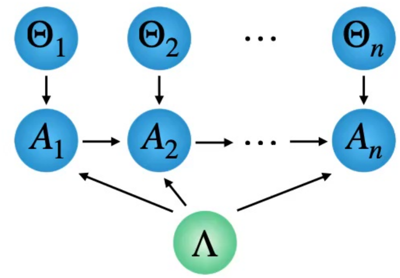
Multistage games

Elements of the game:

Bayesian game

$+$

History $\vec{h} = (h_1, \ldots, h_n)$



A better way of setting correlations (ECD):

$$U_i = \sum_{\vec{a},\vec{\theta},\lambda} \left(\Pi_{i=1}^{n} p(a_i | h_i, \theta_i, \lambda)\right) p(\lambda) p(\vec{\theta}) u_i(\vec{\theta}, \vec{a})$$

We found scenarios in which

- QECD beats QCCD
- QCCD beats ECD
- QCCD ties with QECD that beats ECD

Phys. Rev. A **102**, 042412 (2020)

Relaxing NS condition and CCP

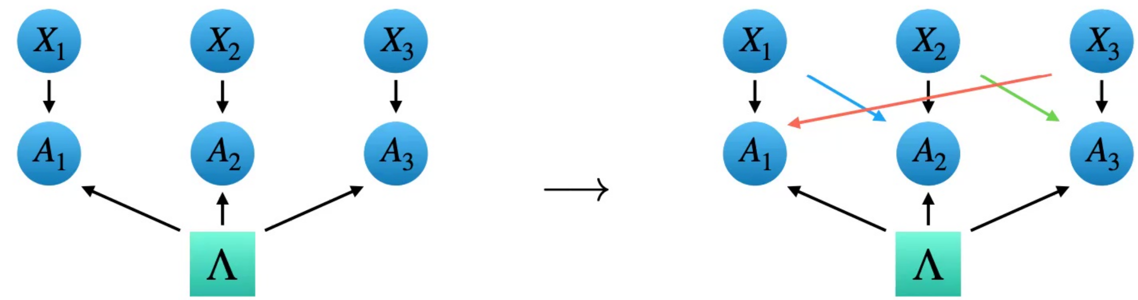
Communication Complexity Problem:

- Minimum amount of communication necessary to perform a task
- Success probability given a fixed communication

Brukner et al. (Phys. Rev. Lett. **92**, 127901 (2004)):

> *For every Bell's inequality, including those which are not known yet, there always exits a CCP, for which the protocol assisted by states which violate the inequality is more efficient than any classical protocol.*

Can we generalize this result?



Inequalities

$$B_n = \sum_{x_1,\dots,x_n=-1}^{1} Q(x_1,\dots,x_n) E_{x_1,\dots,x_n} \leq B_n^C$$

in which

$$E_{x_1,\dots,x_n} = \sum_{a_1,\dots,a_n=-1}^{1} a_1 \dots a_n p(a_1,\dots,a_n|x_1,\dots,x_n)$$

Task for n participants:

- Set $X = \{X_1, \ldots, X_n\} \to q(x_1, \ldots, x_n)$
- Set $Y = \{Y_1, \ldots, Y_n\} \to$ uniform distribution
- Participant i receives as input x_i, y_i, and some subset of X/x_i
- Each participant can broadcast a single bit message m_i
- Shared correlated system $\to$ part i has outcomes a_i

The goal is to evaluate,

$$f(\vec{x}, \vec{y}) = y_1 \ldots y_n S[Q(x_1, \ldots, x_n)]$$

George Moreno

Strategy

- Measures are labeled according with the set of inputs from X received
- Participant i announce $y_i a_i$
- The guess of participant i is:

$$G_i = \prod_{i=1}^{n} m_i = \prod_{i=1}^{n} y_i a_i$$

This strategy is optimal!

Probability of success:

$$P_{Suc} = \frac{1}{2} + \frac{B_n}{2\Gamma}$$

$\rightarrow$ Violation the inequality $\iff$ Higher P_{Suc}

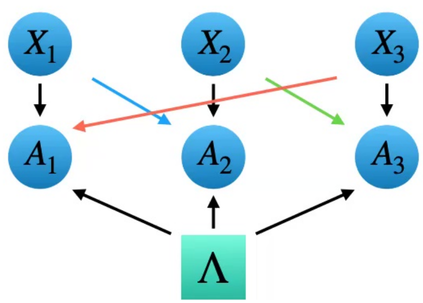
Experimental implementation

Guess-your-neighbor's-input scenario:

$$B_G = \sum_{x_1,x_2,x_3=-1}^{1} Q(x_1,x_2,x_3)E_{x_1,x_2,x_3} \leq 6$$

in which

$$Q(\vec{x}) = 1 - \frac{(1-x_1)(1-x_2)(1-x_3)}{4}$$



arXiv:2106.06552

Violation

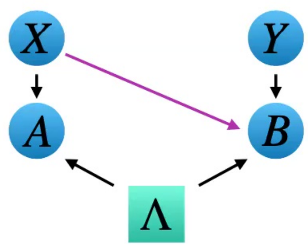
$$B_G = 7.023 \pm 0.036$$

Success probability

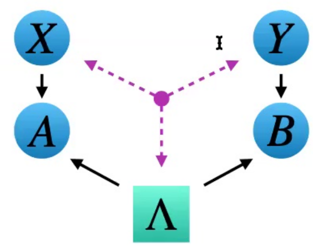
$$P_{Suc} = 0.9389 \pm 0.0049$$

Measurement dependence and Free Will

Measurement dependence in the CHSH scenario



Vs.



