

IQOQI - INSTITUTE FOR QUANTUM OPTICS AND QUANTUM INFORMATION VIENNA



INSTITUTE

# It From Qubit underground:

# how quantum theory and spacetime constrain each other

# Markus P. Müller

IQOQI Vienna & Perimeter Institute



Der Wissenschaftsfonds.

FШF









- 1. Because we will try to be as theory-agnostic/independent as possible, sometimes not even assuming the validity of QT.
- 2. Because some of it is somewhat beyond the mainstream (partially for historical reasons, as we will see).



- 1. Because we will try to be as theory-agnostic/independent as possible, sometimes not even assuming the validity of QT.
- 2. Because some of it is somewhat beyond the mainstream (partially for historical reasons, as we will see).

Most of this research:









$$\begin{split} \rho &= \frac{1}{2} \mathbf{1} + \vec{r} \cdot \vec{\sigma} = \frac{1}{2} \begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} \\ \mathrm{tr}(\rho) &= 1, \quad \rho \geq 0 \Leftrightarrow |\vec{r}| \leq 1. \end{split}$$



$$\begin{split} \rho &= \frac{1}{2} \mathbf{1} + \vec{r} \cdot \vec{\sigma} = \frac{1}{2} \begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} \\ \mathrm{tr}(\rho) &= 1, \quad \rho \geq 0 \Leftrightarrow |\vec{r}| \leq 1. \end{split}$$

$$\rho \mapsto U \rho U^{\dagger} \qquad \longleftrightarrow \qquad \vec{r} \mapsto R_U \vec{r}$$
$$\mathrm{PSU}(2) \qquad \mathrm{SO}(3)$$



$$\begin{split} \rho &= \frac{1}{2} \mathbf{1} + \vec{r} \cdot \vec{\sigma} = \frac{1}{2} \begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} \\ \mathrm{tr}(\rho) &= 1, \quad \rho \geq 0 \Leftrightarrow |\vec{r}| \leq 1. \end{split}$$





1. Motivation

2. Some history: von Weizsäcker & Wootters

3. Relativity of simultaneity and the qubit

# Today

1. Motivation

# 2. Some history: von Weizsäcker & Wootters

3. Relativity of simultaneity and the qubit

#### Motivation

• New ("semi-device-independent") quantum information protocols: inputs / outputs now spatiotemporal DOFs.

# Motivation

• New ("semi-device-independent") quantum information protocols: inputs / outputs now spatiotemporal DOFs.





 New ("semi-device-independent") quantum information protocols: inputs / outputs now spatiotemporal DOFs.



 Rigorous insights into the structural architecture of physics (geometry vs. probability)

very modest steps towards QG?

Wanted: a complete theory of **evolution**.

Wanted: a complete theory of **evolution**.

Wanted: a complete theory of **evolution**.



confined to desert, no fossils: sparse empirical evidence.

Wanted: a complete theory of **evolution**.



confined to desert, no fossils: sparse empirical evidence.

- **Option 1:** try to develop a full-blown theory directly.
- **Option 2:** first, study how the environment constrains biological traits.

Wanted: a complete theory of **evolution**.



confined to desert, no fossils: sparse empirical evidence.

- **Option 1:** try to develop a full-blown theory directly.
- Option 2: first, study how the environment constrains biological traits.
   Needs imagination of how biology could be different.



Wanted: a complete theory of **quantum gravity**.

Wanted: a complete theory of **quantum gravity**.

sparse empirical evidence.

Wanted: a complete theory of **quantum gravity**. sparse empirical evidence.



- **Option 1:** try to develop a full-blown theory directly.
- **Option 2:** first, study how spacetime constrains quantum theory.

Wanted: a complete theory of **quantum gravity**. sparse empirical evidence.



- **Option 1:** try to develop a full-blown theory directly.
- Option 2: first, study how spacetime constrains quantum theory. Needs (mathematical) imagination of how the universe's probabilistic theory could be different.

Wanted: a complete theory of **quantum gravity**. sparse empirical evidence.



- **Option 1:** try to develop a full-blown theory directly.
- Option 2: first, study how spacetime constrains quantum theory. Needs (mathematical) imagination of how the universe's probabilistic theory could be different.



superstrong nonlocality?



higher-order interference?

# Today

1. Motivation

# 2. Some history: von Weizsäcker & Wootters

3. Relativity of simultaneity and the qubit

# Today

1. Motivation

2. Some history: von Weizsäcker & Wootters

3. Relativity of simultaneity and the qubit



Carl-Friedrich von Weizsäcker (1912-2007) Carl Friedrich vonWeizsäcker Aufbau der Physik

Hanser



Holger Lyre



Carl-Friedrich von Weizsäcker (1912-2007)

Carl Friedrich vonWeizsäcker Aufbau der Physik

Hanser



Holger Lyre

Summary via lyre.de/urinfo.htm (imperfect English translation is mine):

Von Weizsäcker gives the following definition of the central notion of "ur-alternative": The binary alternative, out of which the state spaces of quantum theory can be built, is called ur-alternative. The subobject associated with an ur-alternative is called "ur".



Carl-Friedrich von Weizsäcker (1912-2007)



Holger Lyre

Summary via lyre.de/urinfo.htm (imperfect English translation is mine):

Von Weizsäcker gives the following definition of the central notion of "ur-alternative": The binary alternative, out of which the state spaces of quantum theory can be built, is called ur-alternative. The subobject associated with an ur-alternative is called "ur".

1955 and 1958: Out of the three works by von Weizsäcker under the title *Complementarity and Logic*, the third one in particular contains the basic mathematical motive for ur theory: *"The special theory of relativity, insofar as it is a theory of space and time, is already the quantum theory of a deeper simple alternative. The Lorentz group is an (unfaithful) real representation of the group of complex linear transformations of the quantum-mechanical state space of that alternative."* 

The **ur-hypothesis** consists of the assumption that the state spaces of all objects in physics are essentially built out of urs. In the sense of abstract quantum theory, this is a logical, not a spatial atomism. [...]

The **ur-hypothesis** consists of the assumption that the state spaces of all objects in physics are essentially built out of urs. In the sense of abstract quantum theory, this is a logical, not a spatial atomism. [...]

An ur's essential symmetry group is SU(2). A world built of urs should be essentially invariant under this group. The central **fundamental assumption of ur theory** is, that space itself it a consequence of the ur-hypothesis and the symmetry group of the ur.

The **ur-hypothesis** consists of the assumption that the state spaces of all objects in physics are essentially built out of urs. In the sense of abstract quantum theory, this is a logical, not a spatial atomism. [...]

An ur's essential symmetry group is SU(2). A world built of urs should be essentially invariant under this group. The central **fundamental assumption of ur theory** is, that space itself it a consequence of the ur-hypothesis and the symmetry group of the ur.

This assumption can be motivated as follows: one can regard space as the parameter space of interaction strength. A suitable model for space would hence be the parameter space of SU(2) itself, i.e. SU(2) as a homogeneous space. This is topologically an S^3, i.e. the unit sphere of R^4, i.e. isomorphic to the spatial part of an Einstein cosmos. Thus, in ur theory, SU(2) is itself seen as an obvious, approximate model of the cosmos.

The **ur-hypothesis** consists of the assumption that the state spaces of all objects in physics are essentially built out of urs. In the sense of abstract quantum theory, this is a logical, not a spatial atomism. [...]

An ur's essential symmetry group is SU(2). A world built of urs should be essentially invariant under this group. The central **fundamental assumption of ur theory** is, that space itself it a consequence of the ur-hypothesis and the symmetry group of the ur.

