Optimal Measurement Structures for Contextuality Applications

Ravishankar Ramanathan

The University of Hong Kong

with Yuan Liu, Karol Horodecki, Monika Rosicka and Pawel Horodecki, arXiv: 2206.13139

Kochen Specker Theorem

Theorem (Kochen and Specker, Bell). There are sets of atomic propositions represented in quantum theory by vectors $\mathscr{V} := \{ |v_1\rangle, \ldots, |v_n\rangle \} \subset \mathbb{C}^d$, $d \geq 3$ that do not admit a deterministic non-contextual assignment $f : \mathscr{V} \to \{0,1\}$ satisfying

(i) Exclusivity: $\sum_{|v\rangle \in \mathscr{C} \subset \mathscr{V}} f(|v\rangle) \leq 1$ for every subset $\mathscr{C}$ of mutually orthogonal vectors, and

(ii) Completeness: $\sum_{|v\rangle \in \mathscr{C} \subset \mathscr{V}} f(|v\rangle) = 1$ for every subset $\mathscr{C}$ of d mutually orthogonal vectors.

The map f satisfying exclusivity and completeness is called a $\{0,1\}$ coloring of set $\mathscr{V}$.

S. Kochen and E. P. Specker. "The problem of hidden variables in quantum mechanics". Journal of Mathematics and Mechanics 17, 59 (1967).

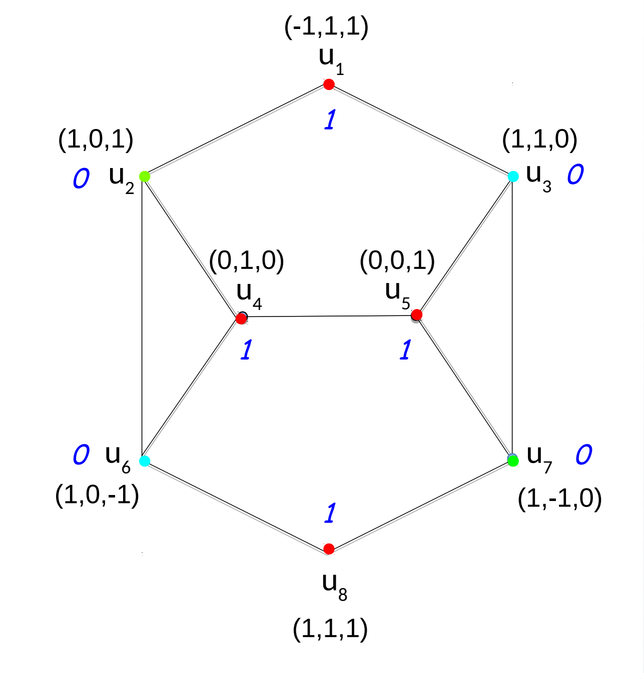
Statistical Proofs of Contextuality

An interesting class of statistical state-dependent proofs was studied by Clifton, Stairs, Hardy and others.

In these, a prediction occurs with certainty in non-contextual theories while this is not the case quantumly.

Considering each vector as an atomic proposition, studied sets are of the form $P \to Q$ or $P \to \overline{Q}$,

and have been termed as definite-prediction sets, true-implies-true (true-implies-false) sets, bugs or gadgets.



R. K. Clifton. American Journal of Physics 61: 443 (1993). A. Cabello , J. R. Portillo, A. Solis, K. Svozil. Phys. Rev. A 98, 012106 (2018).

R. R. et al. Quantum 4, 308 (2020).

Orthogonality Graphs

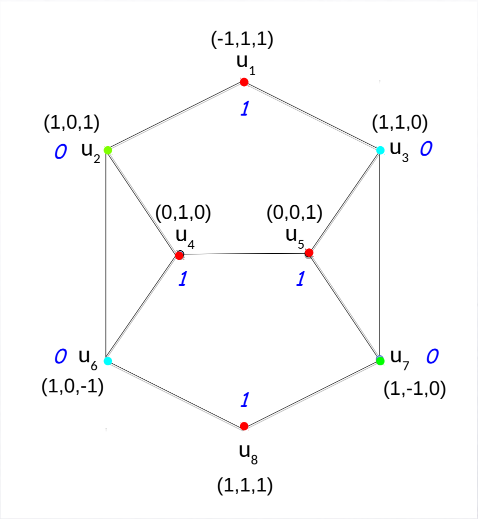
Orthogonality Graph: Represent each vector $|v_i\rangle$ by a vertex v_i of a graph.

Connect any two vertices v_1 and v_2 by an edge if $\langle v_1 | v_2 \rangle = 0$.

$d(G) \geq \omega(G)$ denotes the minimum dimension of an orthogonal representation of G.

Faithful Orthogonal Representation: $v_1 \sim v_2 \leftrightarrow \langle v_1 | v_2 \rangle = 0$ and $v_1 \neq v_2 \leftrightarrow |v_1\rangle \neq |v_2\rangle$.

$d^*(G)$ denotes the minimum dimension of a faithful orthogonal representation of G.

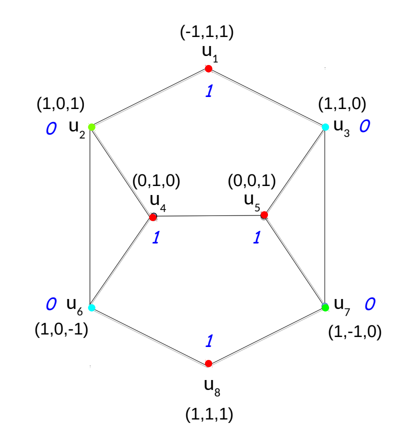


L. Lovasz, M. Saks and A. Schrijver. Linear Algebra and its Applications. 4, 114/115, 439 (1987).

A. Cabello, S. Severini and A. Winter. arXiv: 1010.2163 (2010). Phys. Rev. Lett. 112 040401 (2014).

Gadgets

Definition 1. *[8] A* 01*-gadget in dimension d is a* $\{0,1\}$*-colorable set $\mathcal{S}_{gad} \subset \mathbb{C}^d$ of vectors containing two distinguished non-orthogonal vectors $|u\rangle$ and $|v\rangle$ that nevertheless satisfy $f(u) + f(v) \leq 1$ in every* $\{0,1\}$*-coloring f of $\mathcal{S}_{gad}$. Equivalently, a* 01*-gadget in dimension d is a* $\{0,1\}$*-colorable graph G_{gad} with faithful dimension $d^*(G_{gad}) = \omega(G_{gad}) = d$ and with two distinguished non-adjacent vertices u and v such that $f(u) + f(v) \leq 1$ in every* $\{0,1\}$*-coloring f of G_{gad}.*



R. R. et al. "Gadget structures in proofs of the Kochen-Specker Theorem". Quantum 4, 308 (2020).

Higher-Order Gadgets

Definition 2. *A gadget of order* (m,k) *in dimension* d *is a* $\{0,1\}$*-colorable set of vectors* $\mathcal{S}_{m,k} \subset \mathbb{C}^d$ *containing* m *distinguished mutually non-orthogonal vectors* $\mathcal{S}_{m,k} = \{|v_1\rangle, \ldots, |v_m\rangle\}$*, such that*

- *for every subset* $\mathcal{R} \subset \mathcal{S}_{m,k}$ *of size* k*, there exists a* $\{0,1\}$*-coloring which attributes* 1 *to all vectors in* $\mathcal{R}$*, and*
- *for any subset* $\mathcal{R} \subset \mathcal{S}_{m,k}$ *of size greater than* k*, no* $\{0,1\}$*-coloring exists that attributes* 1 *to all vectors in* $\mathcal{R}$*.*

In words, gadgets of order (m, k) consist of m mutually non-orthogonal vectors such that at most k vectors can be assigned 1 in any $\{0,1\}$ coloring.

Y. Liu, R. R. et al. "Optimal measurement structures for contextuality applications". arXiv: 2206.13139

Significance of Gadgets in Contextuality - I

We show that Gadgets are a necessary ingredient in KS proofs.

Theorem 1. *Every KS set in dimension d contains a gadget of order $(k,k-1)$ for some k satisfying $2 \leq k \leq d$.*

We also show a constructive proof that higher-order $(k, k-1)$ gadgets for arbitrary k with the feature that the k distinguished vectors are arbitrarily close, $\langle m_i | m_j \rangle \to 1$.

Y. Liu, R. R. et al. "Optimal measurement structures for contextuality applications". arXiv: 2206.13139

E. Hrushovski and I. Pitowsky. "Generalizations of Kochen and Specker's theorem and the effectiveness of Gleason's theorem". Studies in History and Philosophy of Science Part B, 35(2):177-194 (2004).

Significance of Gadgets in Contextuality - II

We show that order $(k, k-1)$ Gadgets can be used as building builds to construct novel KS proofs

Fix a value of k in the range $\{2,\ldots,d\}$.

Construction 1. *The gadgets of order $(k,k-1)$ can be used as building blocks (together with a set of bases) to construct Kochen Specker proofs in dimension d.*

Step 1 We begin with k bases sets in dimension d, denoted as $B_1, B_2, \ldots, B_k$. We choose these sets such that no two vectors in different bases sets are identical or orthogonal to each other (one can do this by picking a single basis set B_1 and applying a suitable unitary matrix U_d to B_1).

Step 2 Construct all possible sets $S_i = \left\{|v^q_{B_p}\rangle\right\}$ with $p \in [k] := \{1,\ldots,k\}$ and $q \in [d]$, obtained by choosing a single vector $|v^q_{B_p}\rangle$ from each basis set B_p. In total, we thus have d^k sets S_i with $|S_i| = k$ for each $i \in [d^k]$.

Step 3 Construct for each $i \in [d^k]$ an order $(k,k-1)$ gadget in dimension d with the vectors in the set S_i being the distinguished vectors. Such a gadget can be built following the construction in the previous section, notice that an order $(k,k-1)$ gadget in dimension k serves also as an order $(k,k-1)$ gadget in all dimensions $d \geq k$ by the addition of computational basis vectors $|k+1\rangle, \ldots, |d\rangle$.

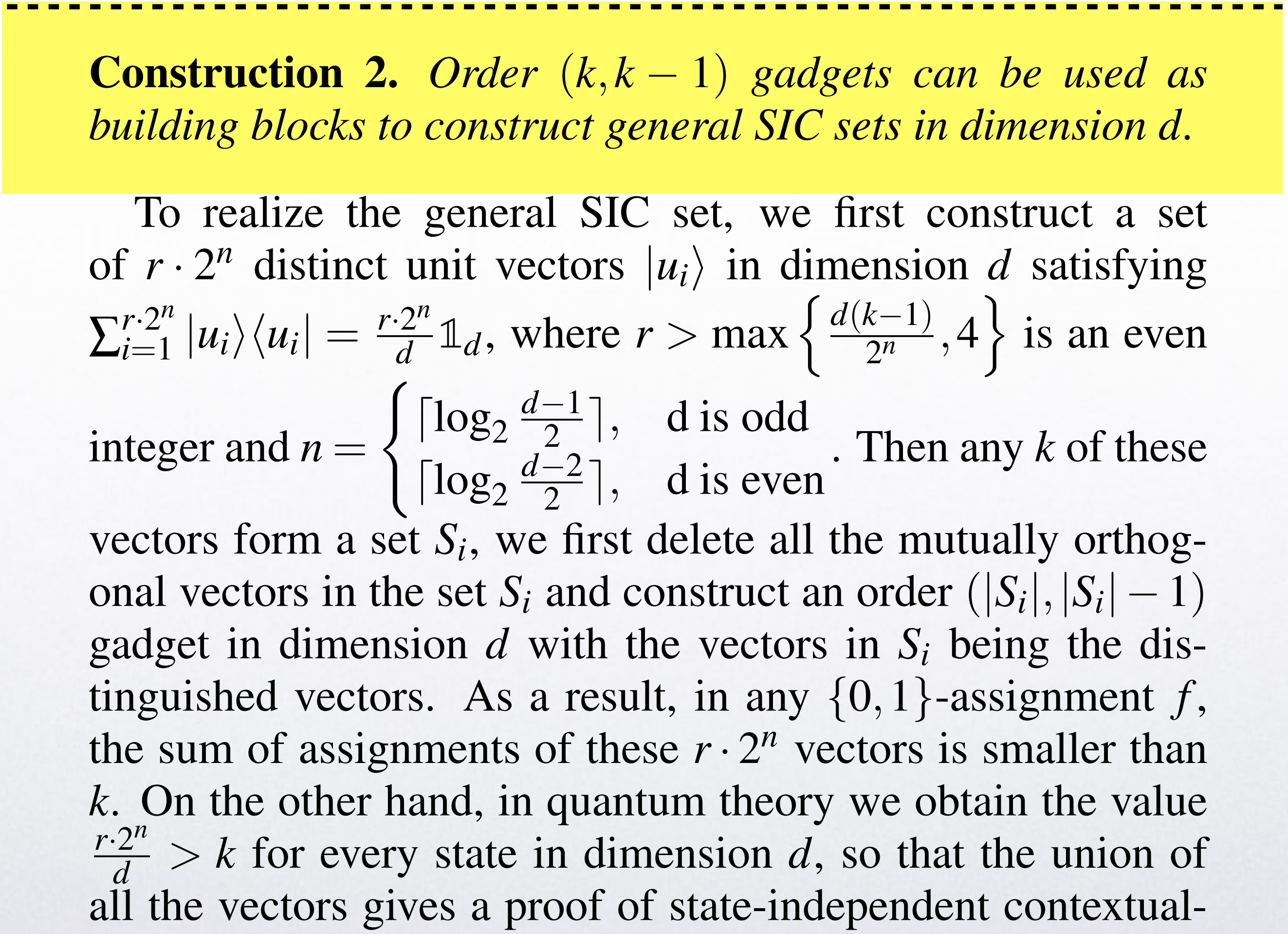
All the vectors in $B_1 \cup B_2 \cup \cdots \cup B_k \cup \mathcal{S}$ form a KS proof, where $\mathcal{S}$ denotes all the high-order gadgets used in Step 3. This follows from the fact that assigning a single value 1 to each of the bases $B_1, \ldots, B_{k-1}$ forces all the vectors in the basis set B_k to be assigned value 0 giving rise to a contradiction. □

Y. Liu, R. R. et al. "Optimal measurement structures for contextuality applications". arXiv: 2206.13139

R. R. et al. "Gadget structures in proofs of the Kochen-Specker Theorem". Quantum 4, 308 (2020).

Significance of Gadgets in Contextuality - III

We also show that order $(k, k-1)$ Gadgets can be used as building builds to construct novel general SIC proofs, a la Yu and Oh.