- Relaxing NS: maximal violation $\rightarrow 1 bit$
- Relaxing MD: maximal violation $\rightarrow 0.046 bit$

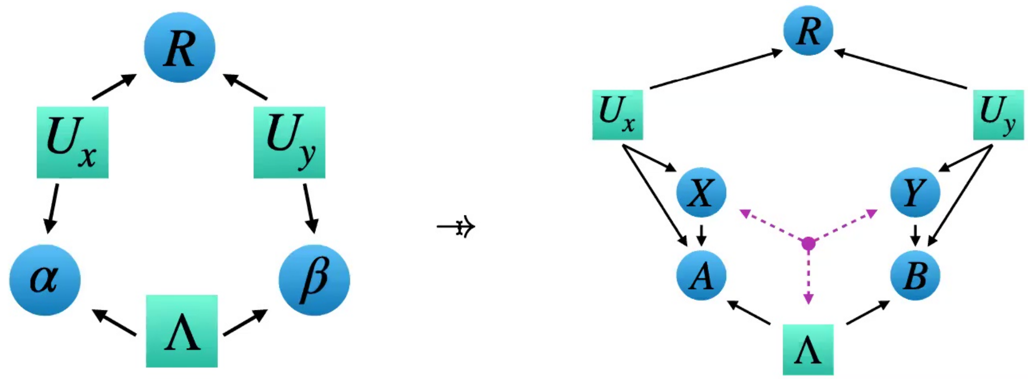
If $p(x, y)$ is uniform:

$$2 - h\left(\frac{4 - CHSH}{8}\right) - \frac{4 + CHSH}{8}\log_2 3 \leq I(X, Y : \Lambda)$$

or

$$(CHSH - 2)/4 \leq \mathcal{M}, \quad \text{for } \mathcal{M} = \sum_{x,y,\lambda} |p(x, y, \lambda) - p(x, y)p(\lambda)|$$

Tobias Fritz (New J. Phys. **14**, 103001 (2012))



Perfect correlation between R and (X, Y), e. g.,

$$p(x = 0, y = 0 | r = 0) = 1$$
$$p(x = 0, y = 1 | r = 1) = 1$$
$$p(x = 1, y = 0 | r = 2) = 1$$
$$p(x = 1, y = 1 | r = 3) = 1$$

implies that MI holds.

Entropic approach

$$h = (H(X_1), \dots, H(X_n), H(X_1, X_2), \dots, H(X_1, X_n), \dots)$$

Shannon cone Γ_n for n variables $\{X_1, \dots, X_n\}$

- Monotonicity
- Strong subadditivity
- $H(\varnothing) = 0$

Constrains implied by our structure

- $I(R : X, Y, \Lambda | U_x, U_y) = 0$
- $I(X : R, Y, U_y | \Lambda, U_x) = 0$
- $I(Y : R, X, U_x | \Lambda, U_y) = 0$

Using Fourier-Motzkin $\to I(X, Y : \Lambda) \leq \Theta(X, Y, R)$,

$$\Theta := \min \begin{cases} H(X, Y|R) \\ H(X, Y) - I(X : Y : R) - I(X : R) - I(Y : R) \\ H(X, Y) + H(R) - 2I(X : Y : R) - 2I(X : R) - 2I(Y : R) \end{cases}$$

If $p(x, y)$ is uniform:

$$2 - h\left(\frac{4 - CHSH}{8}\right) - \frac{4 + CHSH}{8}\log_2 3 \leq \Theta(X, Y, R)$$

or, we can use the fact that

$$\mathcal{M}^2 \leq \frac{I(X, Y : \Lambda)}{\log_2 e}$$

we get to

$$\frac{CHSH - 2}{4} \leq \sqrt{\frac{\Theta(X, Y, R)}{\log_2 e}}$$

Feasibility

Sources of correlation

$$\rho = v|\Psi\rangle\langle\Psi| + \frac{1-v}{4}\mathbb{1}$$

in which

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

For violation

$$v \approx 0.994$$

Nonclassicality

$$v \approx 0.907$$

PRX Quantum **2** 040323 (2021)

Conclusion

- Cryptography
- Game theory
- Communication Complexity Problems (CCP)
- Foundational questions

Thank you!

marcosgeorge.mmf@gmail.com