ÖAW AUSTRIAN ACADEMY OF SCIENCES

IQOQI – INSTITUTE FOR QUANTUM OPTICS AND QUANTUM INFORMATION VIENNA

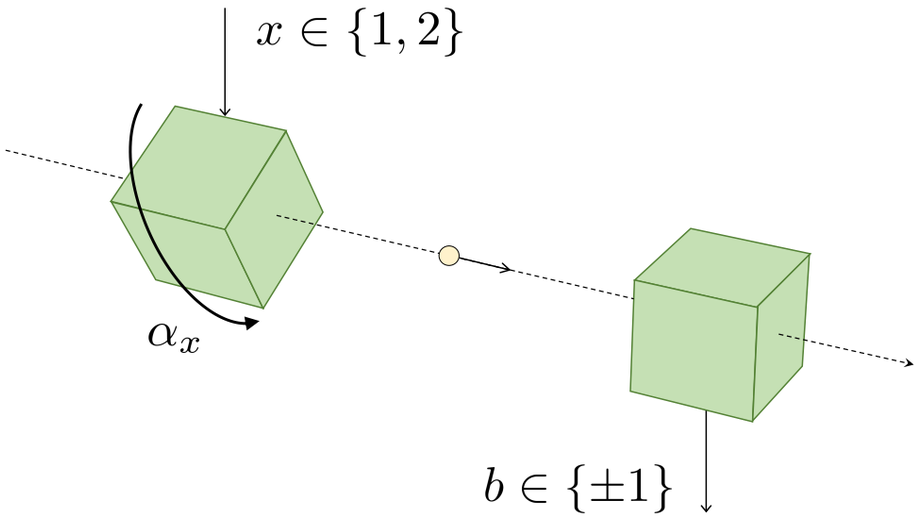
IQI

PI PERIMETER INSTITUTE

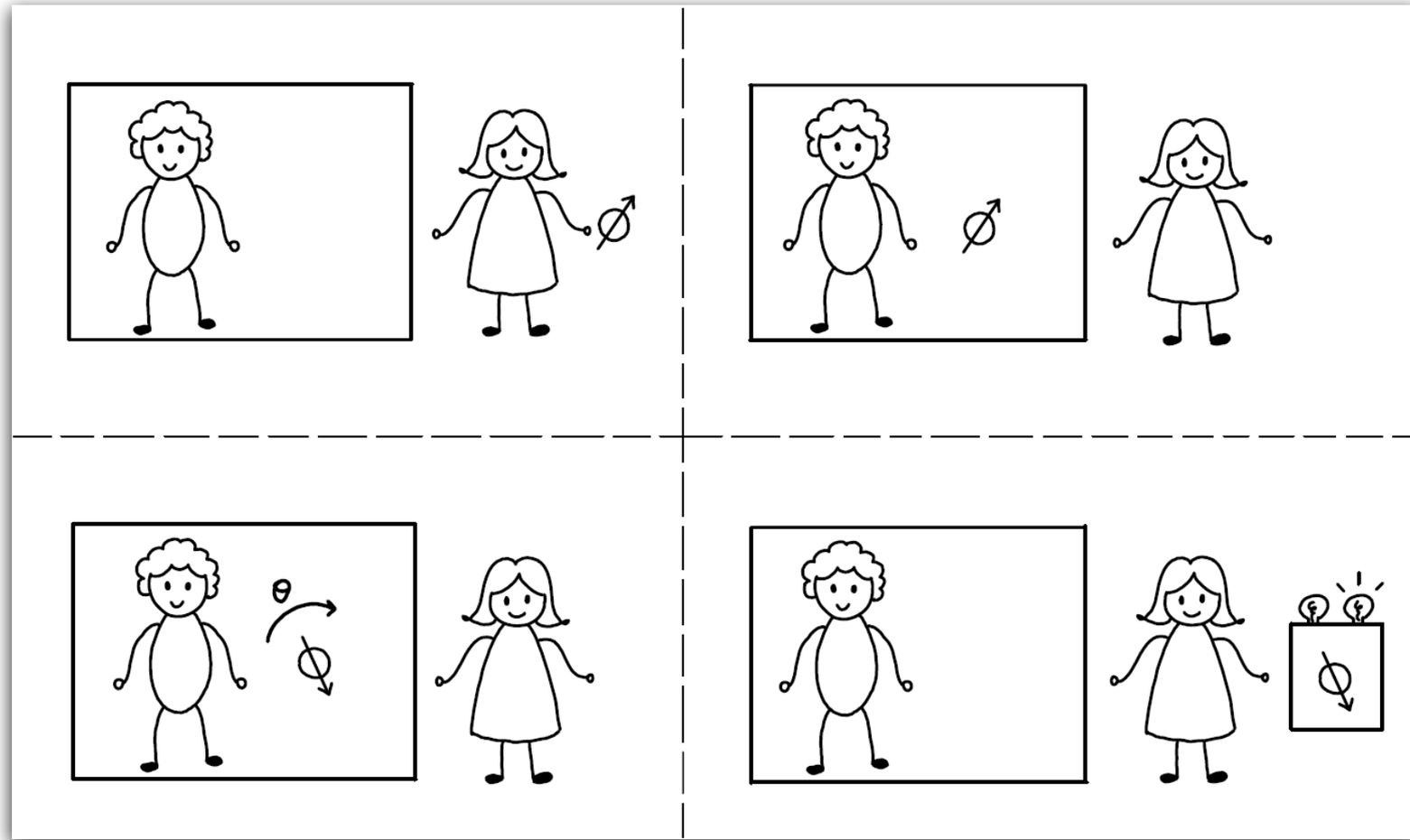
How can probabilities of events depend on spatial rotations in any physical theory?