This assumption can be motivated as follows: one can regard space as the parameter space of interaction strength. A suitable model for space would hence be the parameter space of SU(2) itself, i.e. SU(2) as a homogeneous space. This is topologically an S^3, i.e. the unit sphere of R^4, i.e. isomorphic to the spatial part of an Einstein cosmos. Thus, in ur theory, SU(2) is itself seen as an obvious, approximate model of the cosmos.

The **ur-hypothesis** consists of the assumption that the state spaces of all objects in physics are essentially built out of urs. In the sense of abstract quantum theory, this is a logical, not a spatial atomism. [...]

An ur's essential symmetry group is SU(2). A world built of urs should be essentially invariant under this group. The central **fundamental assumption of ur theory** is, that space itself it a consequence of the ur-hypothesis and the symmetry group of the ur.

This assumption can be motivated as follows: one can regard space as the parameter space of interaction strength. A suitable model for space would hence be the parameter space of SU(2) itself, i.e. SU(2) as a homogeneous space. This is topologically an S^3, i.e. the unit sphere of R^4, i.e. isomorphic to the spatial part of an Einstein cosmos. Thus, in ur theory, SU(2) is itself seen as an obvious, approximate model of the cosmos.

#### 2.3 The Quantized Ur-Tetrad

Up to this point we have used urs as spinorial wavefunctions, i.e., we considered an ur as the first step of quantization of a simple alternative. The second quantization is done by the replacement  $u_r \rightarrow \hat{a}_r$  and  $u_r^* \rightarrow \hat{a}_r^+$  and the BOSE commutation relations

$$[\hat{a}_r, \hat{a}_s^+] = \delta_{rs}, \qquad [\hat{a}_r, \hat{a}_s] = [\hat{a}_r^+, \hat{a}_s^+] = 0.$$
(26)

Thus, we get a quantum field theory of urs, i.e., a many-ur - theory with a variable number of urs. Consequently from (26) the quantization of the ur-tetrad (22) - (25) follows. We use a special choise of the components of the bispinorial ur  $\binom{u}{u^*}$ , i.e.,  $u_r$  with r=1...4 ( $u^*$  denotes an H. Lyre, *Quantum Space-Time and Tetrads*, Int. J. Theor. Phys. **37**, 393—400 (1998).
## Von Weizsäcker's theory of "ur alternatives"

The **ur-hypothesis** consists of the assumption that the state spaces of all objects in physics are essentially built out of urs. In the sense of abstract quantum theory, this is a logical, not a spatial atomism. [...]

An ur's essential symmetry group is SU(2). A world built of urs should be essentially invariant under this group. The central **fundamental assumption of ur theory** is, that space itself it a consequence of the ur-hypothesis and the symmetry group of the ur.

This assumption can be motivated as follows: one can regard space as the parameter space of interaction strength. A suitable model for space would hence be the parameter space of SU(2) itself, i.e. SU(2) as a homogeneous space. This is topologically an S^3, i.e. the unit sphere of R^4, i.e. isomorphic to the spatial part of an Einstein cosmos. Thus, in ur theory, SU(2) is itself seen as an obvious, approximate model of the cosmos.

#### 2.3 The Quantized Ur-Tetrad

Up to this point we have used urs as spinorial wavefunctions, i.e., we considered an ur as the first step of quantization of a simple alternative. The second quantization is done by the replacement  $u_r \to \hat{a}_r$  and  $u_r^* \to \hat{a}_r^+$  and the BOSE commutation relations

$$[\hat{a}_r, \hat{a}_s^+] = \delta_{rs}, \qquad [\hat{a}_r, \hat{a}_s] = [\hat{a}_r^+, \hat{a}_s^+] = 0.$$
(26)

Thus, we get a quantum field theory of urs, i.e., a many-ur - theory with a variable number of urs. Consequently from (26) the quantization of the ur-tetrad (22) - (25) follows. We use a special choise of the components of the bispinorial ur  $\binom{u}{u^*}$ , i.e.,  $u_r$  with r=1...4 ( $u^*$  denotes an H. Lyre, *Quantum Space-Time and Tetrads*, Int. J. Theor. Phys. **37**, 393—400 (1998).





No-cloning theorem, Page-Wootters mechanism...



No-cloning theorem, Page-Wootters mechanism...

PhD thesis, 1980: "The Acquisition of Information from Quantum Measurements".



No-cloning theorem, Page-Wootters mechanism...

PhD thesis, 1980: "The Acquisition of Information from Quantum Measurements".





No-cloning theorem, Page-Wootters mechanism...

PhD thesis, 1980: "The Acquisition of Information from Quantum Measurements".

# Shown **without** assuming QM:

$$\underbrace{d(\psi_{\theta},\psi_{\theta'})} = c \cdot [\theta - \theta']$$

statistical distance for yes-no measurement

"actual" distance of

angles

$$\Leftrightarrow p(\theta) = \cos^2 \frac{n}{2} (\theta - \theta_0)$$

characteristic of spin-*n* particles in QM





No-cloning theorem, Page-Wootters mechanism...

PhD thesis, 1980: "The Acquisition of Information from Quantum Measurements".

# 

$$d(\theta_1, \theta_2) = \frac{1}{\sqrt{n}} \int_{\theta_1}^{\theta_2} \frac{d\theta}{2\Delta\theta} = \int_{\theta_1}^{\theta_2} d\theta \frac{|dp/d\theta|}{2[p(1-p)]^{1/2}}$$

# Shown without assuming QM:

$$\underline{d(\psi_{\theta},\psi_{\theta'})} = c \cdot \left[\theta - \theta'\right]$$

statistical distance for yes-no measurement "actual" distance of angles

 $\Leftrightarrow p(\theta) = \cos^2 \frac{n}{2} (\theta - \theta_0)$ 

characteristic of spin-n particles in QM

PHYSICAL REVIEW D

#### VOLUME 23, NUMBER 2

**15 JANUARY 1981** 

#### Statistical distance and Hilbert space\*

W. K. Wootters

Center for Theoretical Physics, University of Texas, Austin, Texas 78712 (Received 2 September 1980)

A concept of "statistical distance" is defined between different preparations of the same quantum system, or in other words, between different rays in the same Hilbert space. Statistical distance is determined entirely by the size of statistical fluctuations occurring in measurements designed to distinguish one state from another. It is not related, *a priori*, to the usual distance (or angle) between rays. One finds, however, that these two kinds of distance are in fact the same, a result which depends on certain peculiarities of quantum mechanics.

PHYSICAL REVIEW D

#### VOLUME 23, NUMBER 2

**15 JANUARY 1981** 

(3)

#### Statistical distance and Hilbert space\*

W. K. Wootters

Center for Theoretical Physics, University of Texas, Austin, Texas 78712 (Received 2 September 1980)

A concept of "statistical distance" is defined between different preparations of the same quantum system, or in other words, between different rays in the same Hilbert space. Statistical distance is determined entirely by the size of statistical fluctuations occurring in measurements designed to distinguish one state from another. It is not related, *a priori*, to the usual distance (or angle) between rays. One finds, however, that these two kinds of distance are in fact the same, a result which depends on certain peculiarities of quantum mechanics.

 $d(\theta_1, \theta_2) = \lim_{n \to \infty} \frac{1}{\sqrt{n}} \times [\text{maximum number of intermediate orientations each of which is}]$ 

distinguishable (in n trials) from its neighbors].