Construction 2. *Order $(k,k-1)$ gadgets can be used as building blocks to construct general SIC sets in dimension d.*

To realize the general SIC set, we first construct a set of $r \cdot 2^n$ distinct unit vectors $|u_i\rangle$ in dimension d satisfying $\sum_{i=1}^{r \cdot 2^n} |u_i\rangle\langle u_i| = \frac{r \cdot 2^n}{d}\mathbb{1}_d$, where $r > \max\left\{\frac{d(k-1)}{2^n}, 4\right\}$ is an even integer and $n = \begin{cases} \lceil \log_2 \frac{d-1}{2} \rceil, & \text{d is odd} \\ \lceil \log_2 \frac{d-2}{2} \rceil, & \text{d is even} \end{cases}$. Then any k of these vectors form a set S_i, we first delete all the mutually orthogonal vectors in the set S_i and construct an order $(|S_i|, |S_i| - 1)$ gadget in dimension d with the vectors in S_i being the distinguished vectors. As a result, in any $\{0,1\}$-assignment f, the sum of assignments of these $r \cdot 2^n$ vectors is smaller than k. On the other hand, in quantum theory we obtain the value $\frac{r \cdot 2^n}{d} > k$ for every state in dimension d, so that the union of all the vectors gives a proof of state-independent contextual-

Y. Liu, R. R. et al. "Optimal measurement structures for contextuality applications". arXiv: 2206.13139.

S. Yu and C. H. Oh. "State-Independent Proof of Kochen-Specker Theorem with 13 Rays". Physical Review Letters 108, 030402 (2012).

Significance of Gadgets in Contextuality - III

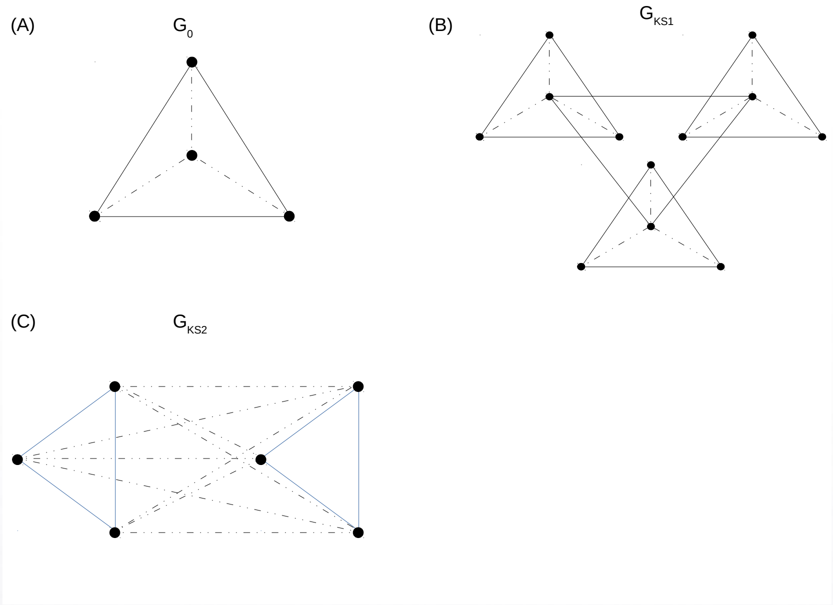
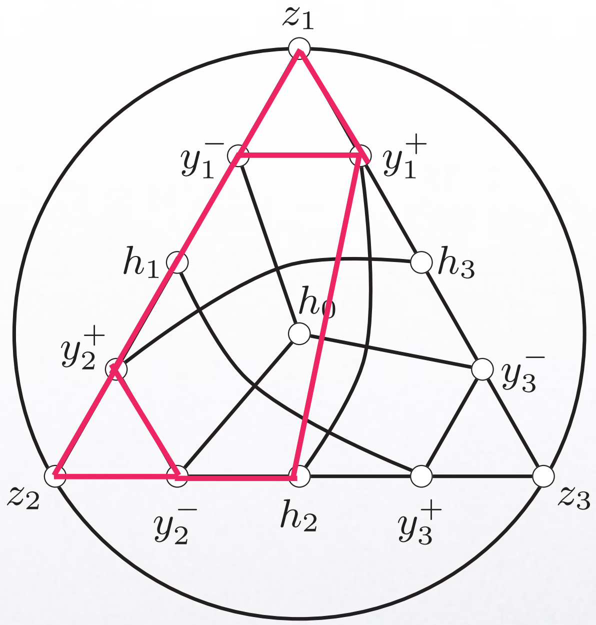


Figure 4: Graphs with the dashed edges denoting 01-gadgets. (a) In any $\{0,1\}$-coloring of the graph G_0, the central vertex is necessarily assigned value 0. (b) Three copies of G_0 with the central vertices forming a basis in $\mathbb{C}^3$ so that the resulting graph G_{KS1} forms a Kochen-Specker proof. (c) Another proof of the KS theorem G_{KS2} is obtained by connecting every pair of vectors in two bases by a 01-gadget.



R. R. et al. "Gadget structures in proofs of the Kochen-Specker Theorem". Quantum 4, 308 (2020).

A. Cabello. "Converting contextuality into nonlocality". Phys. Rev. Lett. 127, 070401 (2021).

Applications

1) Entanglement-Assisted Advantage in Zero-Error Capacity-I

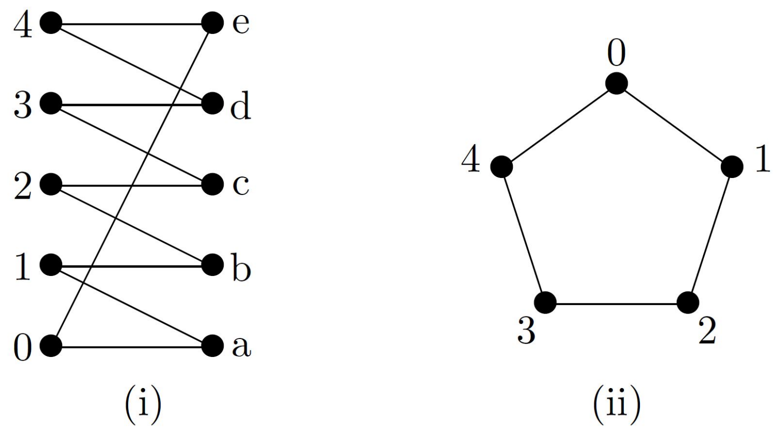
We consider a discrete, memoryless classical channel $\mathcal{N}$ connecting sender Alice and receiver Bob.

Given a single use of such a channel, the maximum number of messages that Alice can send to Bob under the constraint that there be no error is known as the one-shot zero-error capacity of $\mathcal{N}$.

The confusability graph $G(\mathcal{N})$ of channel $\mathcal{N}$ has vertex set as the set of input symbols and two vertices connected by an edge if the corresponding symbols are confusable.

Classically $c_{SR}(\mathcal{N}) = \alpha\left(G(\mathcal{N})\right)$.

Cubitt et al.: for G being a class of KS graphs $c_{SE}(\mathcal{N}) > \alpha\left(G(\mathcal{N})\right)$.



T. Cubitt, D. Leung, W. Matthews and A. Winter. "Improving zero-error classical communication with entanglement".

Physical Review Letters 104(23)

1) Entanglement-Assisted Advantage in Zero-Error Capacity-II

We show that shared entanglement also provides an enhancement of a weighted version of the zero-error communication capacity for a class of gadget graphs.

Assign weights $w = \{w_i\}_{i=1}^{|V|}$ to the input symbols denoting the desirability of their transmission.

The one-shot zero-error capacity is the maximum total weight of any set of non-confusable inputs.

Classically $c_{SR}(\mathcal{N}) = \alpha\left(G(\mathcal{N}), w\right)$.

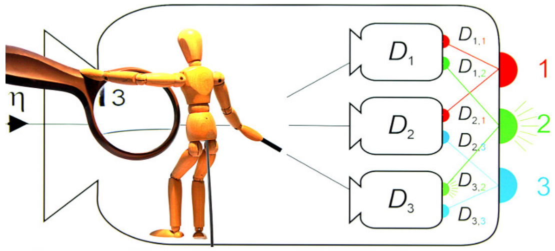
$$w_i = \begin{cases} w^* & i \in V_{\text{dist}} \\ 1 & i \in V \setminus V_{\text{dist}} \end{cases}$$

On the other hand, we prove that for weights chosen as above, for gadgets of order $(k,1)$ for $k > \omega(G)$, it holds that $c_{SE}(G(\mathcal{N}) > \alpha(G(\mathcal{N}), w)$. Such gadgets are $\{0,1\}$ – colorable so are not KS proofs.

Y. Liu, R. R. et al. "Optimal measurement structures for contextuality applications". arXiv: 2206.13139.

2) Using Gadgets to Test Fundamentally Binary Theories - I

Fundamentally Binary Theories are an interesting class of no-signalling theories where measurements yielding many outcomes are constructed out of binary measurements.



Kleinmann, Cabello and Vertesi constructed a Bell-type inequality to exclude the set of fundamentally binary non-signalling correlations as an underlying mechanism behind quantum correlations.

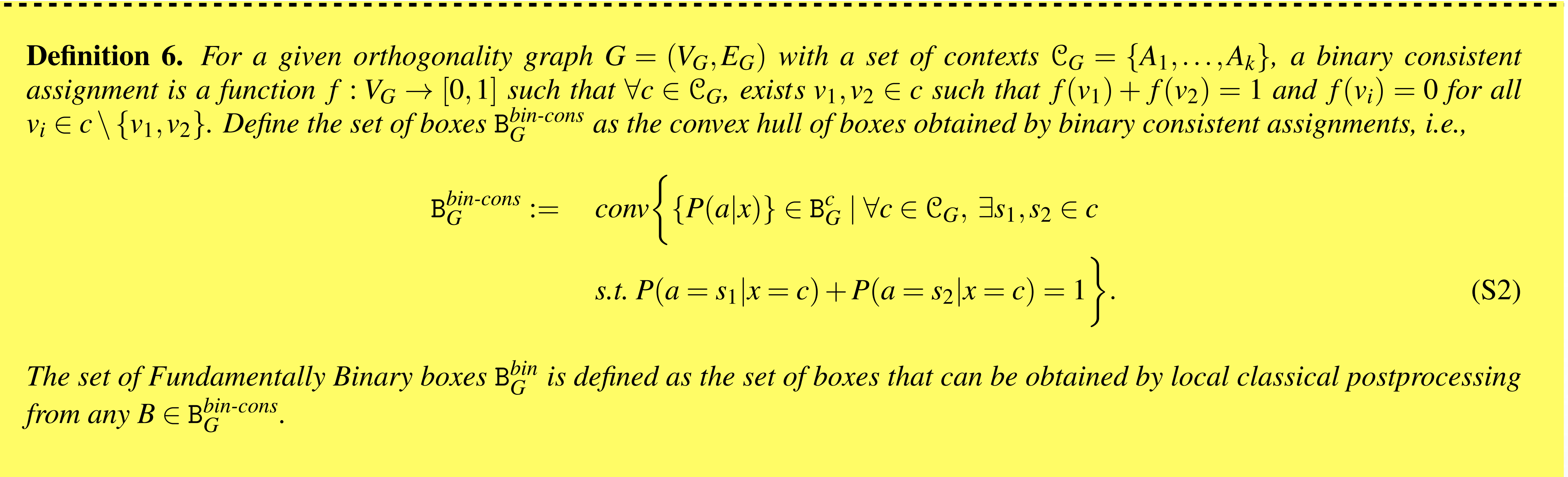
Their proof was experimentally demanding in that $I_q = 2(2/3)^{3/2} \approx 1.0887$ versus $I_{b-ns} = 1$.

We show that the genuinely ternary character of quantum measurements can be certified in a robust manner in a contextuality scenario using gadgets.

M. Kleinmann and A. Cabello. Physical Review Letters 117, 150401 (2016).

Hu et al. "Observation of stronger-than-binary correlations with entangled photonic qutrits". Phys. Rev. Lett. 120, 180402 (2018)

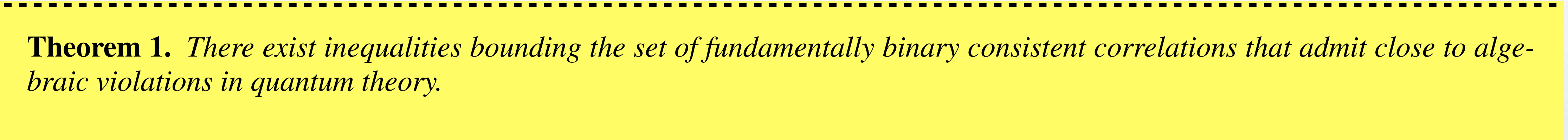
2) Using Gadgets to Test Fundamentally Binary Theories - II



Definition 6. *For a given orthogonality graph $G = (V_G, E_G)$ with a set of contexts $\mathcal{C}_G = \{A_1, \ldots, A_k\}$, a binary consistent assignment is a function $f : V_G \to [0,1]$ such that $\forall c \in \mathcal{C}_G$, exists $v_1, v_2 \in c$ such that $f(v_1) + f(v_2) = 1$ and $f(v_i) = 0$ for all $v_i \in c \setminus \{v_1, v_2\}$. Define the set of boxes $\mathsf{B}_G^{bin\text{-}cons}$ as the convex hull of boxes obtained by binary consistent assignments, i.e.,*

$$\mathsf{B}_G^{bin\text{-}cons} := \quad conv\Big\{\{P(a|x)\} \in \mathsf{B}_G^c \mid \forall c \in \mathcal{C}_G,\ \exists s_1, s_2 \in c \quad s.t.\ P(a = s_1|x = c) + P(a = s_2|x = c) = 1\Big\}. \tag{S2}$$

The set of Fundamentally Binary boxes B_G^{bin} is defined as the set of boxes that can be obtained by local classical postprocessing from any $B \in \mathsf{B}_G^{bin\text{-}cons}$.