Markus P. Müller

IQOQI Vienna & Perimeter Institute



FWF Austrian Science Fund



Overview

1. Motivation (and some history)

2. “Rotation boxes” within and beyond QT

3. A metrological game and the (sub)optimality of QT

4. A theory-independent SDI randomness generator

5. Conclusions

Overview

1. Motivation (and some history)

2. “Rotation boxes” within and beyond QT

3. A metrological game and the (sub)optimality of QT

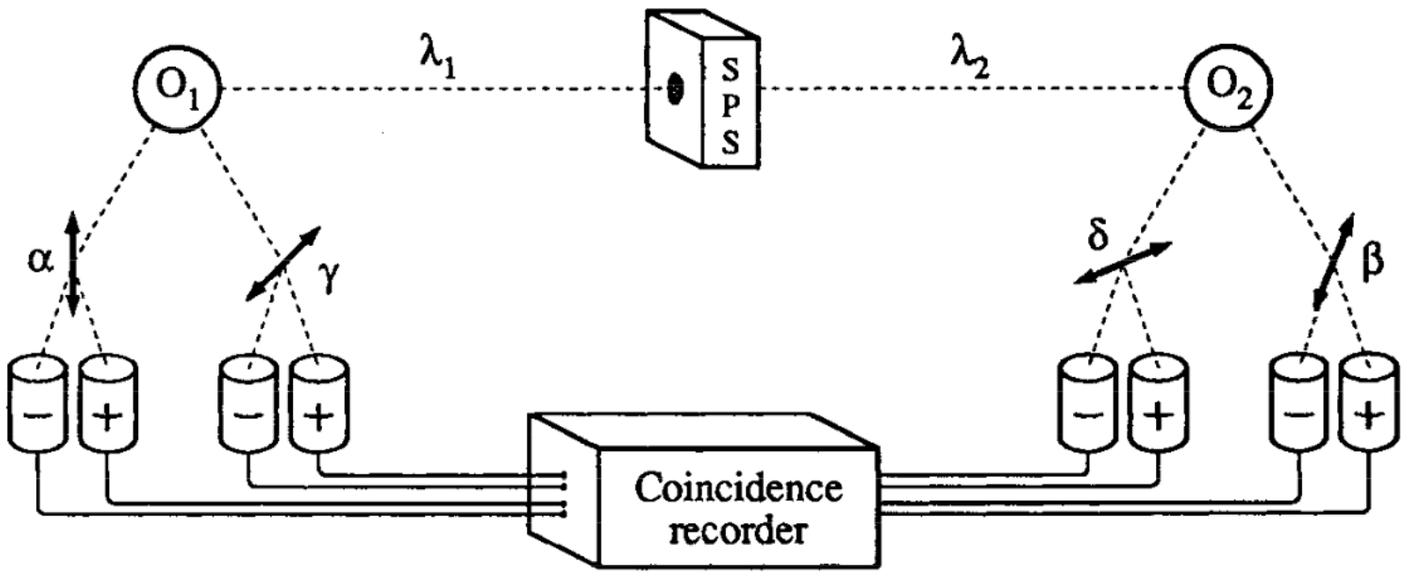
4. A theory-independent SDI randomness generator

5. Conclusions

"Rotation boxes": fourfold motivation

"Rotation boxes": fourfold motivation

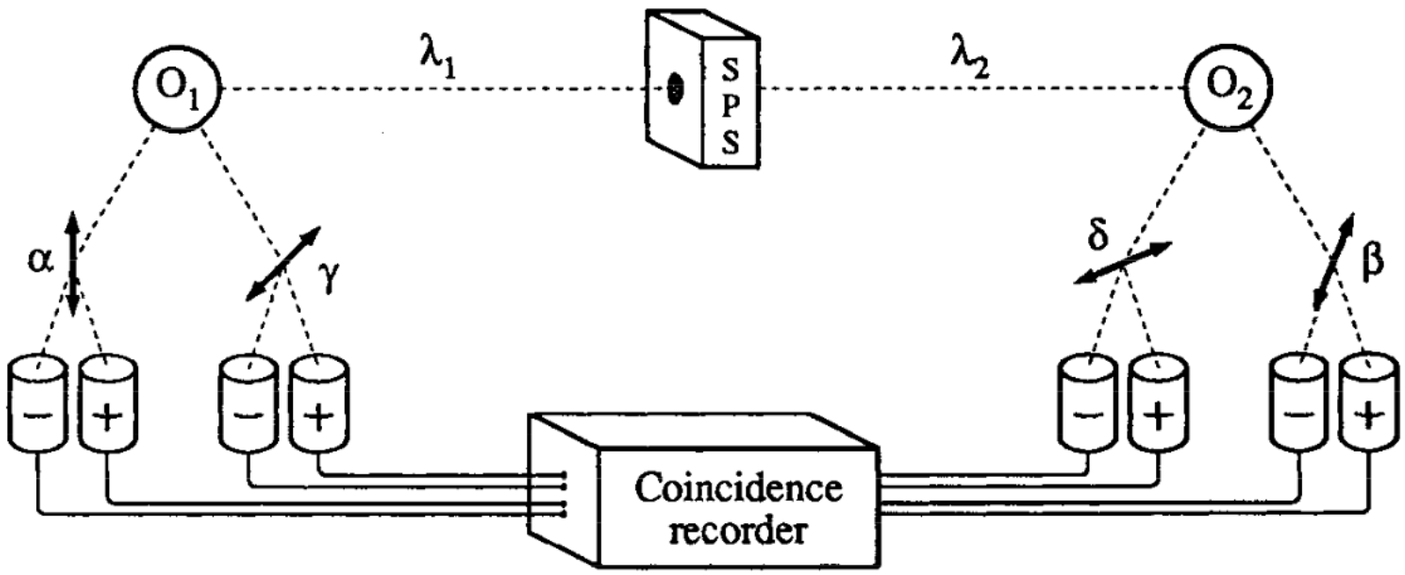
- Why all those **sin**es and **cos**ines in the oldfashioned textbooks? What is the theory-independent status of this?



$$P(a,b|\alpha,\beta) = \frac{1}{4}\left[1 + ab\cos 2(\alpha-\beta)\right]$$

"Rotation boxes": fourfold motivation

- Why all those **sin**es and **cos**ines in the oldfashioned textbooks?
  What is the theory-independent status of this?