Let us now suppose that the experimenter, in making his determination of the value of  $\theta$ , has only a limited number of photons to work with, so that precisely *n* photons actually pass through the filter to be analyzed by the nicol prism. Then, because of the statistical fluctuations associated with a finite sample, the observed frequency of occurrence of yes is only an approximation to the actual probability of yes, the typical error being of the order of  $n^{-1/2}$ . More precisely, the experimenter's uncertainty (root-mean-square deviation) in the value of p is<sup>1,2</sup>

$$\Delta p = \left[\frac{p(1-p)}{n}\right]^{1/2}$$

$$d(\theta_1, \theta_2) = \frac{1}{\sqrt{n}} \int_{\theta_1}^{\theta_2} \frac{d\theta}{2\Delta\theta} = \int_{\theta_1}^{\theta_2} d\theta \frac{|dp/d\theta|}{2[p(1-p)]^{1/2}}$$

# Today

1. Motivation

2. Some history: von Weizsäcker & Wootters

3. Relativity of simultaneity and the qubit

# Today

1. Motivation

# 2. Some history: von Weizsäcker & Wootters

3. Relativity of simultaneity and the qubit





P. Jordan, J. von Neumann, E. Wigner, *On an algebraic generalization of the quantum mechanical formalism,* Annals of Mathematics **35**, 29-64 (1934).



n, J. von Neumann, E. Wigner, *On an algebraic generalization uantum mechanical formalism,* Annals of Mathematics **35**, 1934).







n, J. von Neumann, E. Wigner, *On an algebraic generalization uantum mechanical formalism,* Annals of Mathematics **35**, 1934).







Take care: qutrit etc. **not a ball!**  Does spacetime constrain d?

"Why" *d=3* ?

A. Garner, MM, O. C. O. Dahlsten, Proc. R. Soc. A 473, 20170596 (2017).



A. Garner, MM, O. C. O. Dahlsten, Proc. R. Soc. A 473, 20170596 (2017).



A. Garner, MM, O. C. O. Dahlsten, Proc. R. Soc. A 473, 20170596 (2017).



A. Garner, MM, O. C. O. Dahlsten, Proc. R. Soc. A 473, 20170596 (2017).



North-pole state: particle definitely in upper branch.

A. Garner, MM, O. C. O. Dahlsten, Proc. R. Soc. A 473, 20170596 (2017).



South-pole state: particle definitely in lower branch.





State on equator *z=0*: probability 1/2 for each.





State on equator *z=0*: probability 1/2 for each.  $p(up) = \frac{1}{2}(z+1)$ 



What transformations *T* can we perform locally in one arm... ... reversibly, i.e. without any information loss?



*T* must be a rotation of the Bloch ball (reversible+linear)... ... and must preserve *p*(up), i.e. preserve the *z*-axis.



*T* must be a rotation of the Bloch ball (reversible+linear)... ... and must preserve *p*(up), i.e. preserve the *z*-axis.



*T* must be a rotation of the Bloch ball (reversible+linear)... ... and must preserve *p*(up), i.e. preserve the *z*-axis.

$$\mathcal{G}_A = \mathcal{G}_B \simeq \mathrm{SO}(d-1).$$



Relativity: there's a frame of reference in which  $T_A$  happens before  $T_B$ ...

$$\mathcal{G}_A = \mathcal{G}_B \simeq \mathrm{SO}(d-1).$$



Relativity: there's a frame of reference in which  $T_A$  happens before  $T_B$ ... ... and another frame where it's the other way around.

$$\mathcal{G}_A = \mathcal{G}_B \simeq \mathrm{SO}(d-1).$$





Relativity: there's a frame of reference in which  $T_A$  happens before  $T_B$ ... ... and another frame where it's the other way around.

$$\mathcal{G}_A = \mathcal{G}_B \simeq \mathrm{SO}(d-1).$$



Relativity: there's a frame of reference in which  $T_A$  happens before  $T_B$ ... ... and another frame where it's the other way around.

$$\mathcal{G}_A = \mathcal{G}_B \simeq \mathrm{SO}(d-1).$$



So far, we assumed:  $\mathcal{G}_A = \mathcal{G}_B$ . Assumption of **relationality**.



So far, we assumed:  $\mathcal{G}_A = \mathcal{G}_B$ . Assumption of **relationality**.

Whatever happens in one arm can be **undone** in the other arm.



So far, we assumed:  $\mathcal{G}_A = \mathcal{G}_B$ . Assumption of **relationality**.

Whatever happens in one arm can be **undone** in the other arm.



So far, we assumed:  $\mathcal{G}_A = \mathcal{G}_B$ . Assumption of **relationality**.

Whatever happens in one arm can be **undone** in the other arm.

A1) Beam splitter can prepare any upper-branch probability p.
A2) Every pure state with the same p can be reached by reversible operations applied locally on the two arms.
A3) The groups of operations of A and B are isomorphic.

A1) Beam splitter can prepare any upper-branch probability *p*.
A2) Every pure state with the same *p* can be reached by reversible operations applied locally on the two arms.
A3) The groups of operations of A and B are isomorphic.

**Theorem 6.2.** Under the assumptions A1, A2, A3, relativity of simultaneity (REL) allows for the following possibilities and not more:

- d = 1 (the classical bit), with  $\mathcal{G}_A = \mathcal{G}_B = \{\mathbf{1}\}$  (i.e. without any non-trivial local transformations),
- d = 2 (the quantum bit over the real numbers), with  $\mathcal{G}_A = \mathcal{G}_B = \mathbb{Z}_2$ ,
- d = 3 (the standard quantum bit over the complex numbers), with  $G_A = G_B = SO(2) = U(1)$ ,
- -d = 5 (the quaternionic quantum bit), with  $\mathcal{G}_{AB} = SO(4)$ ,  $\mathcal{G}_A$  the left- and  $\mathcal{G}_B$  the right-isoclinic rotations in SO(4) (or vice versa) which are both isomorphic to SU(2), and  $\mathcal{G}_A \cap \mathcal{G}_B = \{+\mathbb{I}, -\mathbb{I}\}$ .
A1) Beam splitter can prepare any upper-branch probability *p*.
A2) Every pure state with the same *p* can be reached by reversible operations applied locally on the two arms.
A3) The groups of operations of A and B are isomorphic.

**Theorem 6.2.** Under the assumptions A1, A2, A3, relativity of simultaneity (REL) allows for the following possibilities and not more:

- d = 1 (the classical bit), with  $\mathcal{G}_A = \mathcal{G}_B = \{\mathbf{1}\}$  (i.e. without any non-trivial local transformations),
- d = 2 (the quantum bit over the real numbers), with  $\mathcal{G}_A = \mathcal{G}_B = \mathbb{Z}_2$ ,
- d = 3 (the standard quantum bit over the complex numbers), with  $G_A = G_B = SO(2) = U(1)$ ,
- -d = 5 (the quaternionic quantum bit), with  $\mathcal{G}_{AB} = SO(4)$ ,  $\mathcal{G}_A$  the left- and  $\mathcal{G}_B$  the right-isoclinic rotations in SO(4) (or vice versa) which are both isomorphic to SU(2), and  $\mathcal{G}_A \cap \mathcal{G}_B = \{+\mathbb{I}, -\mathbb{I}\}$ .

#### Relativity of simultaneity singles out the **associative division algebras**.

# 1. Quantum (2,2,2)-Bell correlations from symmetry

2. **Open Research**: geometry from probability

3. Motivation: semi-device-independent QIT

4. Theory-independent randomness with spacetime symm.

# 1. Quantum (2,2,2)-Bell correlations from symmetry

2. **Open Research**: geometry from probability

- 3. Motivation: semi-device-independent QIT
- 4. Theory-independent randomness with spacetime symm.