Theorem 1. *There exist inequalities bounding the set of fundamentally binary consistent correlations that admit close to algebraic violations in quantum theory.*

Remark that such separations are not achieved with non-contextuality inequalities from KS proofs since both sets achieve the algebraic value for such inequalities.

Y. Liu, R. R. et al. "Optimal measurement structures for contextuality applications". arXiv: 2206.13139

3) Optimal Semi-device-independent randomness generation using gadgets

In general, proofs of contextuality do not specify which observables are value-indefinite.

For a contextuality test with observables $\{A_1, \ldots, A_k\}$ we want to solve

$$\begin{aligned} &\max P_{guess}(A_i|E) \\ &s.t.\ \ I(P_{A|X}) = I^*, \\ &\qquad P_{A,E|X} \in \mathcal{Q}, \end{aligned}$$

where $I(P_{A|X})$ is a non-contextuality inequality evaluated on observed $P_{A|X}, I^* \in (I_c, I_q]$ and

$\mathcal{Q}$ denotes the set of quantum boxes between Alice and adversary Eve, and

$P_{guess}(A_i|E) = \sum_e P(e)P_e(a = e|i)$ is the guessing probability of Alice's outcome by Eve.

Y. Liu, R. R. et al. "Optimal measurement structures for contextuality applications". arXiv: 2206.13139

S. Gupta, D. Saha, Zhen-Peng Xu, Adán Cabello, A. S. Majumdar.

"Quantum contextuality provides communication complexity advantage". arXiv:2205.03308

3) Optimal Semi-device-independent randomness generation using gadgets

The maximum randomness (min-entropy) per run that can be extracted from a test where the parties perform projective measurements on a system of dimension d is $\log_2 d$.

Optimal test in dimension d : (i) $\exists\, x^*$ s.t. $P_{A|X}(a\,|\,x^*) = 1/d \;\forall a \in [d]$ when I_q is observed.

(ii) the set of vectors realizing G is unique in $\mathbb{C}^{\omega(G)}$ up to unitaries.

We show that gadgets provide an ideal toolbox for this problem, by showing rigid constructions with overlap $|\langle v_1 | v_2 \rangle| = \frac{1}{\sqrt{d}}$, thus certifying $\log_2 d$ bits through an inequality $\beta P(|v_1\rangle) + P(|v_2\rangle) \leq \beta$.

Y. Liu, R. R. et al. "Optimal measurement structures for contextuality applications". arXiv: 2206.13139

4) Non-Monotonicity of Faithful Orthogonal Dimension of a Graph

Given a graph G that has a faithful orthogonal representation in $\mathbb{R}^{d^*_R(G)}$, we might expect that

$d_{R^*}(G \cup \{u, v\}) > d_{R^*}(G)$ and $d_{R^*}(G \backslash \{u, v\}) \leq d_{R^*}(G)$.

Is the graph property $P^{d,n}$ of graphs on n vertices which admit faithful ort. rep. in $\mathbb{R}^d$ monotone-decreasing?

Surprisingly we show that the answer to this question is negative:

There exist graphs with faithful orthogonal representation in $\mathbb{R}^3$ for which deleting a particular edge $\{u, v\}$ increases the faithful orthogonal dimension.

R.R., Y. Liu and P. Horodecki. New J. Phys. 24 033035 (2022).

Free Choice/Measurement Independence

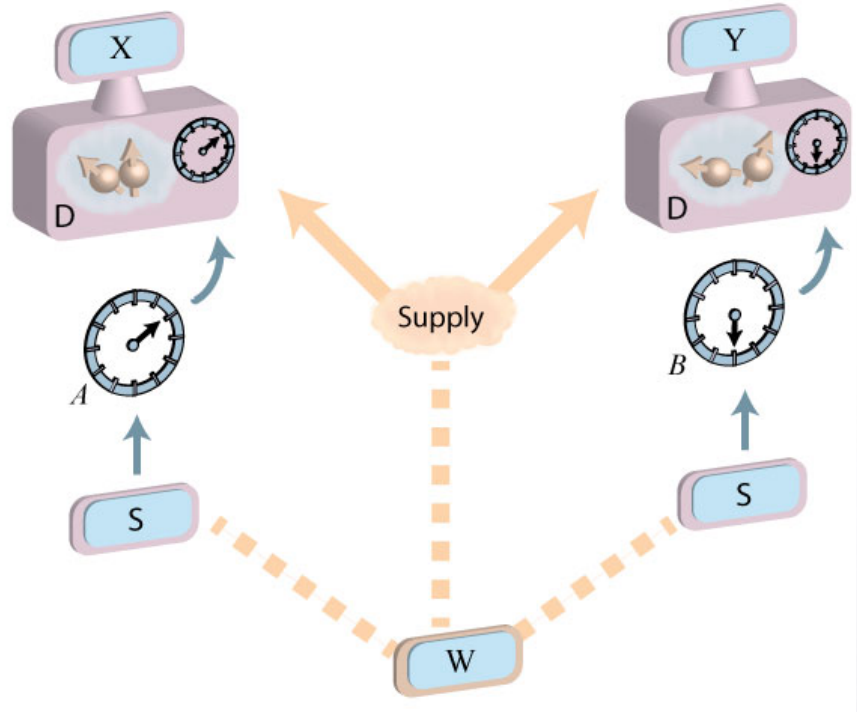
Free Choice/Measurement Independence

Given a set Γ with an (arbitrary) causal order, we can define the concept of a free choice as follows [12]:

> A choice $A \in \Gamma$ is *free* if A is uncorrelated with the set of all $W \in \Gamma$ that satisfy $A \not\rightarrow W$.

Said another way, A is free if the only variables it is correlated with are those it could have caused. Note that the condition $A \not\rightarrow W$ cannot be replaced by $W \rightarrow A$ [13].

Theorem 2—There exists a protocol that takes as input S_i and outputs R such that the following holds under the assumption NS: if S_i are ε-free, for any $\varepsilon < 0.058$, then R is certified to be arbitrarily free, except with arbitrarily small probability.



R. Colbeck and R. Renner. "Free randomness can be amplified". Nature Physics 8, 450-454 (2012).

R. Colbeck and R. Renner. "A short note on the concept of free choice". arXiv:1302.4446.

Bell inequalities: Assumptions

- Assumptions in deriving Bell inequalities:
  - Statistical Completeness/Outcome Independence: All statistical correlations arise from ignorance of the underlying variable λ

$$P(a_1, a_2|x_1, x_2, Q, \lambda) = P(a_1|x_1, x_2, Q\lambda)P(a_2|x_1, x_2, Q, \lambda)$$

    - True for deterministic models. Motivation: Underlying reality with measurement outcomes predetermined.

☞

  - Statistical Locality/Parameter Independence/No-Signaling: Distant measurements do not influence a party's underlying outcome prob. dist.

$$\begin{aligned} P(a_1|x_1, x_2, Q, \lambda) &= P(a_1|x_1, Q, \lambda), \\ P(a_2|x_1, x_2, Q, \lambda) &= P(a_2|x_2, Q, \lambda). \end{aligned}$$

    - Justification comes from Special Relativity when measurements are spacelike separated.

M. J. W. Hall, arXiv: 1511.00729 (2015).

Bell Inequalities: Assumptions

- Assumptions in deriving Bell inequalities:

☞

  - Measurement Independence/Free-Will: Measurement inputs (x_1,x_2) are uncorrelated with the underlying variable λ.

$$P(\lambda|x_1,x_2,Q) = P(\lambda|Q).$$

  - Reality is single valued, Fair Sampling, No Backward Causation, etc.

- Putting it all together, we obtain the Local Hidden Variable (LHV) model:

$$P(a_1,a_2|x_1,x_2,Q) = \int d\lambda P(\lambda|Q)P(a_1|x_1,\lambda,Q)P(a_2|x_2,\lambda,Q).$$

"Challenging local realism with human choices". The BIG Bell Test Collaboration. Nature 557, 212 (2018).

"Cosmic Bell Test: Measurement Settings from Milky Way Stars". Handsteiner et al. Phys. Rev. Lett. 118, 060401 (2017)

Device-Independent and Semi-Device-Independent Quantum Cryptography

Device-Independent (based on Non-locality) and Semi-Device-Independent (based on Contextuality and Steering)

Quantum Cryptography overcome the Implementation Attacks of existing Device-Dependent systems.

DI and SDI Quantum Crypto differ in their assumptions:

	Characterised Source/ Measurements/ Dimension/ Systems	Trusted Private Random Number Generator	Trusted Clocks + Classical Post-processing	Authenticated Classical Channel	No Information Leakage from Measurement Unit
Device-Independent	No	Yes	Yes	Yes	Yes
Semi-Device-Independent	Yes	Yes	Yes	Yes	Yes

Motivation: (Semi)-Device-Independent Quantum Cryptography

The difference in assumptions allows for different security features and different requirements in DI and SDI protocols catering to different applications:

	Security	Size	Rate	Ease of Implementation
Device-Independent	High Security against Quantum & Super-Quantum Adversaries	Spatially separated measurement stations (100m)	Low rate	Requires Loophole-free Bell tests with high visibility
Semi-Device-Independent	Security against Classical & Quantum Adversaries	Compact (single lab) devices	Rate of up to 10 kbps	Implementable in existing photonic setups

Xu et al. "Realistic quantum key distribution with realistic devices". Rev. Mod. Phys. 92, 025002 (2020)

Pirandola et al. "Advances in Quantum Cryptography". arXiv:1906.01645 (2019).

DI RANDOMNESS AMPLIFICATION – STATE-OF-ART

	Eve	Seed	Robustness	# Devices	Source-Device
Colbeck, Renner	NS	Public SV $\epsilon < 0.08$	1/N	2	Indep.
Acin group	NS	SV arb. ϵ	1/N	poly	Indep.
Kessler, A-Friedman	Q	SV arb. ϵ	Const.	2	Markov-chain
Chung, Shi, Wu	Q	H_{min}	Const.	poly	Arbitrary
Ramanathan et al.	NS	SV arb. ϵ	Const.	2	Indep.

R. Colbeck and R. Renner. Nat. Phys. 8, 450 (2012).
K.-M. Chung, Y. Shi and X. Wu. arXiv:1402.4797
R. Gallego et al. Nat. Comm. 4, 2654 (2013).
M. Kessler and R. A-Friedman. arXiv:1705.04148 (2017).

F. Brandao, R.R., A. Grudka, Horodecki^3, T. Szarek and H. Wojewodka. Nat. Comm. 7, 11345 (2016).
R. R. Et al. arXiv:2108.08819.
P. Horodecki and R. R. Nature Communications 10, 1701 (2019).

Towards DI-QRNG/QKD with Arbitrary Min-Entropy Seed

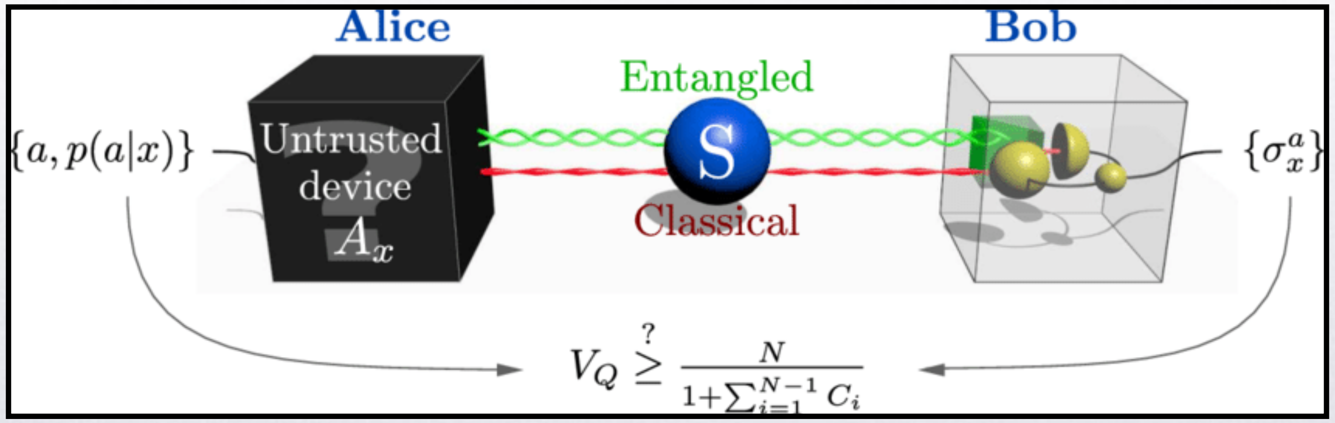
Goals: (i) (Further) closure of Measurement Independence in Fundamental Bell tests

(ii) Achieving DI-QRNG/DI-QKD with arbitrarily weak seeds of randomness.

R. R., Michał Banacki, Ricard Ravell Rodríguez, Paweł Horodecki.

"Single trusted qubit is necessary and sufficient for quantum realisation of extremal no-signaling correlations".

npj Quantum Information volume 8, Article number: 119 (2022) .



M. Banacki, P. Mironowicz, R. Ramanathan, P. Horodecki. New J. Phys. **24** 083003 (2022).

Summary

Gadgets capture the essential contradiction necessary to prove the Kochen-Specker theorem, i.e,

every Kochen-Specker graph contains a gadget and from every gadget one can construct a KS proof.