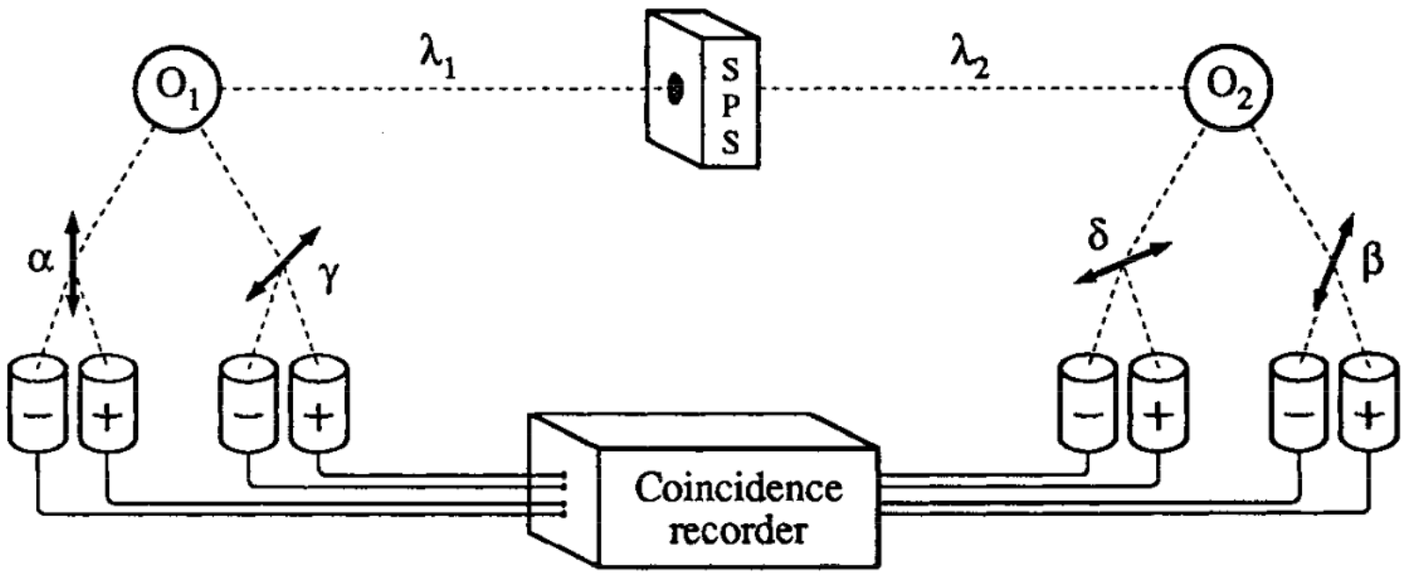


$$P(a,b|\alpha,\beta) = \frac{1}{4}\left[1 + ab\cos 2(\alpha-\beta)\right]$$

- (Very, *very* broadly speaking) **quantum gravity**:
  Spacetime vs. probabilities in the logical structure of our world?

"Rotation boxes": fourfold motivation

- Why all those **sin**es and **cos**ines in the oldfashioned textbooks?
  What is the theory-independent status of this?



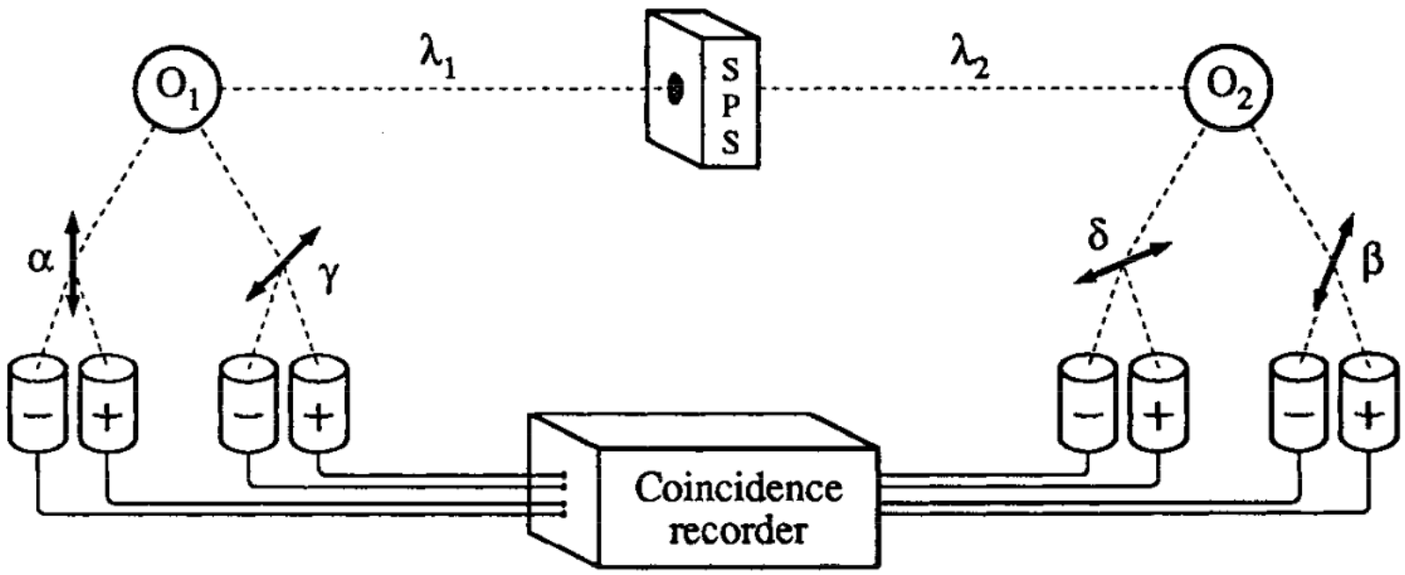
$$P(a,b|\alpha,\beta) = \frac{1}{4}\left[1 + ab\cos 2(\alpha-\beta)\right]$$

- (Very, *very* broadly speaking) **quantum gravity**:
  Spacetime vs. probabilities in the logical structure of our world?