• In **classical** physics / prob. theory:

$$P(a, b|x, y) = \sum_{\lambda \in \Lambda} P_A(a|x, \lambda) P_B(b|y, \lambda) P_{\Lambda}(\lambda)$$



• In **classical** physics / prob. theory:

$$P(a, b|x, y) = \sum_{\lambda \in \Lambda} P_A(a|x, \lambda) P_B(b|y, \lambda) P_{\Lambda}(\lambda)$$

• In **quantum** physics:

 $P(a, b|x, y) = \operatorname{tr}\left[\rho_{AB}(E_x^a \otimes F_y^b)\right]$ 



**No-signalling** conditions:

P(a|x, y) is independent of y, P(b|x, y) is independent of x.

• In **classical** physics / prob. theory:

$$P(a, b|x, y) = \sum_{\lambda \in \Lambda} P_A(a|x, \lambda) P_B(b|y, \lambda) P_{\Lambda}(\lambda)$$

• In quantum physics:

 $P(a, b|x, y) = \operatorname{tr} \left[ \rho_{AB}(E_x^a \otimes F_y^b) \right]$ 



**No-signalling** conditions:

P(a|x, y) is independent of y, P(b|x, y) is independent of x.

• In **classical** physics / prob. theory:

$$P(a, b|x, y) = \sum_{\lambda \in \Lambda} P_A(a|x, \lambda) P_B(b|y, \lambda) P_{\Lambda}(\lambda)$$

• In quantum physics:

$$P(a, b|x, y) = \operatorname{tr}\left[\rho_{AB}(E_x^a \otimes F_y^b)\right]$$

Quantum admits more general *P*'s due to the **violation of Bell inequalities**.

CHSH :=  $|C_{00} + C_{01} + C_{10} - C_{11}| \le 2$  where  $C_{ab} := \mathbb{E}(x \cdot y|a, b)$ .

CHSH :=  $|C_{00} + C_{01} + C_{10} - C_{11}| \le 2$  where  $C_{ab} := \mathbb{E}(x \cdot y|a, b)$ .



CHSH :=  $|C_{00} + C_{01} + C_{10} - C_{11}| \le 2$  where  $C_{ab} := \mathbb{E}(x \cdot y|a, b)$ .



S. Popescu and D. Rohrlich, Found. Phys. 24, 379 (1994):

Are quantum correlations the most general P(a, b|x, y) that satisfy the no-signalling principle?

CHSH :=  $|C_{00} + C_{01} + C_{10} - C_{11}| \le 2$  where  $C_{ab} := \mathbb{E}(x \cdot y|a, b)$ .



S. Popescu and D. Rohrlich, Found. Phys. 24, 379 (1994):

Are quantum correlations the most general P(a, b|x, y) that satisfy the no-signalling principle?

No. Counterexample: the PR-box correlations  $p(+1,+1|a,b) = p(-1,-1|a,b) = \frac{1}{2}$ if  $(a,b) \in \{(0,0), (0,1), (1,0)\}$  CHSH=4  $p(+1,-1|1,1) = p(-1,+1|1,1) = \frac{1}{2}$ 

CHSH :=  $|C_{00} + C_{01} + C_{10} - C_{11}| \le 2$  where  $C_{ab} := \mathbb{E}(x \cdot y|a, b)$ .



S. Popescu and D. Rohrlich, Found. Phys. 24, 379 (1994):

Are quantum correlations the most general P(a, b|x, y) that satisfy the no-signalling principle?

No. Counterexample: the PR-box correlations  $p(+1,+1|a,b) = p(-1,-1|a,b) = \frac{1}{2}$ if  $(a,b) \in \{(0,0), (0,1), (1,0)\}$  CHSH=4  $p(+1,-1|1,1) = p(-1,+1|1,1) = \frac{1}{2}$ 





## **No-signalling** conditions:

P(a|x, y) is independent of y, P(b|x, y) is independent of x.



## **No-signalling** conditions:

P(a|x, y) is independent of y, P(b|x, y) is independent of x.

### Why study such correlations?

- Foundational: "Why" does nature admit Q but not more? Principles?
- Applications in DI-independent protocols.

## Single black boxes





### Single black boxes



Inputs and outputs are typically taken as **abstract labels** (bits etc.)

Allce and Dob share a composite system. Locally and independently, each

Single black boxes an input (x and y), and then records the output (a and b).

The experiment is characterized as a black box by its joint conditional probability distribution P(a,b | x,y).



Inputs and outputs are typically inputs may have additional taken as **abstracting being project**<sup>1</sup> we consider when these inputs

## What if inputs (and / or outputs) are **spatiotemporal quantities**?





 $\Lambda \Lambda \Lambda \Lambda \Lambda \Lambda$ 

a

**ANGLES** The orientation of polarization filter in a inhomogeneity of a

DIRECTIONS The direction of photonic experiment. magnetic field.

**DURATIONS** The duration of Rabi oscillations applied

to an atomic system.

Suppose a black box P reacts to the direction of an applied external magnetic field. The statistics of obtaining outcome *a* are  $P(a | \mathbf{x})$ . Since the input is spatiotemporal, we could first rotate our device through some  $R^{-1} \in SO(3)$ , and then perform the same experiment. This composite procedure defines a new black box P', whose response to

Allce and Dob share a composite system. Locally and independently, each

Single black boxes an input (x and y), and then records the output (a and b).

The experiment is characterized as a black box by its joint conditional probability distribution P(a,b | x,y).

a



Inputs and outputs are typically inputs may have additional taken as **abstracting being project**<sup>1</sup> we consider when these inputs

What if inputs (and / or outputs) are **spatiotemporal quantities**?







**ANGLES** The orientation of The direction of polarization filter in a inhomogeneity of a photonic experiment. magnetic field.

**DURATIONS** The duration of Rabi oscillations applied to an atomic system.

This is the case in many actual experimental settings.

Suppose a black box P reacts to the direction of an applied external magnetic field. The statistics of obtaining outcome *a* are  $P(a | \mathbf{x})$ . Since the input is spatiotemporal, we could first rotate our device through some  $R^{-1} \in SO(3)$ , and then perform the same experiment. This composite procedure defines a new black box P', whose response to

composite system. Locally and independently, each

Single black boxes an input (x and y), and then records the output (a and b).

The experiment is characterized as a black box by its joint conditional probability distribution P(a,b|x,y).



Inputs and outputs are typically taken as **abstracting** inputs to spatiotemporal degrees of freedom.

What if inputs (and / or outputs) are **spatiotemporal quantities**?



ANGLESDIRECTIONSThe orientation of<br/>polarization filter in a<br/>photonic experiment.The direction of<br/>inhomogeneity of a<br/>magnetic field.



The duration of Rabi oscillations applied to an atomic system.

- This is the case in many actual experimental settings.
- Study interplay of probability, space and time under minimal assumptions (even without assuming QT).

Suppose a black box P reacts to the direction of an applied external magnetic field . The statistics of obtaining outcome *a* are P(*a*|**x**). Since the input is spatiotemporal, we could first rotate our device through some  $R^{-1} \in SO(3)$ , and then perform the same experiment. This composite procedure defines a new black box P', whose response to

composite system. Locally and independently, each

Single black boxes an input (x and y), and then records the output (a and b).

The experiment is characterized as a black box by its joint conditional probability distribution P(a,b|x,y).



Inputs and outputs are typically taken as **abstracting** in our project<sup>1</sup> we consider when these inputs taken as **abstracting one in spatiotemporal degrees of freedom**.