Gadgets provide an ideal toolbox for contextuality applications including

(i) constructing classical channels exhibiting entanglement-assisted advantage in zero-error communication,

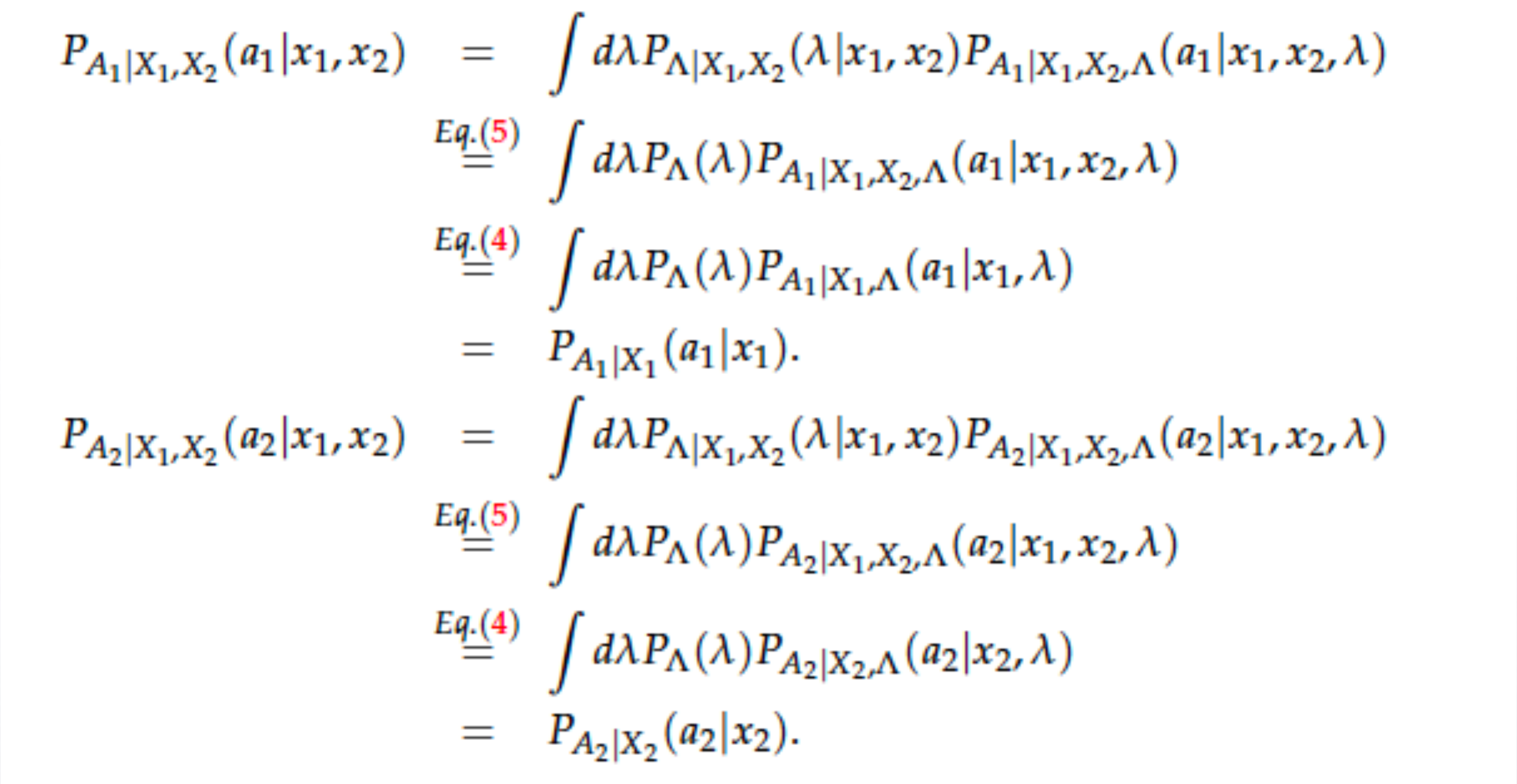
(ii) finding optimal tests for contextuality-based randomness generation and

(iii) identifying separations between quantum theory and binary generalised probabilistic theories.

Thank you!

No-Signalling

- One can ‘deduce’ the no-signalling constraints from the assumptions of measurement independence and parameter independence



$$\begin{aligned}
P_{A_1|X_1,X_2}(a_1|x_1,x_2) &= \int d\lambda P_{\Lambda|X_1,X_2}(\lambda|x_1,x_2)P_{A_1|X_1,X_2,\Lambda}(a_1|x_1,x_2,\lambda)\\
&\overset{Eq.(5)}{=} \int d\lambda P_{\Lambda}(\lambda)P_{A_1|X_1,X_2,\Lambda}(a_1|x_1,x_2,\lambda)\\
&\overset{Eq.(4)}{=} \int d\lambda P_{\Lambda}(\lambda)P_{A_1|X_1,\Lambda}(a_1|x_1,\lambda)\\
&= P_{A_1|X_1}(a_1|x_1).\\
P_{A_2|X_1,X_2}(a_2|x_1,x_2) &= \int d\lambda P_{\Lambda|X_1,X_2}(\lambda|x_1,x_2)P_{A_2|X_1,X_2,\Lambda}(a_2|x_1,x_2,\lambda)\\
&\overset{Eq.(5)}{=} \int d\lambda P_{\Lambda}(\lambda)P_{A_2|X_1,X_2,\Lambda}(a_2|x_1,x_2,\lambda)\\
&\overset{Eq.(4)}{=} \int d\lambda P_{\Lambda}(\lambda)P_{A_2|X_2,\Lambda}(a_2|x_2,\lambda)\\
&= P_{A_2|X_2}(a_2|x_2).
\end{aligned}$$

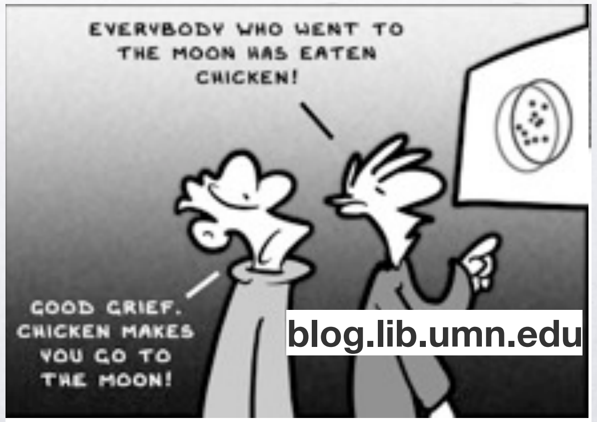
P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

Motivation for parameter independence: Causality

- As usual in Bell non-locality, let us work within the classical spacetime of Special Relativity.

- Causality: No causal loops. i.e. *No faster-than-light transmission of information from one spacetime location to another space-like separated location.*

- Causality violated if an effect at spacetime location A precedes its cause at spacetime location B ($t_A < t_B$) in some inertial reference frame.


EVERYBODY WHO WENT TO THE MOON HAS EATEN CHICKEN!
GOOD GRIEF. CHICKEN MAKES YOU GO TO THE MOON!
blog.lib.umn.edu

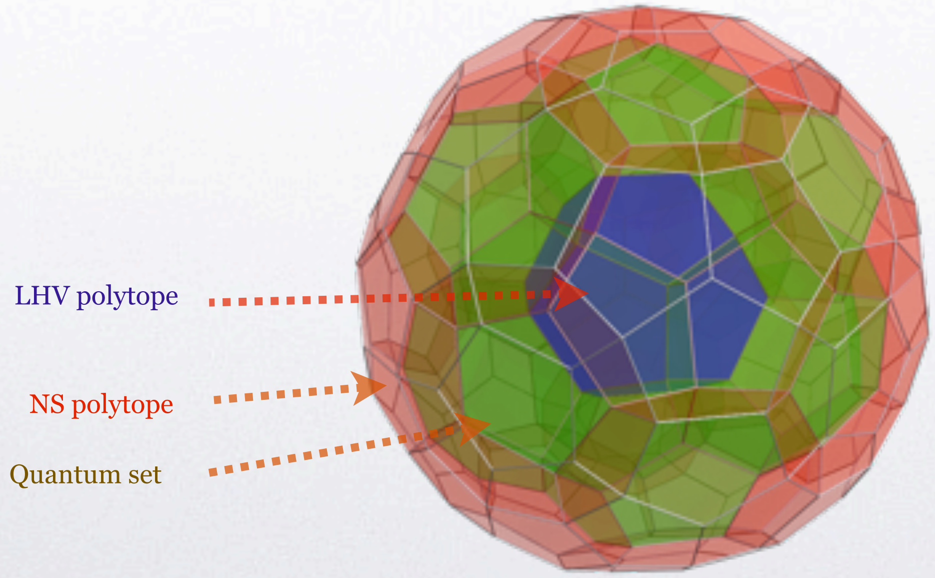
Correlation is not causation!

No-Signaling Polytope

- Box: Set of cond. prob. dist. P(**a**|**x**) = P(a_1,...,a_n|x_1,...,x_n).
- Non-negativity: P(**a**|**x**) ≥ 0. Normalization: $\sum_{\mathbf{a}}$ P(**a**|**x**) = 1.
- Multi-party No-Signaling (Directly generalize from the two-party case):

$$\boxed{\sum_{a_j} P(a_1,\ldots,a_j,\ldots,a_n|x_1,\ldots,x_j,\ldots,x_n) = \sum_{a_j} P(a_1,\ldots,a_j,\ldots,a_n|x_1,\ldots,x'_j,\ldots,x_n) \quad \forall j, x_j, x'_j, \mathbf{a}\setminus a_j, \mathbf{x}\setminus x_j.}$$

- LHV polytope ⊂ Quantum Correlations ⊂ No-Signaling Polytope

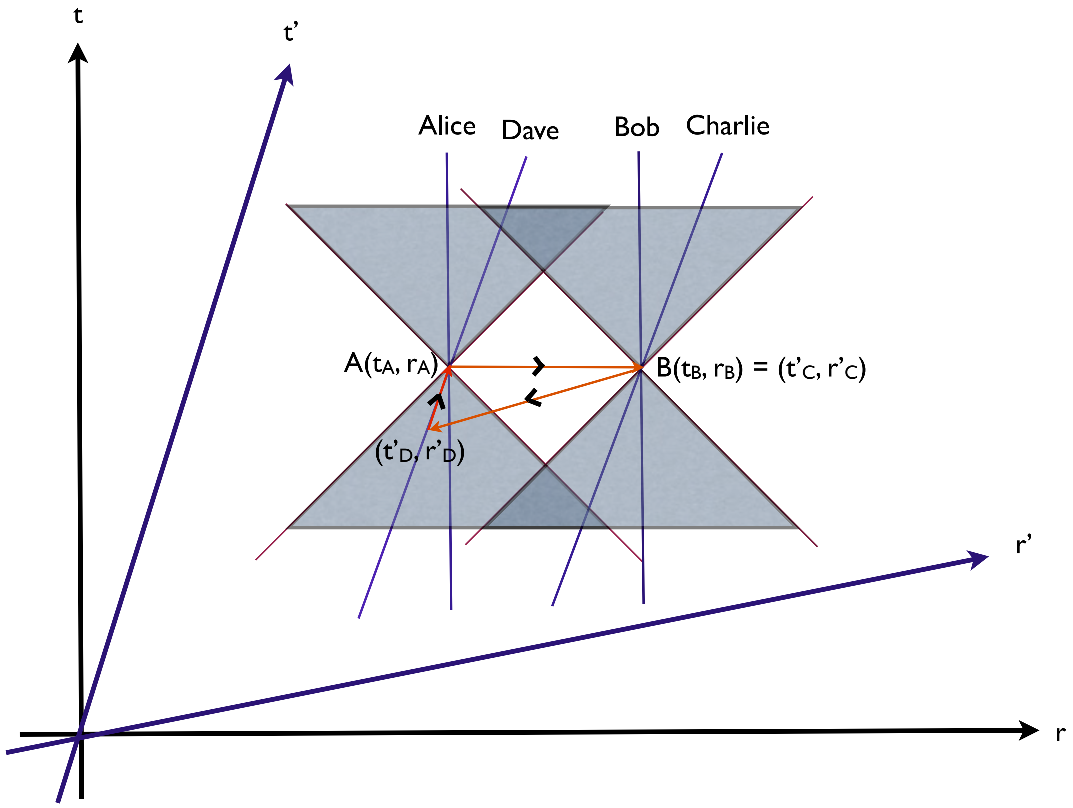


Consequence of causality?

Two-party No-Signaling from Relativistic Causality

- Formalism: Spacetime Random Variable (strv = r.v. generated at spacetime location (t,**r**)).
- Alice inputs x, obtains output a (instantaneously) at spacetime location A.
- Bob inputs y, obtains output b (instantaneously) at spacetime location B.
- FreeWill + Causality => NoSignaling.

$$
\begin{aligned}
P(a_1|x_1,x_2,Q,\lambda) &= P(a_1|x_1,Q,\lambda),\\
P(a_2|x_1,x_2,Q,\lambda) &= P(a_2|x_2,Q,\lambda).
\end{aligned}
$$



R. Colbeck and R. Renner, Free randomness can be amplified, Nature Physics 8, 450-454 (2012).

P. Horodecki and R. R., *in preparation*. P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

Multi-party No-Signaling from Relativistic Causality

- Spacetime rv's: Alice's measurement input-output rv's (x,a) at spacetime location A, Bob's (y,b) at B, Charlie's (z,c) at C.