- **Applications**: Harness the structure of space and time to constrain the correlations / certify randomness from fewer assumptions etc.?

"Rotation boxes": fourfold motivation

- Why all those **sin**es and **cos**ines in the oldfashioned textbooks?
  What is the theory-independent status of this?



$$P(a,b|\alpha,\beta) = \frac{1}{4}\left[1 + ab\cos 2(\alpha-\beta)\right]$$

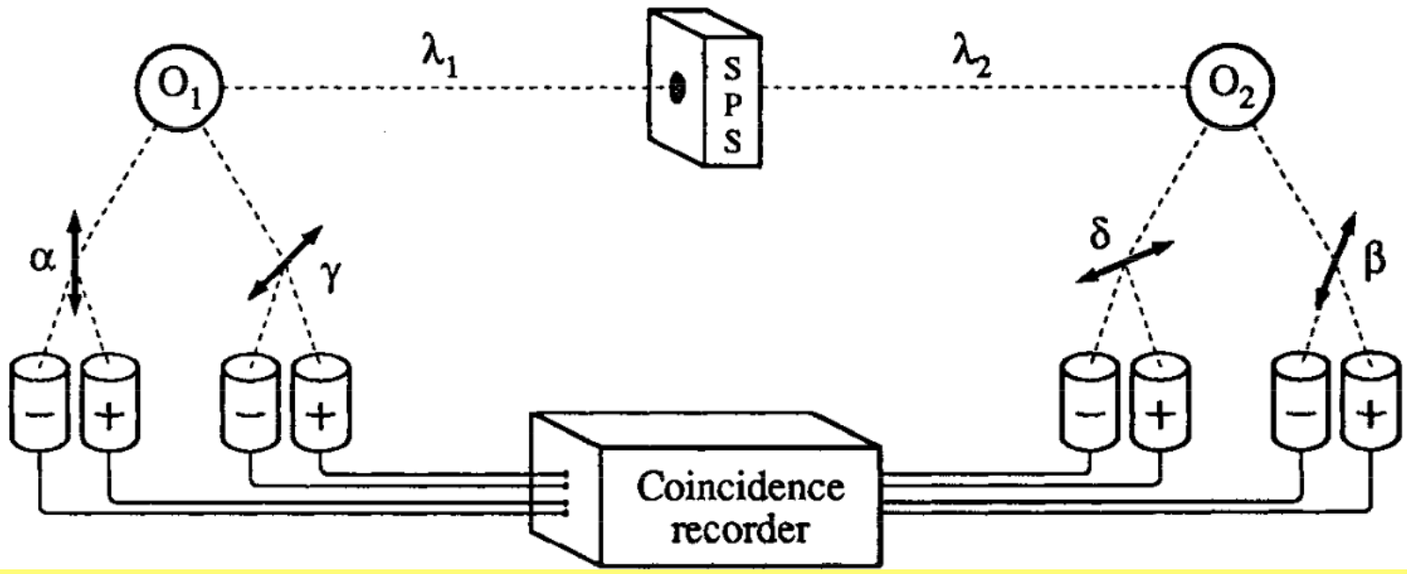
- (Very, *very* broadly speaking) **quantum gravity**:
  Spacetime vs. probabilities in the logical structure of our world?

- **Applications**: Harness the structure of space and time to constrain the correlations / certify randomness from fewer assumptions etc.?

- **Mathematically beautiful** interplay of group representation theory and convex geometry (orbitopes etc.)

"Rotation boxes": fourfold motivation

- Why all those **sin**es and **cos**ines in the oldfashioned textbooks? What is the theory-independent status of this?



$$P(a,b|\alpha,\beta) = \frac{1}{4}\left[1 + ab\cos 2(\alpha-\beta)\right]$$

- (Very, *very* broadly speaking) **quantum gravity**: Spacetime vs. probabilities in the logical structure of our world?

- **Applications**: Harness the structure of space and time to constrain the correlations / certify randomness from fewer assumptions etc.?

- **Mathematically beautiful** interplay of group representation theory and convex geometry (orbitopes etc.)

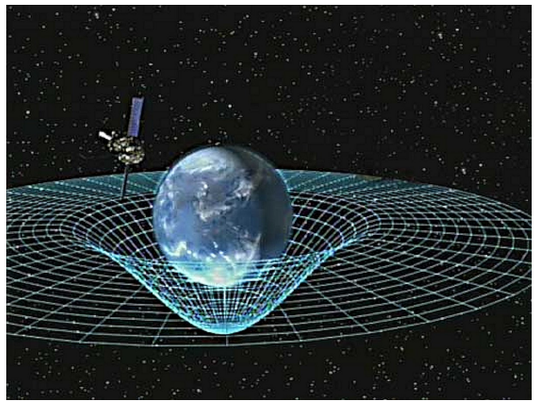
Probability and spacetime

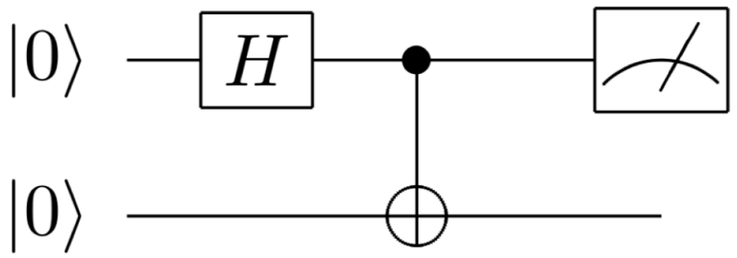
Consider these two distinct aspects of the physical world:

Probability and spacetime

Consider these two distinct aspects of the physical world:

- Spacetime (a theory of **geometry**)
- (Abstract) quantum theory (a theory of **probability**)

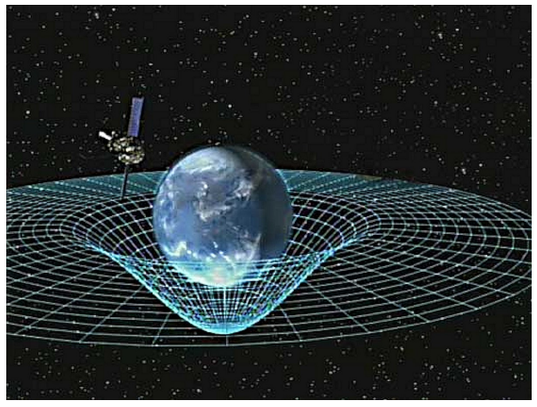


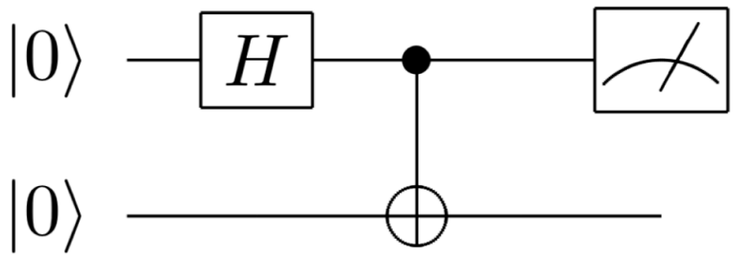


Probability and spacetime

Consider these two distinct aspects of the physical world:

- Spacetime (a theory of **geometry**)
- (Abstract) quantum theory (a theory of **probability**)



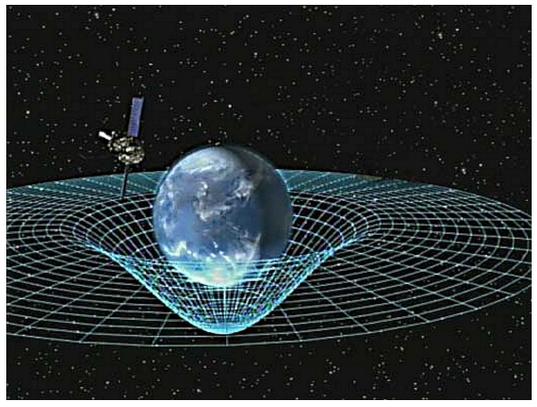


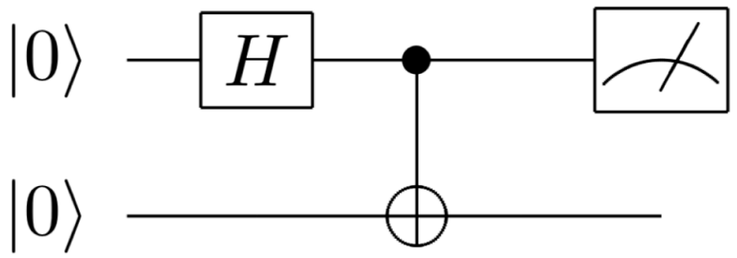
How do they play together / constrain each other / are they unified?

Probability and spacetime

Consider these two distinct aspects of the physical world:

- Spacetime (a theory of **geometry**)
- (Abstract) quantum theory (a theory of **probability**)





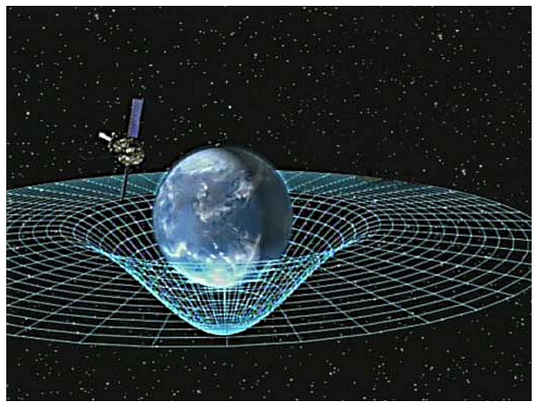
How do they play together / constrain each other / are they unified?

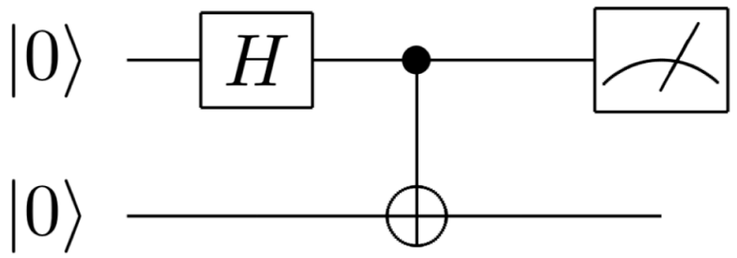
- **Quantum Field Theory:** historical success story of asking this question for special relativity and quantum mechanics.
- **Quantum Gravity:** work in progress of doing this for GR+QM.

Probability and spacetime

Consider these two distinct aspects of the physical world:

- Spacetime (a theory of **geometry**)
- (Abstract) quantum theory (a theory of **probability**)





How do they play together / constrain each other / are they unified?