What if inputs (and / or outputs) are **spatiotemporal quantities**?



ANGLESDIRECTIONSThe orientation of<br/>polarization filter in a<br/>photonic experiment.The direction of<br/>inhomogeneity of a<br/>magnetic field.



- The duration of Rabi oscillations applied to an atomic system.
- This is the case in many actual experimental settings.
- Study interplay of probability, space and time under minimal assumptions (even without assuming QT).
- Use spacetime symmetries in protocols?

Suppose a black box P reacts to the direction of an applied external magnetic field . The statistics of obtaining outcome *a* are P( $a | \mathbf{x}$ ). Since the input is spatiotemporal, we could first rotate our device through some  $R^{-1} \in SO(3)$ , and then perform the same experiment. This composite procedure defines a new black box P', whose response to

composite system. Locally and independently, each

Single black boxes an input (x and y), and then records the output (a and b).

The experiment is characterized as a black box by its joint conditional probability distribution P(a,b|x,y).



Inputs and outputs are typically taken as **abstractive abstractive abstractive** 

What if inputs (and / or outputs) are **spatiotemporal quantities**?



ANGLESDIRECTIONSThe orientation of<br/>polarization filter in a<br/>photonic experiment.The direction of<br/>inhomogeneity of a<br/>magnetic field.



- This is the case in many actual experimental settings.
- Study interplay of probability, space and time under minimal assumptions (even without assuming QT).
- Use spacetime symmetries in protocols? Suppose a black box P reacts to the direction of an applied

and then perform the same experiment. This composite procedure defines a new black box P', whose response to











- Default direction of inhomogeneity of field:  $\vec{x}_0$ .
- Spatial rotation applied to it:  $R \in \mathcal{G} = SO(3)$ .





- Default direction of inhomogeneity of field:  $\vec{x}_0$ .
- Spatial rotation applied to it:  $R \in \mathcal{G} = SO(3)$ .
- Stabilizer subgroup  $\mathcal{H} \simeq \mathrm{SO}(2)$ , i.e.  $R\vec{x}_0 = \vec{x}_0$  for  $R \in \mathcal{H}$ .





- Default direction of inhomogeneity of field:  $\vec{x}_0$ .
- Spatial rotation applied to it:  $R \in \mathcal{G} = SO(3)$ .
- Stabilizer subgroup  $\mathcal{H} \simeq \mathrm{SO}(2)$ , i.e.  $R\vec{x}_0 = \vec{x}_0$  for  $R \in \mathcal{H}$ .
- Manifold of inputs: the **unit sphere**,  $S^2 = SO(3)/SO(2)$ .





- Default direction of inhomogeneity of field:  $\vec{x}_0$ .
- Spatial rotation applied to it:  $R \in \mathcal{G} = SO(3)$ .
- Stabilizer subgroup  $\mathcal{H} \simeq \mathrm{SO}(2)$ , i.e.  $R\vec{x}_0 = \vec{x}_0$  for  $R \in \mathcal{H}$ .
- Manifold of inputs: the **unit sphere**,  $S^2 = SO(3)/SO(2)$ .

• In general, inputs are elements of a homogeneous space,  $\mathcal{G}/\mathcal{H}$ .







**Example:** Stern-Gerlach experiment  $\mathcal{G} = SO(3)$  (spatial rotations)  $\mathcal{H} = SO(2)$  (axial symmetry of magnetic field)  $\vec{x} \in \mathcal{G}/\mathcal{H} = S^2$  (unit vector: field direction)





**Example:** Polarizer,  $P(a|\alpha)$ .  $\mathcal{G} = SO(2)$  (rotations around beam axis)  $\mathcal{H} = \{\mathbf{1}\}$  (no additional symmetry)  $\alpha \in \mathcal{G}/\mathcal{H} = SO(2).$ 



click / no click:  $a = \pm 1$ .



**Example:** Input is time t, P(a|t).  $\mathcal{G} = (\mathbb{R}, +)$  (group of time translations)  $\mathcal{H} = \{1\}$  (no additional symmetry)  $\vec{x} = t \in \mathbb{R}$ 






$$\mathcal{G} = \mathrm{SO}(2) \times \mathrm{SO}(2)$$

$$T_{\alpha,\beta} = \bigoplus_{m,n} \begin{pmatrix} \cos(m\alpha - n\beta) & \sin(m\alpha - n\beta) \\ -\sin(m\alpha - n\beta) & \cos(m\alpha - n\beta) \end{pmatrix}.$$



$$P(a, b | \alpha, \beta) := \sum_{m=0}^{2J} \sum_{n=-2J}^{2J} c_{mn}^{ab} \cos(m\alpha - n\beta) + s_{mn}^{ab} \sin(m\alpha - n\beta),$$

$$\mathcal{G} = \mathrm{SO}(2) \times \mathrm{SO}(2)$$

$$T_{\alpha,\beta} = \bigoplus_{m,n} \begin{pmatrix} \cos(m\alpha - n\beta) & \sin(m\alpha - n\beta) \\ -\sin(m\alpha - n\beta) & \cos(m\alpha - n\beta) \end{pmatrix}.$$



**Examples:**  $C(\alpha, \beta) := \sum_{a,b=-1}^{+1} abP(a, b|\alpha, \beta)$   $(a, b = \pm 1)$ 



$$P(a, b | \alpha, \beta) := \sum_{m=0}^{2J} \sum_{n=-2J}^{2J} c_{mn}^{ab} \cos(m\alpha - n\beta) + s_{mn}^{ab} \sin(m\alpha - n\beta),$$

 $= C(-2) = \sum^{+1} ID(-1)$ 

**Examples:**  $C(\alpha, \beta) := \sum_{a,b=-1}^{+1} abP(a,b|\alpha,\beta)$   $(a,b=\pm 1)$ 

• Two-photon singlet state:  $C(\alpha, \beta) = -\cos[2(\alpha - \beta)].$ 



$$P(a, b | \alpha, \beta) := \sum_{m=0}^{2J} \sum_{n=-2J}^{2J} c_{mn}^{ab} \cos(m\alpha - n\beta) + s_{mn}^{ab} \sin(m\alpha - n\beta),$$

**Examples:**  $C(\alpha, \beta) := \sum_{a,b=-1}^{+1} abP(a,b|\alpha,\beta)$   $(a,b=\pm 1)$ 

• Two-photon singlet state:

$$C(\alpha,\beta) = -\cos[2(\alpha-\beta)].$$

• Science-fiction polarizers:  

$$C(\alpha, \beta) = -\frac{2}{7} \cos[3(\alpha - \beta)] - \cos(\alpha - \beta)$$



$$P(a, b | \alpha, \beta) := \sum_{m=0}^{2J} \sum_{n=-2J}^{2J} c_{mn}^{ab} \cos(m\alpha - n\beta) + s_{mn}^{ab} \sin(m\alpha - n\beta),$$

 $\mathcal{G} = \mathrm{SO}(2) \times \mathrm{SO}(2)$ 

**Examples:**  $C(\alpha, \beta) := \sum_{a,b=-1}^{+1} abP(a, b|\alpha, \beta)$ 

- Two-photon singlet state:  $C(\alpha, \beta) = -\cos[2(\alpha - \beta)].$
- Science-fiction polarizers:  $C(\alpha,\beta) = -\frac{2}{7}\cos[3(\alpha-\beta)] - \cos(\alpha-\beta).$



"science-fictionpolarizers"

A. J. P. Garner, M. Krumm, MM, Phys. Rev. Research 2, 013112 (2020).

A. J. P. Garner, M. Krumm, MM, Phys. Rev. Research 2, 013112 (2020).



 $\mathcal{G} = \mathrm{SO}(d) \times \mathrm{SO}(d)$  $(d \ge 2)$ 

A. J. P. Garner, M. Krumm, MM, Phys. Rev. Research 2, 013112 (2020).



 $\mathcal{G} = \mathrm{SO}(d) \times \mathrm{SO}(d)$ 

 $(d \ge 2)$ 

## Assumptions for now:

Probabilities transform **locally fundamentally**, i.e.  $P(a, b | R\vec{x}_0, S\vec{y}_0)$  is linear in the rotation matrices R, S.