- No-Signaling:

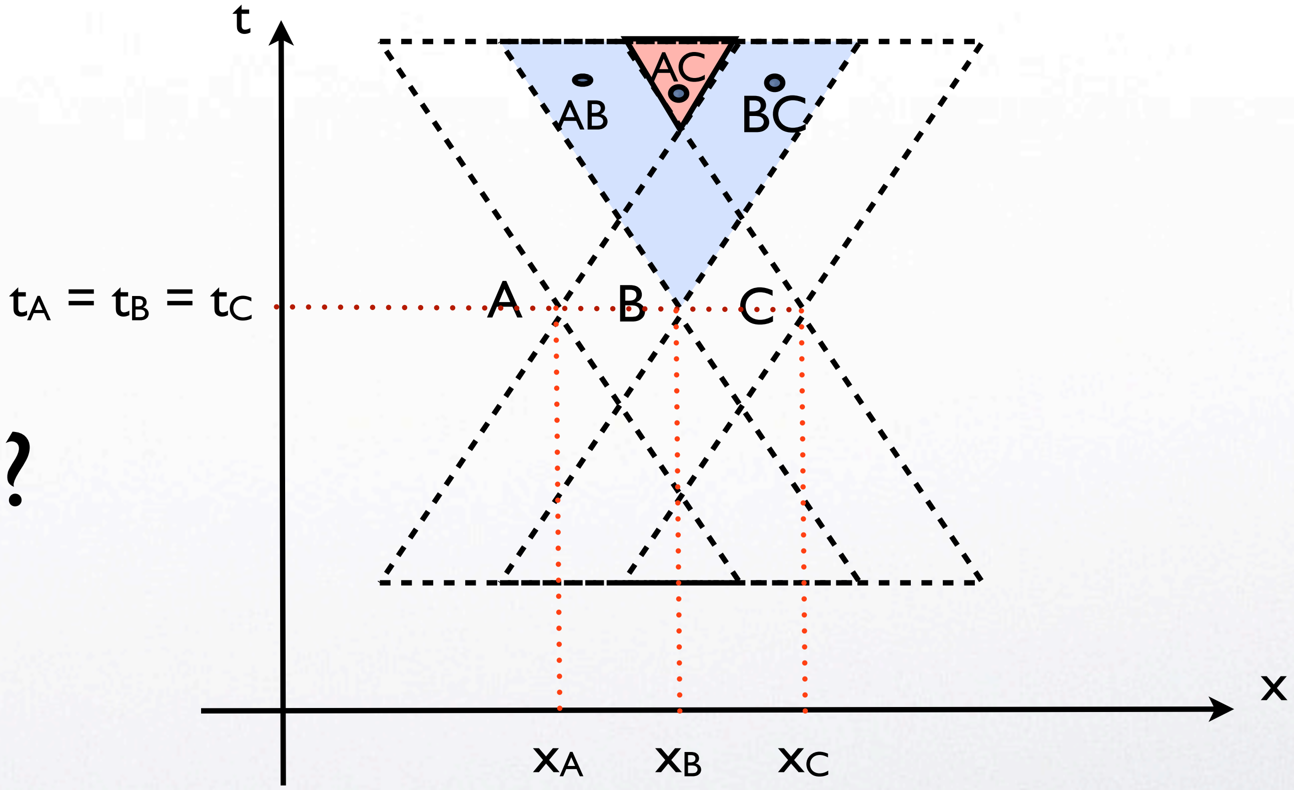
$$\sum_c P(a,b,c|x,y,z) = \sum_c P(a,b,c|x,y,z') \quad \forall z,z',a,b,x,y$$

$$\boxed{\sum_b P(a,b,c|x,y,z) = \sum_b P(a,b,c|x,y',z) \quad \forall y,y',a,c,x,z} \; ?$$

$$\sum_a P(a,b,c|x,y,z) = \sum_a P(a,b,c|x',y,z) \quad \forall x,x',b,c,y,z.$$

- AB output marginal independent of C's input.
  AC output marginal independent of B's input.
  BC output marginal independent of A's input.

- A, B, C individual marginals well-defined.



Notice that intersection of future light cones of A and C is contained within the future light cone of B

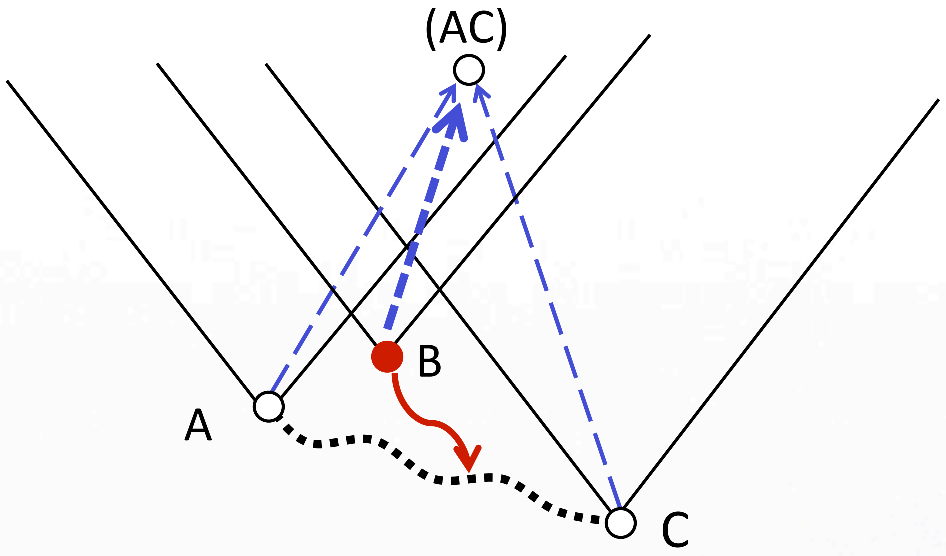
J. Grunhaus, S. Popescu and D. Rohrlich, Phys. Rev. A 53, 3781 (1996).
S. Popescu and D. Rohrlich, Non-Locality as an axiom for quantum theory, arXiv:9508009 (1995).
P. Horodecki and R. R., *in preparation*. P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

Multi-party No-Signaling from Relativistic Causality

- Observation: Alice and Bob check correlations at spacetime location AB (the correlations give rise to the spacetime variable AB at this location). Similarly, Alice-Charlie at AC as well as Bob-Charlie at BC.

- Argument: Suppose a (superluminal) influence propagates from B to AC, changing the correlations AC while keeping marginals A and C fixed.

- Proof: shows that such a influence does not lead to any causal loops.



- Justification: Spacetime random variable AC representing correlations is only registered at a point located within the future light cone of B. It means that effectively information has been sent from B to its future which ensures no causal loops.

J. Grunhaus, S. Popescu and D. Rohrlich, Phys. Rev. A 53, 3781 (1996).

S. Popescu and D. Rohrlich, arXiv:9605004 (1996).

P. Horodecki and R. R., *in preparation.* P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

Modified Multi-party No-Signaling from Relativistic Causality

- Modified 3-party constraints that prevent causality violations (when Bob is in appropriate space-time region):

$$\begin{aligned}
\sum_{c} P(a,b,c|x,y,z) &= \sum_{c} P(a,b,c|x,y,z') \quad \forall z,z',a,b,x,y\\
\sum_{a} P(a,b,c|x,y,z) &= \sum_{a} P(a,b,c|x',y,z) \quad \forall x,x',b,c,y,z\\
\sum_{a,b} P(a,b,c|x,y,z) &= \sum_{a,b} P(a,b,c|x',y',z) \quad \forall x,x',y,y',c,z\\
\sum_{b,c} P(a,b,c|x,y,z) &= \sum_{b,c} P(a,b,c|x,y',z') \quad \forall y,y',z,z',a,x.
\end{aligned}$$

- In general, in the n-party scenario (for a 1-D spatial arrangement of parties): Let $S_{m,k}^{n}$ denote a contiguous subset of [n] with initial element m and size k.

$$P(\mathbf{a}_{S^n_{m,k}}|\mathbf{x}_{S^n_{m,k}}) = \sum_{\mathbf{a}'_{(S^n_{m,k})^c}} P(\mathbf{a}'|\mathbf{x}') = \sum_{\mathbf{a}''_{(S^n_{m,k})^c}} P(\mathbf{a}''|\mathbf{x}'') \qquad \forall 1 \leq k \leq n-1, 1 \leq m \leq n-k+1$$

$$\text{for all } \mathbf{a}',\mathbf{a}'' \text{ with } \mathbf{a}'_{S^n_{m,k}} = \mathbf{a}''_{S^n_{m,k}} = \mathbf{a}_{S^n_{m,k}} \text{ and for all}$$

$$\mathbf{x}',\mathbf{x}'' \text{ with } \mathbf{x}'_{S^n_{m,k}} = \mathbf{x}''_{S^n_{m,k}} = \mathbf{x}_{S^n_{m,k}}.$$

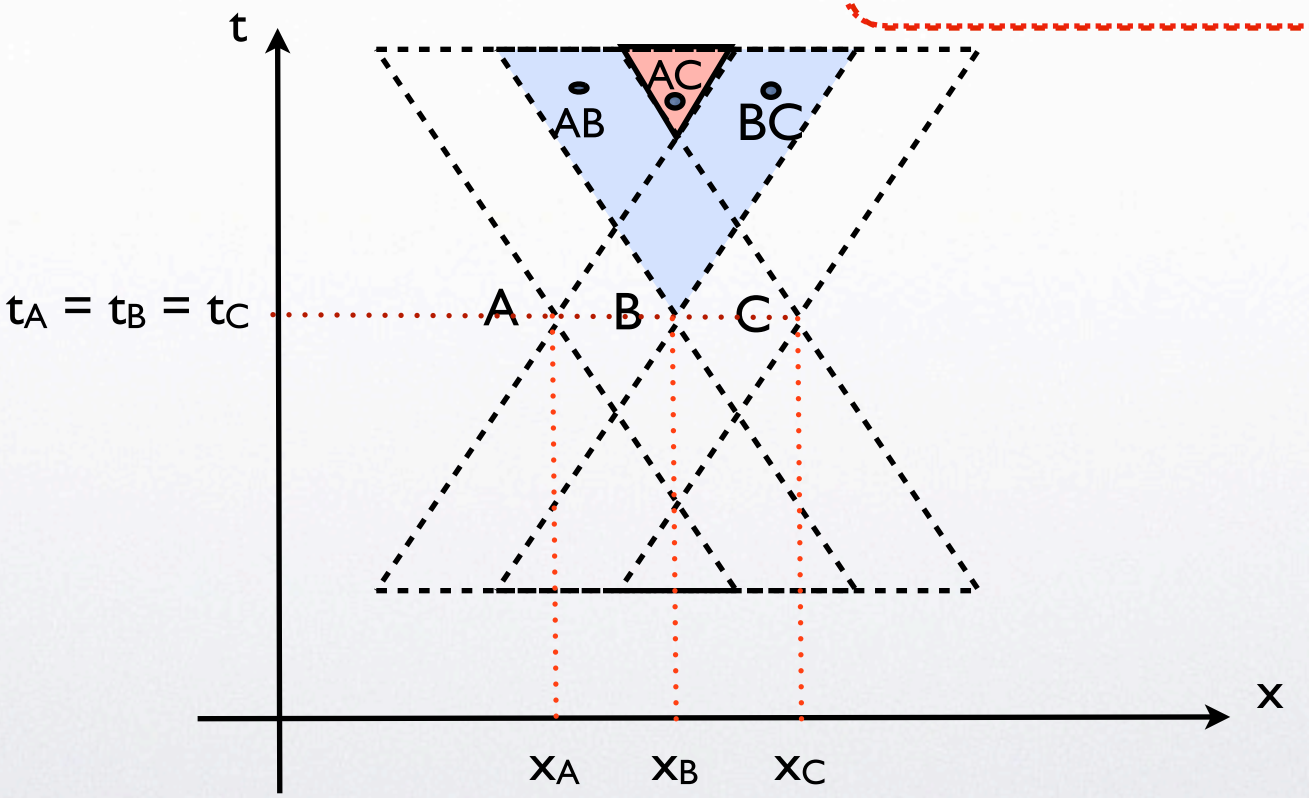
P. Horodecki and R. R., *in preparation.* P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

Compatibility with Free Will

- Free-Will conditions are intimately connected with No-Signaling constraints:

$$\begin{aligned} P(a,c|x,y,z) &= \frac{P(a,c|x,z)P(y|a,c,x,z)}{P(y|x,z)} \\ &= P(a,c|x,z) \end{aligned}$$

Free-Will: $\boxed{\boxed{P(y|a,c,x,z) \overset{?}{=} P(y|x,z)} = P(y)}$

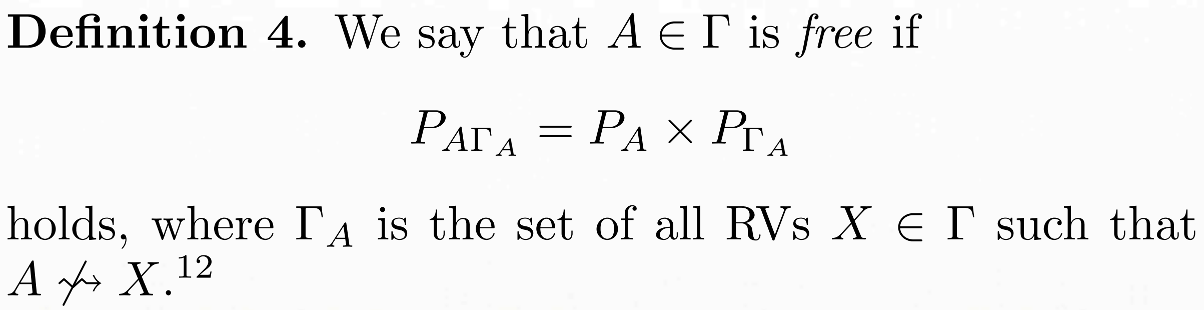


R. Colbeck and R. Renner, Free randomness can be amplified, Nature Physics 8, 450-454 (2012).

R. Colbeck and R. Renner, A short note on the concept of free choice, arXiv: 1302.4446 (2013).

Compatibility with Free Will

- Colbeck-Renner (formalising Bell): *A spacetime random variable is free if the only variables it is correlated with are those it could have caused, i.e., those in its future light cone.*



Definition 4. We say that $A \in \Gamma$ is *free* if

$$P_{A\Gamma_A} = P_A \times P_{\Gamma_A}$$

holds, where Γ_A is the set of all RVs $X \in \Gamma$ such that $A \not\rightsquigarrow X$.[12]

- If we modify NS constraints, should also modify free-will constraints.

Compatibility with Free-Will

- Argument: Correlations AC properly seen as spacetime r.v. generated in the future light cone of B.

Definition 4. *Let $A_{X_i \nrightarrow} = \{A_j\}$ denote a set of outputs A_j such that the correlation SRV $C_{\{A_j\}}$ between all the A_j is generated outside the future light cone of X_i. Then X_i is said to be free if the following condition is satisfied:*

$$P(X_i|\boldsymbol{X} \setminus X_i, A_{X_i \nrightarrow}, S_{P_1 \dots P_n}) = P(X_i). \tag{25}$$

- CR: No extension of quantum theory compatible with usual notion of free-will can have better predictive power (for instance, Bohmian theories).

P. Horodecki and R.R, *in preparation.* P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)
R. Colbeck and R. Renner, No extension of quantum theory can have improved predictive power, Nature Communications 2, 411 (2011).

Finite superluminal causal influences as explanations of quantum nonlocality

- Breakthrough result of Bancal et al. : A multi-party Bell experiment that shows any finite-speed v-causal model leads to signaling.