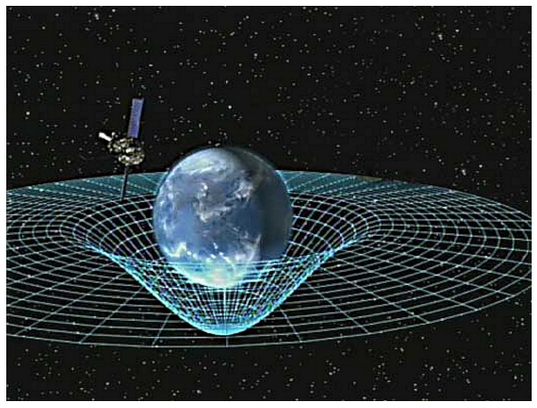
- **Quantum Field Theory:** historical success story of asking this question for special relativity and quantum mechanics.
- **Quantum Gravity:** work in progress of doing this for GR+QM.

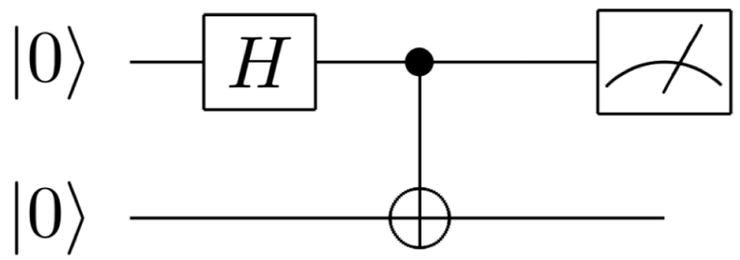
This work: first, simplest steps of asking this for **arbitrary prob. theories.**

Probability and spacetime

Consider these two distinct aspects of the physical world:

- Spacetime (a theory of **geometry**)
- *Some* theory of **probability**.



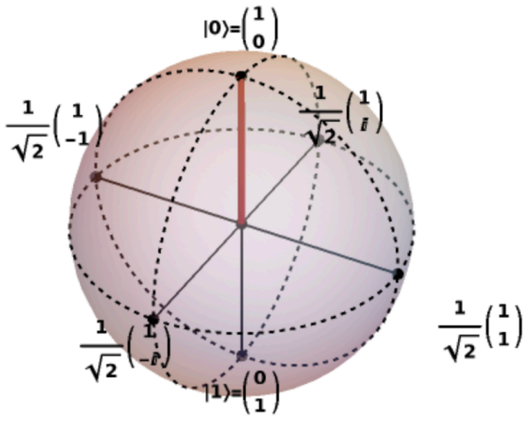


How do they play together / constrain each other / are they unified?

- **Quantum Field Theory:** historical success story of asking this question for special relativity and quantum mechanics.
- **Quantum Gravity:** work in progress of doing this for GR+QM.

This work: first, simplest steps of asking this for **arbitrary prob. theories.**

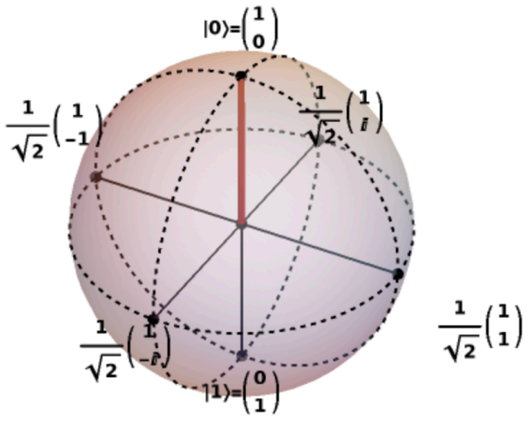
Invitation: the qubit and spatial rotations



Qubit Bloch ball

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$$

Invitation: the qubit and spatial rotations



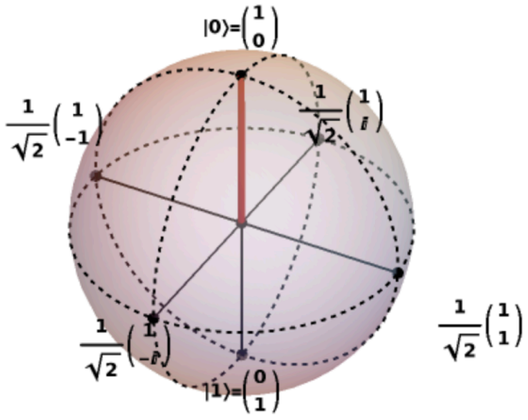
Qubit Bloch ball

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$$

$$\rho = \frac{1}{2}\mathbf{1} + \vec{r}\cdot\vec{\sigma} = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix}$$

$$\mathrm{tr}(\rho) = 1, \quad \rho \geq 0 \Leftrightarrow |\vec{r}| \leq 1.$$

Invitation: the qubit and spatial rotations



Qubit Bloch ball

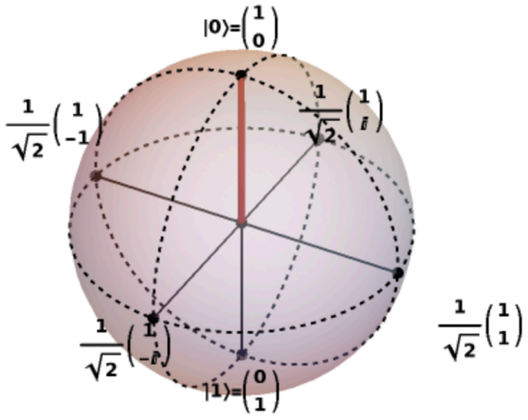
$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$$

$$\rho = \frac{1}{2}\mathbf{1} + \vec{r}\cdot\vec{\sigma} = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix}$$