A. J. P. Garner, M. Krumm, MM, Phys. Rev. Research 2, 013112 (2020).



## Assumptions for now:

Probabilities transform **locally fundamentally**, i.e.  $P(a, b | R\vec{x}_0, S\vec{y}_0)$  is linear in the rotation matrices R, S.

 $\mathcal{G} = \mathrm{SO}(d) \times \mathrm{SO}(d)$  $(d \ge 2)$ 

Reversing the input  $\vec{x} \mapsto -\vec{x}$ reverses the output  $a \mapsto -a$ .

A. J. P. Garner, M. Krumm, MM, Phys. Rev. Research 2, 013112 (2020).



### Assumptions for now:

Probabilities transform **locally fundamentally**, i.e.  $P(a, b | R\vec{x}_0, S\vec{y}_0)$  is linear in the rotation matrices R, S.

 $\mathcal{G} = \mathrm{SO}(d) \times \mathrm{SO}(d)$  $(d \ge 2)$ 

Reversing the input  $\vec{x} \mapsto -\vec{x}$ reverses the output  $a \mapsto -a$ .

Theorem. In any world where these assumptions hold (not assuming QT!), Alice and Bob see quantum correlations (i.e. in Q). (For arbitrarily many settings, 2 outcomes.)

A. J. P. Garner, M. Krumm, MM, Phys. Rev. Research 2, 013112 (2020).



## Assumptions for now:

Probabilities transform **locally fundamentally**, i.e.  $P(a, b | R\vec{x}_0, S\vec{y}_0)$  is linear in the rotation matrices R, S.

 $\mathcal{G} = \mathrm{SO}(d) \times \mathrm{SO}(d)$  $(d \ge 2)$ 

Reversing the input  $\vec{x} \mapsto -\vec{x}$ reverses the output  $a \mapsto -a$ .

**Theorem:** The quantum (2,2,2)-correlations **Q** are **exactly those** that can be obtained by  $SO(d) \times SO(d)$ -boxes that satisfy the assumptions above, restricted to 2 inputs per party, and supplemented with shared randomness.

## 1. Quantum (2,2,2)-Bell correlations from symmetry

2. **Open Research**: geometry from probability

- 3. Motivation: semi-device-independent QIT
- 4. Theory-independent randomness with spacetime symm.

# 1. Quantum (2,2,2)-Bell correlations from symmetry

2. **Open Research**: geometry from probability

## 3. Motivation: semi-device-independent QIT

4. Theory-independent randomness with spacetime symm.

## Open Research: geometry from probability

Very related to Wootters' insights. See also:

R. Penrose, Angular Momentum: An Approach to Combinatorial Space-Time, 1971.

MM, S. Carrozza, and P. A. Höhn, *Is the local linearity of space-time inherited from the linearity of probabilities?*, J. Phys. A: Math. Theor. **50**, 054003 (2017).

### Very related to Wootters' insights. See also:

R. Penrose, Angular Momentum: An Approach to Combinatorial Space-Time, 1971.

MM, S. Carrozza, and P. A. Höhn, *Is the local linearity of space-time inherited from the linearity of probabilities?*, J. Phys. A: Math. Theor. **50**, 054003 (2017).

Why should there be linear or Euclidean structure in our world?!







### Very related to Wootters' insights. See also:

R. Penrose, Angular Momentum: An Approach to Combinatorial Space-Time, 1971.

MM, S. Carrozza, and P. A. Höhn, *Is the local linearity of space-time inherited from the linearity of probabilities?*, J. Phys. A: Math. Theor. **50**, 054003 (2017).

Why should there be linear or Euclidean structure in our world?!







$$p(a) = \sum_{b} p(a|b)p(b).$$

These structures are very well-motivated in probability theory!

#### Open Research: geometry from probability



Bill Wootters, PhD thesis, 1980: "The Acquisition of Information from Quantum Measurements":



### Open Research: geometry from probability



Bill Wootters, PhD thesis, 1980: "The Acquisition of Information from Quantum Measurements":



"But why should the statistical distance between two orientations be equal to the angle between them? The best answer we know is the one given at the end of Section A, namely, that the angles we observe in nature may ultimately be derived from the probabilities of the outcomes of spin measurements, which are more primary."

## Rules of the game





You are given two black boxes, for which the manufacturer promises that they implement projective Stern-Gerlach measurements along some directions a and b that you don't know. The devices give the result (+ or -) on a digital display. You find "devices" in your world that prepare spin-(1/2) systems in states. You can press a button and prepare the state, but don't know which one

it is. The universe gives a supply of many such devices (not necessarily uniformly distributed), exhausting the quantum state space.





You are given two black boxes, for which the manufacturer promises that they implement projective Stern-Gerlach measurements along some directions a and b that you don't know.

The devices give the result (+ or -) on a digital display.

You find "devices" in your world that prepare spin-(1/2) systems in states. You can press a button and prepare the state, but don't know which one it is. The universe gives a supply of many such devices (not necessarily uniformly distributed), exhausting the quantum state space.

**Goal:** determine the angle  $\angle(\vec{a}, \vec{b})$ .

**Note:** you are only allowed to "press buttons" and record digital outcomes. You don't know how to measure lengths, angles, add vectors...

However, you know the type of system that a device prepares.



### Rules of the game



## Sketch of solution:

• Search the world for preparation devices until you find one such that, for the systems prepared by that state if fed into device A,

 $p_A(+) \approx 1.$ 

• Feed the states of that device into measurement device B. Then:

$$p_B(+) \approx \cos^2 \frac{\angle(\vec{a}, \vec{b})}{2}.$$

## Rules of the game



## Sketch of solution:

• Search the world for preparation devices until you find one such that, for the systems prepared by that state if fed into device A,

$$p_A(+) \approx 1.$$

• Feed the states of that device into measurement device B. Then:

$$p_B(+) \approx \cos^2 \frac{\angle(\vec{a}, \vec{b})}{2}.$$

### **Research questions:**

- What are the detailed operational assumptions in this scenario?
- Can we get rid of the assumption of a *projective* measurement?
- Can we show that this is (suitably generalized) *classically impossible*?

# 1. Quantum (2,2,2)-Bell correlations from symmetry

2. **Open Research**: geometry from probability

## 3. Motivation: semi-device-independent QIT

4. Theory-independent randomness with spacetime symm.

## 1. Quantum (2,2,2)-Bell correlations from symmetry

2. **Open Research**: geometry from probability

3. Motivation: semi-device-independent QIT

4. Theory-independent randomness with spacetime symm.

**Goal:** Generate certified random bits.

**Goal:** Generate certified random bits.

Why not just send single photons on a half-silvered mirror?



**Goal:** Generate certified random bits.

Why not just send single photons on a half-silvered mirror?



**Goal:** Generate certified random bits.

Why not just send single photons on a half-silvered mirror?