- *Under the restricted free-will/ relativistic causality constraints, in the measurement configurations considered so far, one can explain the quantum correlations by means of a v-causal model.*

- Work in progress: Can further modified BI's rule out v-causal explanations?

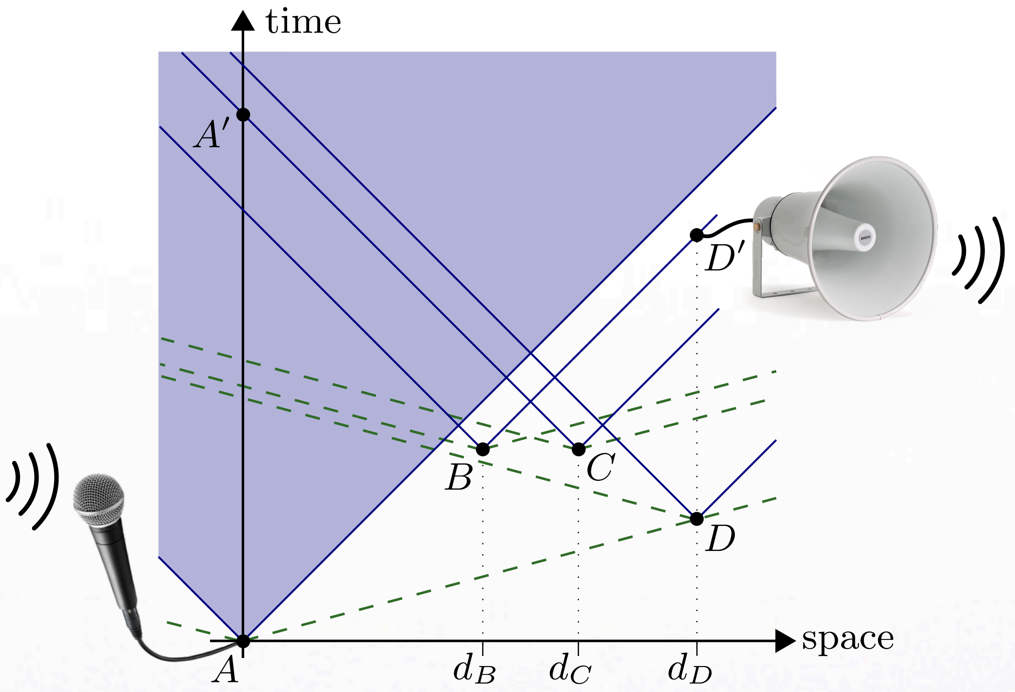
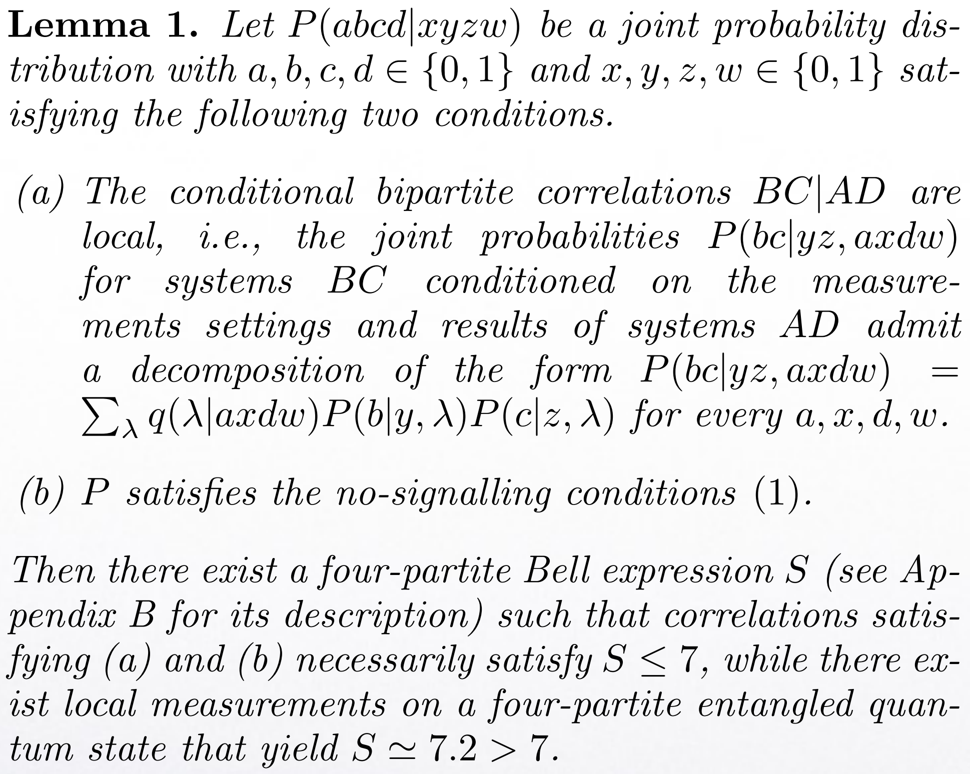


FIG. 3. Four-partite Bell-type experiment characterized by the spacetime ordering $R = (A < D < (B \sim C))$. Since B and C are both measured after A and D and satisfy $B \sim C$, the $BC|AD$ correlations produced by a v-causal model are local (see Appendix C). A violation of the inequality of Lemma 1 by the model therefore implies that the corresponding correlations must violate the no-signalling conditions (1). At least one of the tripartite correlations ABC, ABD, ACD, or BCD must then depend on the measurement setting of the remaining party. The marginal ABD (ACD) cannot depend on z (y), since this measurement setting is freely chosen at C (B), which is outside the past v-cone of A, B (C) and D (see also Appendix D). It thus follows that either the marginal ABC must depend on the measurement setting w of system D or that the marginal BCD must depend on the measurement setting x of system A (or both). Let the four systems

J.-D. Bancal, S. Pironio, A. Acin, Y.-C. Liang, V. Scarani and N. Gisin, Nature Physics 8, 867 (2012).

P. Horodecki and R.R, *in preparation*. P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

Quantum non-locality based on finite-superluminal influences leads to signaling

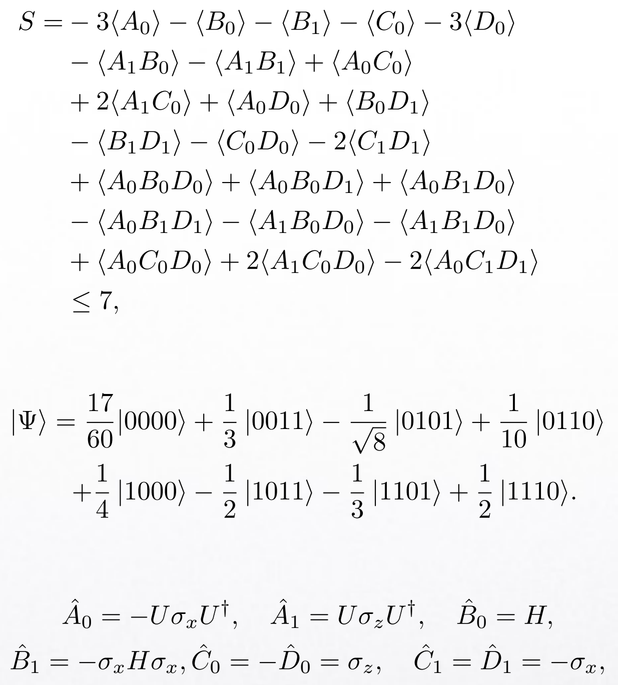


Lemma 1. *Let $P(abcd|xyzw)$ be a joint probability distribution with $a,b,c,d \in \{0,1\}$ and $x,y,z,w \in \{0,1\}$ satisfying the following two conditions.*

(a) The conditional bipartite correlations $BC|AD$ are local, i.e., the joint probabilities $P(bc|yz,axdw)$ for systems BC conditioned on the measurements settings and results of systems AD admit a decomposition of the form $P(bc|yz,axdw) = \sum_\lambda q(\lambda|axdw)P(b|y,\lambda)P(c|z,\lambda)$ for every a,x,d,w.

(b) P satisfies the no-signalling conditions (1).

Then there exist a four-partite Bell expression S (see Appendix B for its description) such that correlations satisfying (a) and (b) necessarily satisfy $S \leq 7$, while there exist local measurements on a four-partite entangled quantum state that yield $S \simeq 7.2 > 7$.



$$\begin{aligned}
S =& -3\langle A_0\rangle - \langle B_0\rangle - \langle B_1\rangle - \langle C_0\rangle - 3\langle D_0\rangle\\
&- \langle A_1B_0\rangle - \langle A_1B_1\rangle + \langle A_0C_0\rangle\\
&+ 2\langle A_1C_0\rangle + \langle A_0D_0\rangle + \langle B_0D_1\rangle\\
&- \langle B_1D_1\rangle - \langle C_0D_0\rangle - 2\langle C_1D_1\rangle\\
&+ \langle A_0B_0D_0\rangle + \langle A_0B_0D_1\rangle + \langle A_0B_1D_0\rangle\\
&- \langle A_0B_1D_1\rangle - \langle A_1B_0D_0\rangle - \langle A_1B_1D_0\rangle\\
&+ \langle A_0C_0D_0\rangle + 2\langle A_1C_0D_0\rangle - 2\langle A_0C_1D_1\rangle\\
&\leq 7,
\end{aligned}$$

$$\begin{aligned}
|\Psi\rangle =& \frac{17}{60}|0000\rangle + \frac{1}{3}|0011\rangle - \frac{1}{\sqrt{8}}|0101\rangle + \frac{1}{10}|0110\rangle\\
&+\frac{1}{4}|1000\rangle - \frac{1}{2}|1011\rangle - \frac{1}{3}|1101\rangle + \frac{1}{2}|1110\rangle.
\end{aligned}$$

$$\hat{A}_0 = -U\sigma_x U^\dagger, \quad \hat{A}_1 = U\sigma_z U^\dagger, \quad \hat{B}_0 = H,$$
$$\hat{B}_1 = -\sigma_x H\sigma_x, \hat{C}_0 = -\hat{D}_0 = \sigma_z, \quad \hat{C}_1 = \hat{D}_1 = -\sigma_x,$$

J.-D. Bancal et al. Nature Physics 8, 867 (2012).
P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019). *In prep.*

Device-Independent crypto against Relativistic Eavesdroppers

- Boxes $P(\mathbf{a}|\mathbf{x}) = P(a_1,\ldots,a_n|x_1,\ldots,x_n)$ must carry a label of space-time locations of measurement events $P^{((t1,r1),\ldots,(tn,rn))}(a_1,\ldots,a_n|x_1,\ldots,x_n)$.

- The set of boxes $P(\mathbf{a}|\mathbf{x})$ respecting relativistic causality forms a larger dimensional polytope containing the usual NS polytope.

- LHV polytope $\subset$ Quantum Correlations $\subset$ No-Signaling Polytope $\subset$ Causality Polytope.

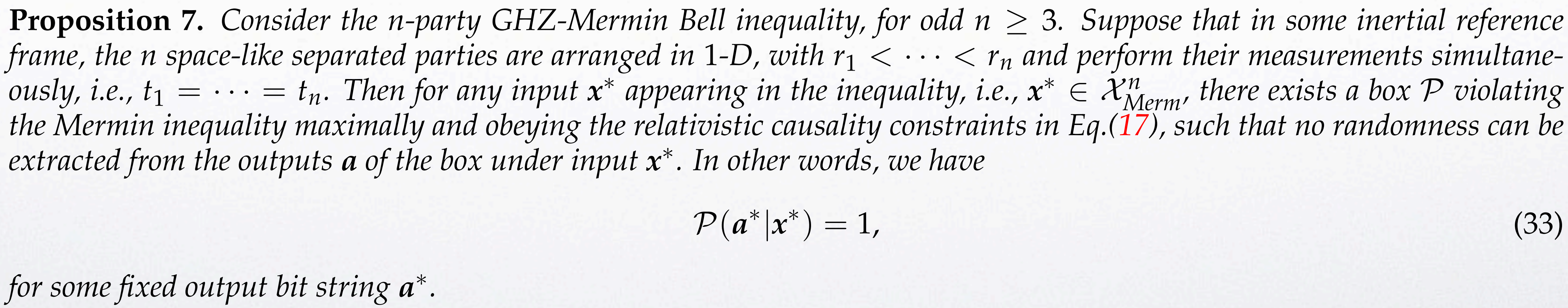
- In DIQKD against relativistic eavesdroppers, this gives a larger set of attack strategies for Eve.

R. Colbeck and R. Renner, Free randomness can be amplified, Nature Physics 8, 450-454 (2012).
R. Gallego et al., Full randomness from arbitrarily deterministic events, Nat. Comm. 4, 2654 (2013).
F. G. S. L. Brandao, R. R, A. Grudka, Horodecki^3, T. Szarek, H. Wojewodka, Nat Comm. 7, 11345 (2016).

Device-Independent Randomness Amplification against Relativistic Eve

- Randomness amplification of Santha-Vazirani sources: need BI with algebraic violation. Paradigmatic example: GHZ-Mermin inequality.

- We show that no randomness can be extracted from the settings that appear in the Mermin inequality under the new constraints, even with maximal violation.