$$\mathrm{tr}(\rho) = 1, \quad \rho \geq 0 \Leftrightarrow |\vec{r}| \leq 1.$$

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

Invitation: the qubit and spatial rotations



Qubit Bloch ball

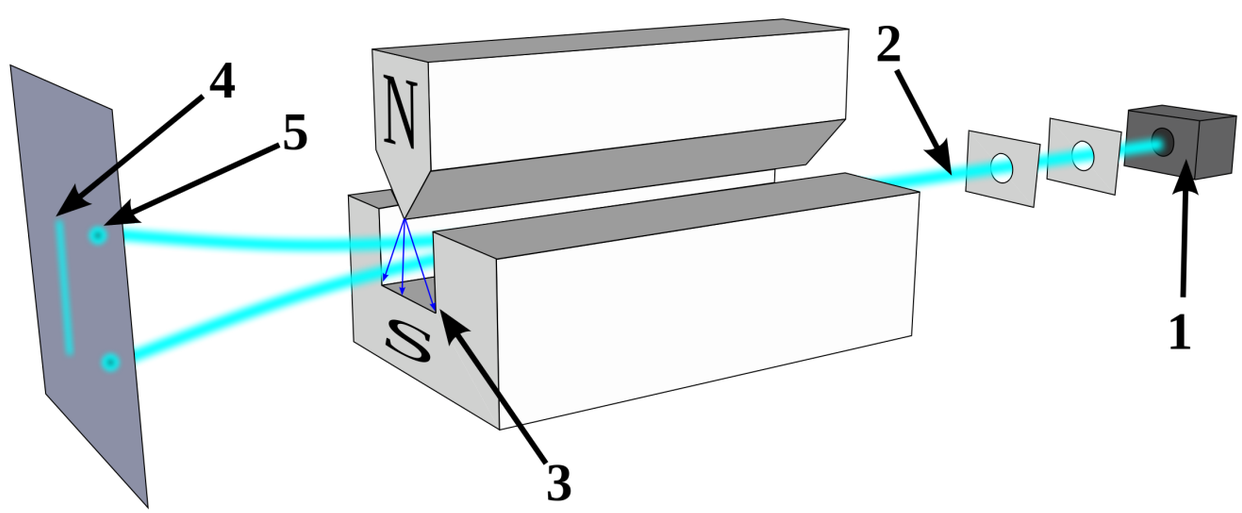
$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$$

$$\rho = \frac{1}{2}\mathbf{1} + \vec{r}\cdot\vec{\sigma} = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix}$$

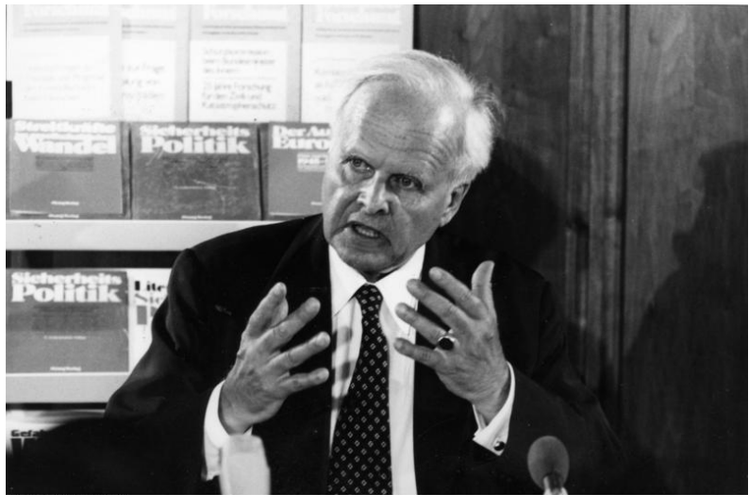
$$\mathrm{tr}(\rho) = 1, \quad \rho \geq 0 \Leftrightarrow |\vec{r}| \leq 1.$$

$$\rho \mapsto U\rho U^\dagger \qquad \vec{r} \mapsto R_U\vec{r}$$

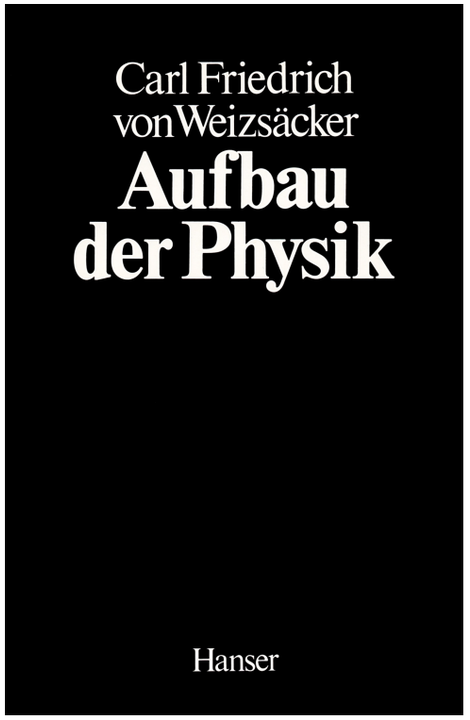
$$\mathrm{PSU}(2) \longleftrightarrow \mathrm{SO}(3)$$



Von Weizsäcker’s theory of ”ur alternatives” (1955-58)