### **Device-independent** randomness expansion:

Violation of Bell inequality  $\Rightarrow$  outcomes uncorrelated with rest of the world

See e.g.: A. Acín, *Randomness and quantum non-locality*, QCRYPT 2012 talk. V. Scarani, *Bell nonlocality*, Oxford Graduate Texts (2019).

Semi-device-independent (SDI): allow communication, add assumption.

Semi-device-independent (SDI): allow communication, add assumption.

$$x \in \{1, 2, 3, 4\} \longrightarrow S \xrightarrow{\rho_x} M \xrightarrow{\rho_x} x \in \{1, 2\}$$
$$x \in \{1, 2, 3, 4\} \xrightarrow{\mathbf{S}} \mathbf{S} \xrightarrow{\mathrm{dim}\,\mathcal{H} = 2} \xrightarrow{\mathbf{M} \to a \in \{\pm 1\}} \mathbf{M}$$

$$g \in \{1, 2\} \xrightarrow{\lambda} \mathbf{M} \xrightarrow{\lambda} \mathbf{$$

$$x \in \{1, 2, 3, 4\}$$
  $\longrightarrow$   $S$   $\longrightarrow$   $M$   $\longrightarrow$   $a \in \{\pm 1\}$   
Observed correlations  $p(c|x, y)$  imply  $H(A|X, Y, \Lambda) \gg 0$ .  
Drawback, assumption not physically well-motivated & requires QT.



$$x \in \{1, 2, 3, 4\} \xrightarrow{\mathbf{S}} \mathbf{S} \xrightarrow{\mathrm{dim}\,\mathcal{H} = 2} \xrightarrow{\mathbf{M} \to a \in \{\pm 1\}} \mathbf{M}$$

$$g \in \{1, 2\} \xrightarrow{\lambda} \mathbf{M} \xrightarrow{\lambda} \mathbf{$$

**Drawback:** assumption not physically well-motivated & requires QT.

**Observation:** in many experiments, settings are spatiotemporal quantities.

Idea: reformulate in terms of spacetime symmetries, w/o assuming QT. Can quantum phenomenology / functionality be reproduced?

# 1. Quantum (2,2,2)-Bell correlations from symmetry

2. **Open Research**: geometry from probability

3. Motivation: semi-device-independent QIT

4. Theory-independent randomness with spacetime symm.

# 1. Quantum (2,2,2)-Bell correlations from symmetry

2. **Open Research**: geometry from probability

3. Motivation: semi-device-independent QIT

4. Theory-independent randomness with spacetime symm.







If input is x=1: do nothing to preparation device; if x=2: **rotate it** (relative to measurement device) **by angle** α.



If input is x=1: do nothing to preparation device; if x=2: **rotate it** (relative to measurement device) **by angle** α.

SDI assumption: "spin" of system ≤ J

No further assumptions on devices / system.



If input is x=1: do nothing to preparation device; if x=2: **rotate it** (relative to measurement device) **by angle** α.

SDI assumption: "spin" of system ≤ J No further assumptions on devices / system.

Rotation described by (projective) unitary representation of SO(2):

$$U_{\alpha} = \bigoplus_{j=-J}^{J} n_j e^{ij\alpha}, \qquad P(b|\alpha) = \operatorname{tr}(M_b U_{\alpha} \rho U_{\alpha}^{\dagger}).$$









 "Boring" deterministic correlations: outcome b independent of x





 "Boring" deterministic correlations: outcome b independent of x

 "Interesting" deterministic correlations: outcome b is a function of x





- "Boring" deterministic correlations: outcome b independent of x
- "Interesting" deterministic correlations: outcome b is a function of x

Suppose  $(E_1, E_2)$  observed. Looks random. But:





 "Boring" deterministic correlations: outcome b independent of x

 "Interesting" deterministic correlations: outcome b is a function of x

Suppose  $(E_1, E_2)$  observed. Looks random. But:  $(E_1, E_2) = \sum_{\lambda} p(\lambda) (E_1^{(\lambda)}, E_2^{(\lambda)})_{det}$ 





 "Boring" deterministic correlations: outcome b independent of x

 "Interesting" deterministic correlations: outcome b is a function of x

Suppose  $(E_1, E_2)$  observed. Looks random. But:  $(E_1, E_2) = \sum_{\lambda} p(\lambda) (E_1^{(\lambda)}, E_2^{(\lambda)})_{det}$ 





Which correlations are possible?



Which correlations are possible? Theorem: exactly those:  $\frac{1}{2} \left( \sqrt{1+E_1} \sqrt{1+E_2} + \sqrt{1-E_1} \sqrt{1-E_2} \right) \ge \begin{cases} \cos(J\alpha) & \text{if } |J\alpha| < \frac{\pi}{2} \\ 0 & \text{if } |J\alpha| > \frac{\pi}{2} \end{cases}$ 

C. L. Jones, S. L. Ludescher, A. Aloy, MM, arXiv:2210.14811

using results of

T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, S. Pironio, Quantum 1, 33 (2017).



(-1,+1)

 $E_2$ 

(-1, -1)

 $\boldsymbol{\Gamma}$ 



Which correlations are possible? **Theorem:** exactly those:

$$\frac{1}{2}\left(\sqrt{1+E_1}\sqrt{1+E_2} + \sqrt{1-E_1}\sqrt{1-E_2}\right) \ge \begin{cases} \cos(J\alpha) & \text{if } |J\alpha| < \frac{\pi}{2} \\ 0 & \text{if } |J\alpha| \ge \frac{\pi}{2} \end{cases}$$



## Blue curved set of correlations.

If observed correlation away from red line: certifiable private randomness.





- Can we formulate our SDI assumption without quantum terminology?
- Can we use the protocol to certify random numbers without QT?



- Can we formulate our SDI assumption without quantum terminology?
- Can we use the protocol to certify random numbers without QT?
- Can we understand the curved boundary of correlations from spatial symmetry alone, without assuming QT?





- Can we formulate our SDI assumption without quantum terminology?
- Can we use the protocol to certify random numbers without QT?
- Can we understand the curved boundary of correlations from spatial symmetry alone, without assuming QT?

Yes we can:



$$\mathcal{Q}_J := \left\{ \alpha \mapsto p(+1|\alpha) \mid p(b|\alpha) = \operatorname{tr}(M_b U_\alpha \rho U_\alpha^{\dagger}) \right\},\,$$

- $\{E_b\}$  some POVM,  $\rho$  some density matrix,
- $U_{\alpha} = \bigoplus_{j=-J}^{J} n_j e^{ij\alpha}$ , with arbitrary multiplicities  $n_j$ .

$$\mathcal{Q}_J := \left\{ \alpha \mapsto p(+1|\alpha) \mid p(b|\alpha) = \operatorname{tr}(M_b U_\alpha \rho U_\alpha^{\dagger}) \right\},\,$$

- $\{E_b\}$  some POVM,  $\rho$  some density matrix,
- $U_{\alpha} = \bigoplus_{j=-J}^{J} n_j e^{ij\alpha}$ , with arbitrary multiplicities  $n_j$ .

**Consequence:** every *p* is a trigonometric polynomial of degree 2**J** 

(e.g. 
$$p(+|\alpha) = \frac{1}{2} + \frac{1}{2}\cos\alpha$$
 for  $J = \frac{1}{2}$  ).

$$\mathcal{Q}_J := \left\{ \alpha \mapsto p(+1|\alpha) \mid p(b|\alpha) = \operatorname{tr}(M_b U_\alpha \rho U_\alpha^{\dagger}) \right\},\,$$

- $\{E_b\}$  some POVM,  $\rho$  some density matrix,
- $U_{\alpha} = \bigoplus_{j=-J}^{J} n_j e^{ij\alpha}$ , with arbitrary multiplicities  $n_j$ .