Proposition 7. *Consider the n-party GHZ-Mermin Bell inequality, for odd $n \geq 3$. Suppose that in some inertial reference frame, the n space-like separated parties are arranged in 1-D, with $r_1 < \cdots < r_n$ and perform their measurements simultaneously, i.e., $t_1 = \cdots = t_n$. Then for any input $\boldsymbol{x}^*$ appearing in the inequality, i.e., $\boldsymbol{x}^* \in \mathcal{X}^n_{Merm}$, there exists a box $\mathcal{P}$ violating the Mermin inequality maximally and obeying the relativistic causality constraints in Eq.(17), such that no randomness can be extracted from the outputs $\boldsymbol{a}$ of the box under input $\boldsymbol{x}^*$. In other words, we have*

$$\mathcal{P}(\boldsymbol{a}^*|\boldsymbol{x}^*) = 1, \tag{33}$$

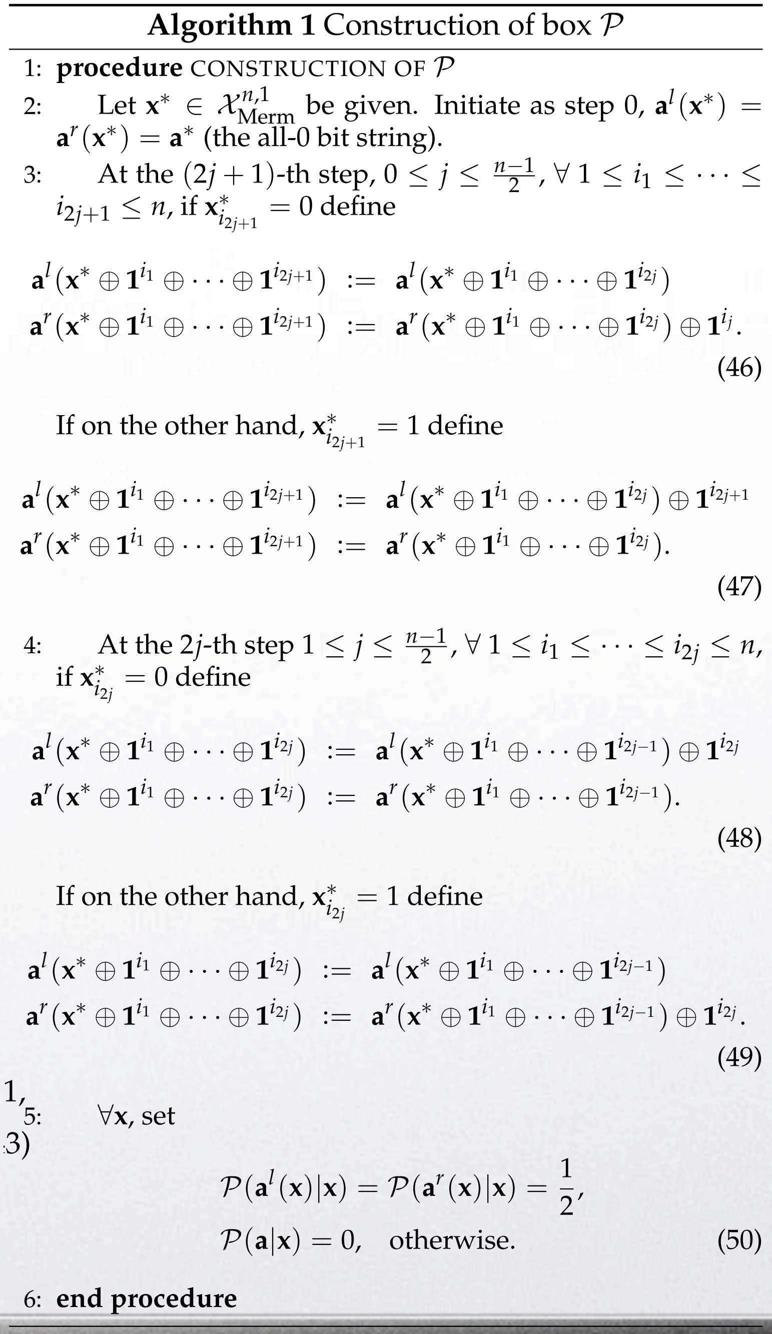
for some fixed output bit string $\boldsymbol{a}^*$.

C. Dhara, G. de la Torre, A. Acin, Phys. Rev. Lett. 112, 100402 (2014).
R. Gallego et al., Full randomness from arbitrarily deterministic events, Nat. Comm. 4, 2654 (2013).
F. G. S. L. Brandao, R. R, A. Grudka, Horodecki^3, T. Szarek, H. Wojewodka, Nat Comm. 7, 11345 (2016).

P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

DI Randomness Amplification against relativistic Eve

- Proof is by construction of box P(a|x) that satisfies:
    - GHZ-Mermin constraints
    - Causality constraints
    - returns deterministic output for settings appearing in the inequality.



Algorithm 1 Construction of box $\mathcal{P}$

```
procedure CONSTRUCTION OF $\mathcal{P}$
    Let $\mathbf{x}^* \in \mathcal{X}^{n,1}_{\mathrm{Merm}}$ be given. Initiate as step 0, $\mathbf{a}^l(\mathbf{x}^*) = \mathbf{a}^r(\mathbf{x}^*) = \mathbf{a}^*$ (the all-0 bit string).
    At the $(2j+1)$-th step, $0 \le j \le \frac{n-1}{2}$, $\forall\, 1 \le i_1 \le \cdots \le i_{2j+1} \le n$, if $\mathbf{x}^*_{i_{2j+1}} = 0$ define
        $\mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j+1}}) := \mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j}})$
        $\mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j+1}}) := \mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j}}) \oplus \mathbf{1}^{i_j}$.   (46)
    If on the other hand, $\mathbf{x}^*_{i_{2j+1}} = 1$ define
        $\mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j+1}}) := \mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j}}) \oplus \mathbf{1}^{i_{2j+1}}$
        $\mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j+1}}) := \mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j}})$.   (47)
    At the $2j$-th step $1 \le j \le \frac{n-1}{2}$, $\forall\, 1 \le i_1 \le \cdots \le i_{2j} \le n$, if $\mathbf{x}^*_{i_{2j}} = 0$ define
        $\mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j}}) := \mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j-1}}) \oplus \mathbf{1}^{i_{2j}}$
        $\mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j}}) := \mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j-1}})$.   (48)
    If on the other hand, $\mathbf{x}^*_{i_{2j}} = 1$ define
        $\mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j}}) := \mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j-1}})$
        $\mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j}}) := \mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \cdots \oplus \mathbf{1}^{i_{2j-1}}) \oplus \mathbf{1}^{i_{2j}}$.   (49)
    $\forall \mathbf{x}$, set
        $\mathcal{P}(\mathbf{a}^l(\mathbf{x})|\mathbf{x}) = \mathcal{P}(\mathbf{a}^r(\mathbf{x})|\mathbf{x}) = \frac{1}{2}$,
        $\mathcal{P}(\mathbf{a}|\mathbf{x}) = 0$,   otherwise.   (50)
end procedure
```

P. Horodecki and R. R., *in preparation.*

P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

Device-Independent QKD against relativistic Eve

- The chained Bell inequalities $I^{m,ch}_{AB}$ are a family of two-party correlation Bell inequalities (XOR games) with m inputs and 2 outputs per party.

$$\mathcal{I}^{m,\mathrm{ch}}_{AB} := \sum_{i=1}^{m} \left[\langle A_i B_i \rangle + \langle A_i B_{i+1} \rangle\right] \leq 2m - 2,$$

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

$$A_i := \sin(\alpha_i)\sigma_x + \cos(\alpha_i)\sigma_z,$$
$$B_j := \sin(\beta_j)\sigma_x + \cos(\beta_j)\sigma_z.$$

with $\alpha_i := \frac{\pi(2i-1)}{m}$ and $\beta_j := \frac{\pi(j-1)}{m}$ for $i, j = 1, \ldots, m$.

- QM: $I^{m,ch}_{AB}$ = 2m Cos(π/2m). NS: $I^{m,ch}_{AB}$ = 2m.

- In the limit m→∞, a perfect key bit between Alice and Bob is obtained (BHK, BCK, BKS) against the usual No-Signaling adversary. Underlying property: Monogamy of non-local correlations.

Proposition 4 ([39]). *Any no-signaling distribution for which $\mathcal{I}^{m,ch}_{AB} < \mathcal{I}^*$ satisfies*

$$P(A_k = a) \leq \frac{1}{2}(1 + \mathcal{I}^*),$$
$$P(B_l = b) \leq \frac{1}{2}(1 + \mathcal{I}^*),$$

for all $a, b \in \{0, 1\}$ and $k, l \in [m]$.

$$\mathcal{I}^{m,\mathrm{ch}}_{AB} + \langle KE_1 \rangle \leq 2m.$$

$$I(B:E) \leq \mathcal{I}^{m,\mathrm{ch}}_{AB}.$$

J. Barrett, A. Kent and S. Pironio, Phys. Rev. Lett. 97, 170409 (2006).

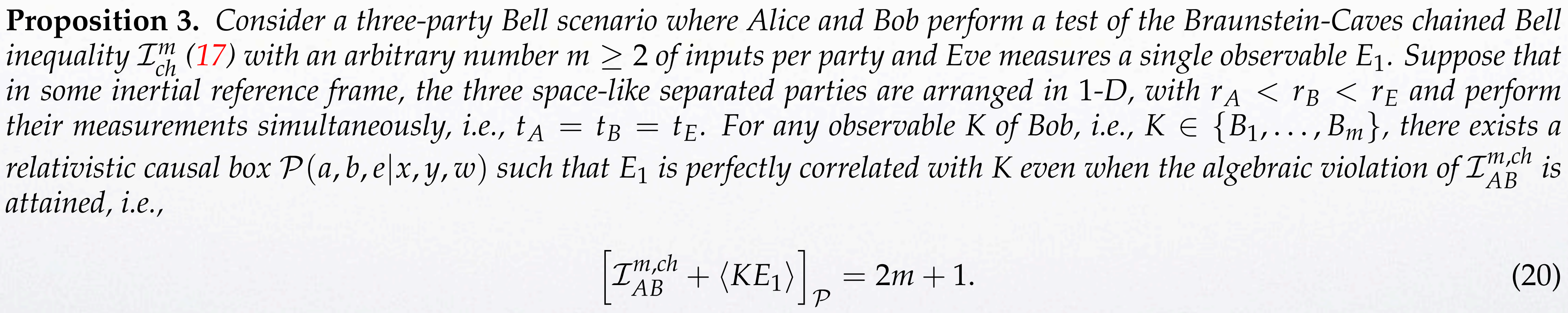
J. Barrett, L. Hardy and A. Kent, Phys. Rev. Lett. 95, 010503 (2005).

J. Barrett, R. Colbeck and A. Kent, Phys. Rev. A 86, 062326 (2012).

Device-Independent QKD against relativistic Eve

- In a Device-Independent framework, the relativistic causality conditions allow Eve to gain maximal information about the output key bit of such a protocol.

- Eve's observable is maximally correlated with the chosen observable of the honest parties even when algebraic violation is observed.



Proposition 3. *Consider a three-party Bell scenario where Alice and Bob perform a test of the Braunstein-Caves chained Bell inequality $\mathcal{I}^{m}_{ch}$ (17) with an arbitrary number $m \geq 2$ of inputs per party and Eve measures a single observable E_1. Suppose that in some inertial reference frame, the three space-like separated parties are arranged in 1-D, with $r_A < r_B < r_E$ and perform their measurements simultaneously, i.e., $t_A = t_B = t_E$. For any observable K of Bob, i.e., $K \in \{B_1, \dots, B_m\}$, there exists a relativistic causal box $\mathcal{P}(a, b, e|x, y, w)$ such that E_1 is perfectly correlated with K even when the algebraic violation of $\mathcal{I}^{m,ch}_{AB}$ is attained, i.e.,*

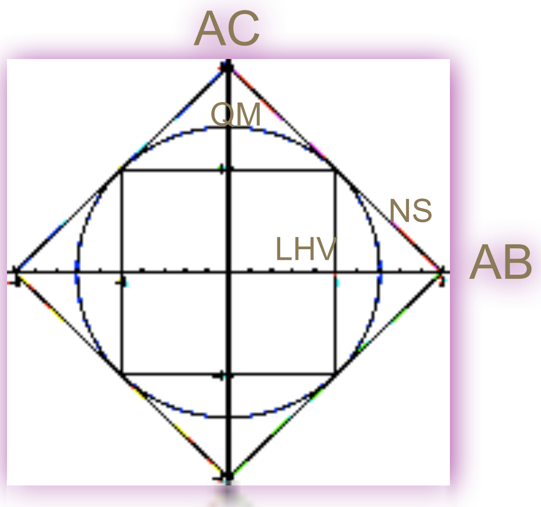
$$\left[\mathcal{I}^{m,ch}_{AB} + \langle K E_1 \rangle\right]_{\mathcal{P}} = 2m + 1. \tag{20}$$

P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

P. Horodecki and R.R, *in preparation.*

General properties of no-signaling theories

- Monogamy:Violation of CHSH Bell inequality by Alice-Bob precludes violation by Alice-Charlie.



$$B_{CHSH} = \left| E(A_1, B_1)_{LR} + E(A_1, B_2)_{LR} + E(A_2, B_1)_{LR} - E(A_2, B_2)_{LR} \right| \leq 2$$

Proposition 3. *Consider a three-party Bell scenario, with Alice, Bob and Charlie each performing two measurements $x, y, z \in \{0, 1\}$ of two outcomes $a, b, c \in \{0, 1\}$ respectively. Suppose that in some inertial reference frame, the three space-like separated parties are arranged in 1-D, with $r_A < r_B < r_C$ and perform their measurements simultaneously, i.e., $t_A = t_B = t_C$. Then, there exists a three-party relativistically causal box $\mathcal{P}(a, b, c|x, y, z)$ such that*

$$\langle CHSH \rangle_{AB} + \langle CHSH \rangle_{BC} = 8. \tag{19}$$

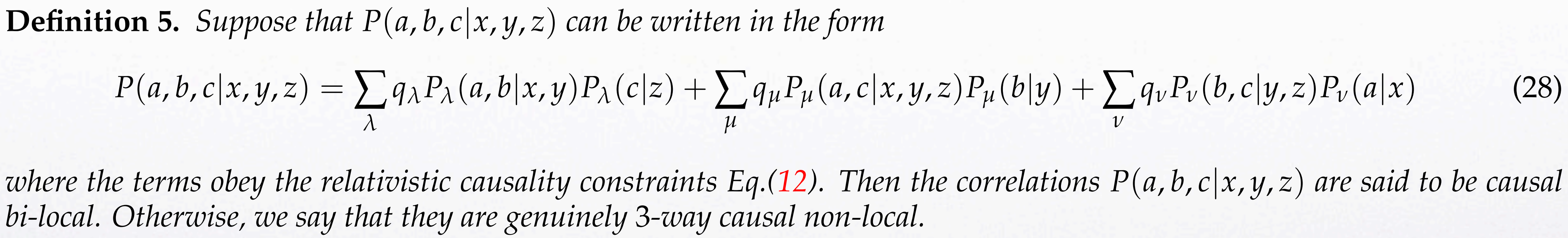
L. Masanes, A. Acin and N. Gisin, Phys. Rev. A 73, 012112 (2006).