**Consequence:** every *p* is a trigonometric polynomial of degree 2**J** 

(e.g. 
$$p(+|\alpha) = \frac{1}{2} + \frac{1}{2}\cos\alpha$$
 for  $J = \frac{1}{2}$ ).

• Definition of (general) **spin-J rotation boxes**:

$$\mathcal{R}_J := \left\{ \alpha \mapsto p(+1|\alpha) = c_0 + \sum_{j=1}^{2J} c_j \cos(j\alpha) + s_j \sin(j\alpha) \right\},\$$
$$0 \le p(+1|\alpha) \le 1 \quad \text{for all } \alpha.$$

$$\mathcal{Q}_J := \left\{ \alpha \mapsto p(+1|\alpha) \mid p(b|\alpha) = \operatorname{tr}(M_b U_\alpha \rho U_\alpha^{\dagger}) \right\},\,$$

• Definition of (general) **spin-J rotation boxes**:

$$\mathcal{R}_J := \left\{ \alpha \mapsto p(+1|\alpha) = c_0 + \sum_{j=1}^{2J} c_j \cos(j\alpha) + s_j \sin(j\alpha) \right\},\,$$

$$\mathcal{Q}_J := \left\{ \alpha \mapsto p(+1|\alpha) \mid p(b|\alpha) = \operatorname{tr}(M_b U_\alpha \rho U_\alpha^{\dagger}) \right\},\,$$

• Definition of (general) **spin-J rotation boxes**:

$$\mathcal{R}_J := \left\{ \alpha \mapsto p(+1|\alpha) = c_0 + \sum_{j=1}^{2J} c_j \cos(j\alpha) + s_j \sin(j\alpha) \right\},\,$$

$$\mathcal{Q}_J := \left\{ \alpha \mapsto p(+1|\alpha) \mid p(b|\alpha) = \operatorname{tr}(M_b U_\alpha \rho U_\alpha^{\dagger}) \right\},\,$$

• Definition of (general) **spin-J rotation boxes**:

$$\mathcal{R}_J := \left\{ \alpha \mapsto p(+1|\alpha) = c_0 + \sum_{j=1}^{2J} c_j \cos(j\alpha) + s_j \sin(j\alpha) \right\},\,$$

Clearly  $Q_J \subseteq \mathcal{R}_J$ .

$$\mathcal{Q}_J := \left\{ \alpha \mapsto p(+1|\alpha) \mid p(b|\alpha) = \operatorname{tr}(M_b U_\alpha \rho U_\alpha^{\dagger}) \right\},\,$$

• Definition of (general) **spin-J rotation boxes**:

$$\mathcal{R}_J := \left\{ \alpha \mapsto p(+1|\alpha) = c_0 + \sum_{j=1}^{2J} c_j \cos(j\alpha) + s_j \sin(j\alpha) \right\},\,$$

Clearly  $Q_J \subseteq \mathcal{R}_J$ .

It can be shown directly that  $\mathcal{Q}_0 = \mathcal{R}_0$  and  $\mathcal{Q}_{1/2} = \mathcal{R}_{1/2}$ .

However, for some larger **J**, we have  $Q_J \subsetneq \mathcal{R}_J$ , details soon:

A. Aloy, T. Galley, C. L. Jones, S. L. Ludescher, MM, upcoming (2023).

$$\mathcal{Q}_J := \left\{ \alpha \mapsto p(+1|\alpha) \mid p(b|\alpha) = \operatorname{tr}(M_b U_\alpha \rho U_\alpha^{\dagger}) \right\},\,$$

• Definition of (general) **spin-J rotation boxes**:

$$\mathcal{R}_J := \left\{ \alpha \mapsto p(+1|\alpha) = c_0 + \sum_{j=1}^{2J} c_j \cos(j\alpha) + s_j \sin(j\alpha) \right\},\,$$

Clearly  $Q_J \subseteq \mathcal{R}_J$ . It can be shown directly that  $Q_0 = \mathcal{R}_0$  and  $Q_{1/2} = \mathcal{R}_{1/2}$ . However, for some larger J, we have  $Q_J \subsetneq \mathcal{R}_J$ , details soon: A. Aloy, T. Galley, C. L. Jones, S. L. Ludescher, MM, upcoming (2023).

 $\mathcal{R}_J$  from rep. of SO(2) on (non-quantum) "orbitope" state spaces

# Boxes for only **two** input angles
$$\frac{1}{2} \left( \sqrt{1 + E_1} \sqrt{1 + E_2} + \sqrt{1 - E_1} \sqrt{1 - E_2} \right) \ge \begin{cases} \cos(J\alpha) & \text{if } |J\alpha| < \frac{\pi}{2} \\ 0 & \text{if } |J\alpha| \ge \frac{\pi}{2} \end{cases}$$



$$\frac{1}{2} \left( \sqrt{1 + E_1} \sqrt{1 + E_2} + \sqrt{1 - E_1} \sqrt{1 - E_2} \right) \ge \begin{cases} \cos(J\alpha) & \text{if } |J\alpha| < \frac{\pi}{2} \\ 0 & \text{if } |J\alpha| \ge \frac{\pi}{2} \end{cases}$$



$$\frac{1}{2} \left( \sqrt{1 + E_1} \sqrt{1 + E_2} + \sqrt{1 - E_1} \sqrt{1 - E_2} \right) \ge \begin{cases} \cos(J\alpha) & \text{if } |J\alpha| < \frac{\pi}{2} \\ 0 & \text{if } |J\alpha| \ge \frac{\pi}{2} \end{cases}$$



$$\frac{1}{2}\left(\sqrt{1+E_1}\sqrt{1+E_2} + \sqrt{1-E_1}\sqrt{1-E_2}\right) \ge \begin{cases} \cos(J\alpha) & \text{if } |J\alpha| < \frac{\pi}{2} \\ 0 & \text{if } |J\alpha| \ge \frac{\pi}{2} \end{cases}$$



**Theorem:**  $Q_{J,\alpha} = \mathcal{R}_{J,\alpha}$ . C. L. Jones, S. L. Ludescher, A. Aloy, MM, arXiv:2210.14811

$$\frac{1}{2} \left( \sqrt{1 + E_1} \sqrt{1 + E_2} + \sqrt{1 - E_1} \sqrt{1 - E_2} \right) \ge \begin{cases} \cos(J\alpha) & \text{if } |J\alpha| < \frac{\pi}{2} \\ 0 & \text{if } |J\alpha| \ge \frac{\pi}{2} \end{cases}$$



**Theorem:**  $Q_{J,\alpha} = \mathcal{R}_{J,\alpha}$ . C. L. Jones, S. L. Ludescher, A. Aloy, MM, arXiv:2210.14811

Can derive set of quantum correlations without assuming QT.

$$\frac{1}{2} \left( \sqrt{1 + E_1} \sqrt{1 + E_2} + \sqrt{1 - E_1} \sqrt{1 - E_2} \right) \ge \begin{cases} \cos(J\alpha) & \text{if } |J\alpha| < \frac{\pi}{2} \\ 0 & \text{if } |J\alpha| \ge \frac{\pi}{2} \end{cases}$$



**Theorem:**  $Q_{J,\alpha} = \mathcal{R}_{J,\alpha}$ . C. L. Jones, S. L. Ludescher, A. Aloy, MM, arXiv:2210.14811

Can derive set of quantum correlations without assuming QT.

Even eavesdropper with classical side information about beyond-quantum physics cannot predict the outcomes.