P. Horodecki and R. R., *in preparation.* P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

Genuine multipartite nonlocality

- Multiparty non-locality: Several classes of non-local correlations including Svetlichy S_2-local, NS_2-local, T_2-local with $NS_2 \subset T_2 \subset S_2$.

- We introduce a new class of models C_2:



Definition 5. *Suppose that $P(a,b,c|x,y,z)$ can be written in the form*

$$P(a,b,c|x,y,z) = \sum_{\lambda} q_\lambda P_\lambda(a,b|x,y) P_\lambda(c|z) + \sum_{\mu} q_\mu P_\mu(a,c|x,y,z) P_\mu(b|y) + \sum_{\nu} q_\nu P_\nu(b,c|y,z) P_\nu(a|x) \tag{28}$$

where the terms obey the relativistic causality constraints Eq.(12). Then the correlations $P(a,b,c|x,y,z)$ are said to be causal bi-local. Otherwise, we say that they are genuinely 3-way causal non-local.

J.-D. Bancal, J. Barrett, N. Gisin, S. Pironio, Phys. Rev. A. 88, 014102 (2013).

G. Svetlichny, Phys. Rev. D 35, 3066 (1987). P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

P. Horodecki and R.R, *in preparation.* P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

Genuine Multiparty Nonlocality

- In the Bell scenario B(2,2,2) we give an inequality and quantum correlations obtained by suitable measurements on W-states that lead to its violation demonstrating genuine multiparty nonlocality.

$$
\begin{aligned}
0 \leq 6 &- 2\langle A_1B_1\rangle - 2\langle A_2B_1\rangle - (1/2)\langle A_1C_1\rangle_{y=1} - (1/2)\langle A_1C_1\rangle_{y=2} + (1/2)\langle A_2C_1\rangle_{y=1} + (1/2)\langle A_2C_1\rangle_{y=2} - \langle A_1B_2C_1\rangle \\
&+\langle A_2B_2C_1\rangle - (1/2)\langle A_1C_2\rangle_{y=1} - (1/2)\langle A_1C_2\rangle_{y=2} + (1/2)\langle A_2C_2\rangle_{y=1} + (1/2)\langle A_2C_2\rangle_{y=2} + \langle A_1B_2C_2\rangle - \langle A_2B_2C_2\rangle
\end{aligned}
$$

$$
|W\rangle = \frac{1}{\sqrt{3}}\left(|001\rangle + |010\rangle + |100\rangle\right).
$$

$$
\begin{aligned}
A_i &= \sin(\alpha_i)\sigma_x + \cos(\alpha_i)\sigma_z, \\
B_j &= \sin(\beta_j)\sigma_x + \cos(\beta_j)\sigma_z, \\
C_k &= \sin(\gamma_k)\sigma_x + \cos(\gamma_k)\sigma_z.
\end{aligned}
$$

$$
\mathcal{I}^{\mathrm{qm}} \leq -0.67.
$$

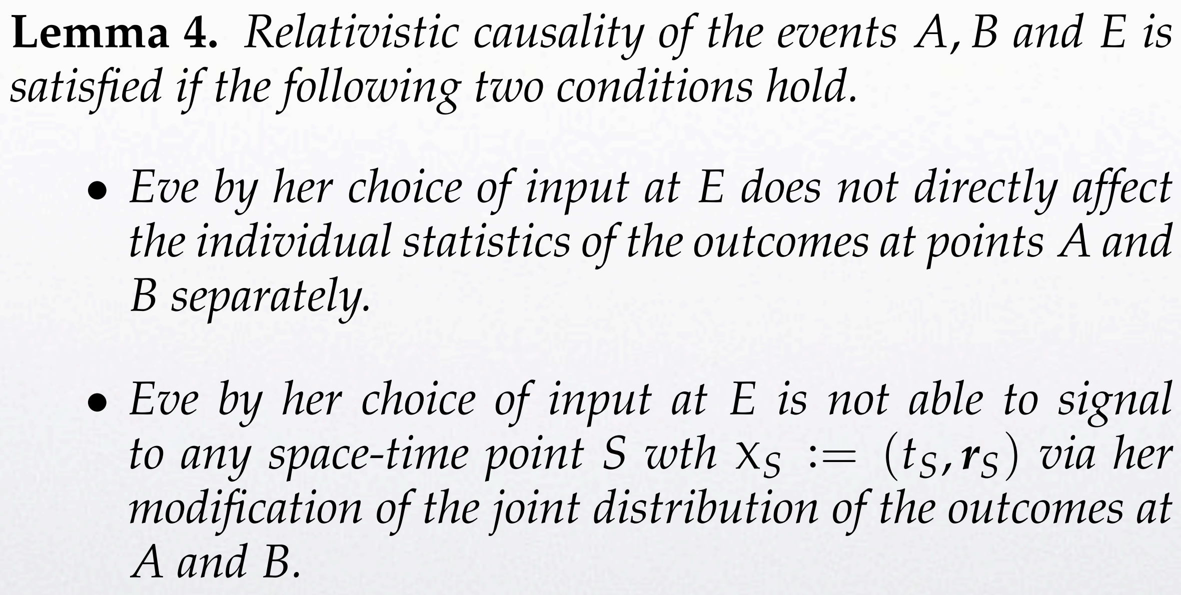
$$
\alpha_1 = 4.51, \alpha_2 = -1.76, \beta_1 = 4.81, \beta_2 = 6.13, \gamma_1 = -1.13, \gamma_2 = 4.98.
$$

P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

P. Horodecki and R.R, *in preparation.*

Preferred Frame of Reference

- Consider superluminal influences in a preferred frame *I* at speed u > c.
- Fix (t_A, r_A) and (t_B, r_B).
- Which (t_E, r_E) are allowed space-time region from which an Eve is able to influence correlations without violating causality?

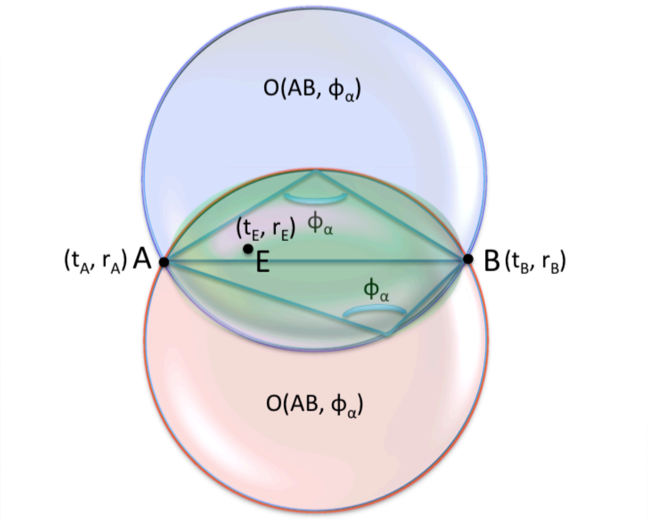


Lemma 4. *Relativistic causality of the events A, B and E is satisfied if the following two conditions hold.*

- *Eve by her choice of input at E does not directly affect the individual statistics of the outcomes at points A and B separately.*
- *Eve by her choice of input at E is not able to signal to any space-time point S wth $\mathrm{x}_S := (t_S, \boldsymbol{r}_S)$ via her modification of the joint distribution of the outcomes at A and B.*

P. Horodecki and R. R., *in preparation*.

Preferred frame of reference



Theorem 7. *Consider measurement events A, B with corresponding space coordinates $\boldsymbol{r}_A, \boldsymbol{r}_B$ in a chosen inertial reference frame I. Then a measurement event E can superluminally influence the correlations between A and B at speed $u > c$ without violating causality in I if and only if its space coordinate $\boldsymbol{r}_E$ satisfies*

$$\boldsymbol{r}_E \in Seg(\bigcirc(AB;\varphi_\alpha)) \qquad (39)$$

for any circle $\bigcirc$ with AB as a chord and having angle φ_α as the angle in the corresponding minor segment, where $\varphi_\alpha = \pi - 2\arcsin(\alpha)$ and $\alpha = c/u$.

$$t'_A \geq t_A = t_E + \frac{|\mathbf{r}_A - \mathbf{r}_E|}{u}$$
$$t'_B \geq t_B = t_E + \frac{|\mathbf{r}_B - \mathbf{r}_E|}{u}$$

If we abandon the notion of a preferred frame, the regions transform. Consequences are still Lorentz covariant.

P. Horodecki and R. R., *in preparation*.

Summary

- *Re-examined the derivation of the no-signaling constraints from causality.*
- Implications in many directions, including quantum cryptographic and finite-superluminal explanations of quantum non-local correlations.

- This work is supported by the John Templeton Foundation and ERC AdG grant QOLAPS.

erc European Research Council

Thank you!

JOHN TEMPLETON FOUNDATION

http://en.wikipedia.org/wiki/600-cell

Summary and Open Questions

- Re-examine the ubiquitous no-signaling constraints from strict relativistic causality.
- Superluminal travel is logically perfectly possible as long as it leads to a consistent story that unfolds in time.
- “Non-local yet causal” theory that is different from Bohmian: allows for a notion of free-will.
- Open: “Extended quantum correlations” that obey the new constraints. Principles to rule out such correlations and dynamics.
- This work is supported by: John Templeton Foundation and ERC AdG grant QOLAPS.

Thank you!

No-Signaling Polytope

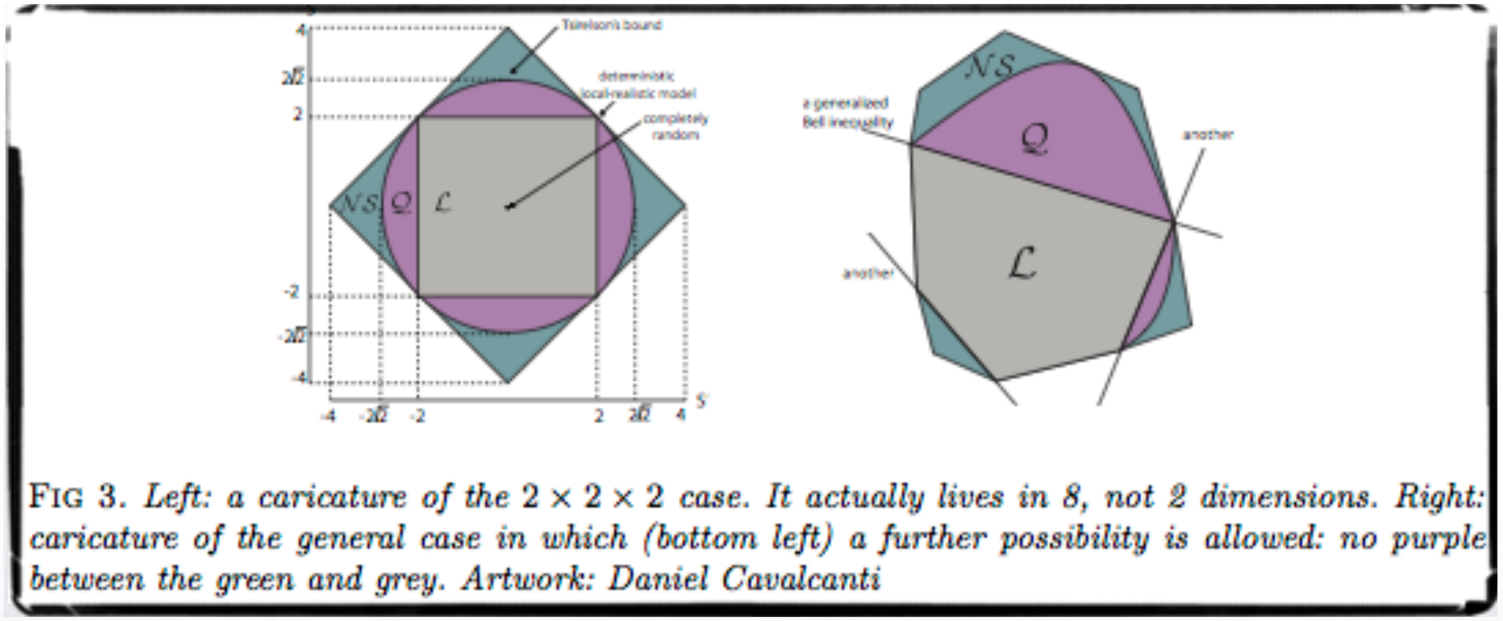
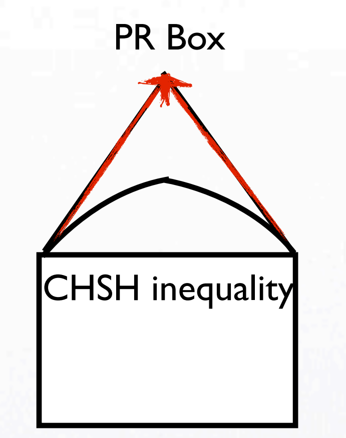


FIG 3. *Left: a caricature of the 2 × 2 × 2 case. It actually lives in 8, not 2 dimensions. Right: caricature of the general case in which (bottom left) a further possibility is allowed: no purple between the green and grey. Artwork: Daniel Cavalcanti*



- LHV ⊂ Q ⊂ NS.
- In the B(2,2,2) scenario, non-local extreme box of NS is the PR box.

		x2 = 0		x2 = 1	
		a2 = 0	a2 = 1	a2 = 0	a2 = 1
x1 = 0	a1 = 0	1/2	0	1/2	0
	a1 = 1	0	1/2	0	1/2
x1 = 1	a1 = 0	1/2	0	0	1/2
	a1 = 1	0	1/2	1/2	0

$a1 \oplus a2 = x1 . x2$

- No signal carrying information can propagate faster than light - No-Signaling Principle.
  - Captured in the Bell scenario (n,m,k) by a set of constraints on the $P(a_1,\ldots,a_n|x_1,\ldots,x_n)$.
  - E.g. In the three party Bell scenario

$$\sum_{a_3} P(a_1, a_2, a_3 \,|\, x_1, x_2, x_3) = \sum_{a_3} P(a_1, a_2, a_3 \,|\, x_1, x_2, x_3') \qquad \forall a_1, a_2, x_1, x_2, x_3, x_3'$$