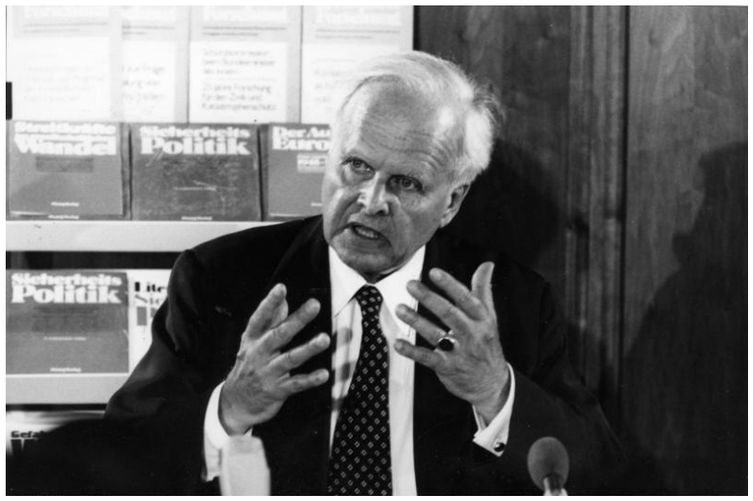
Carl-Friedrich von Weizsäcker
(1912-2007)



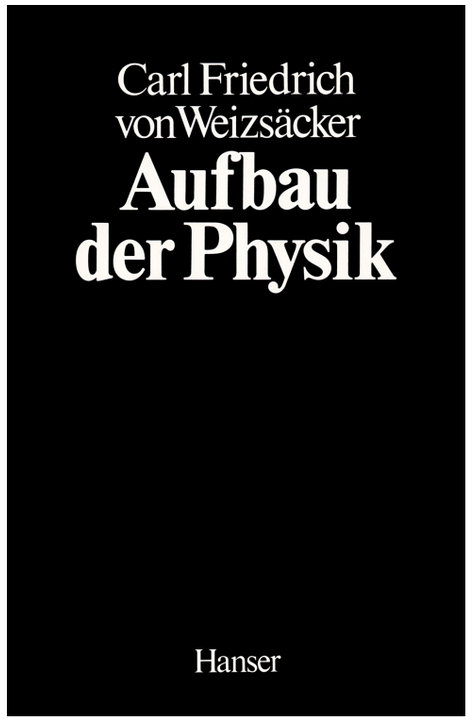


Holger Lyre

Von Weizsäcker's theory of "ur alternatives" (1955-58)



Carl-Friedrich von Weizsäcker
(1912-2007)



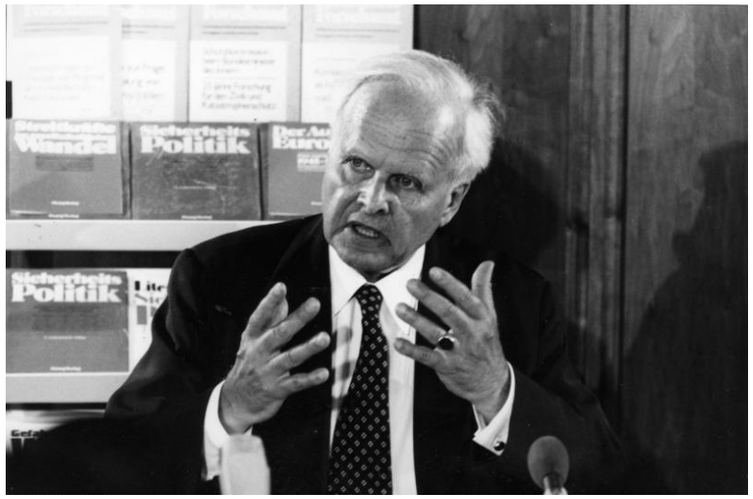


Holger Lyre

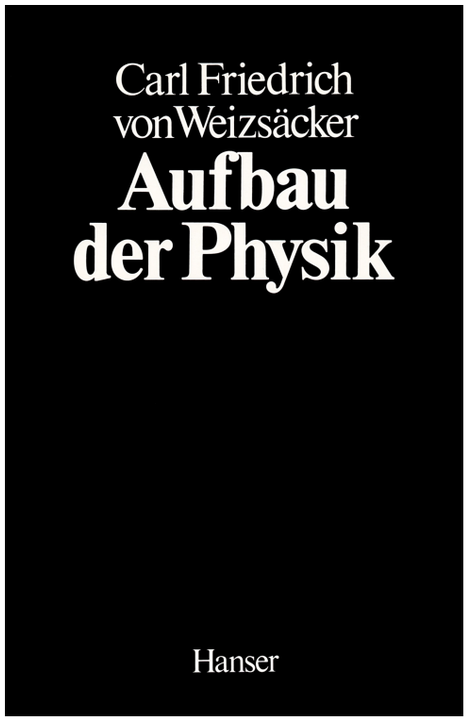
Summary via lyre.de/urinfo.htm (imperfect English translation is mine):

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".

Von Weizsäcker's theory of "ur alternatives" (1955-58)



Carl-Friedrich von Weizsäcker
(1912-2007)





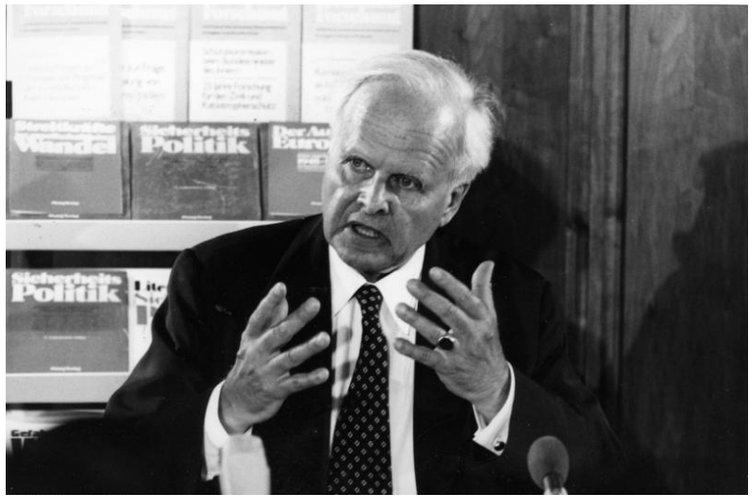
Holger Lyre

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

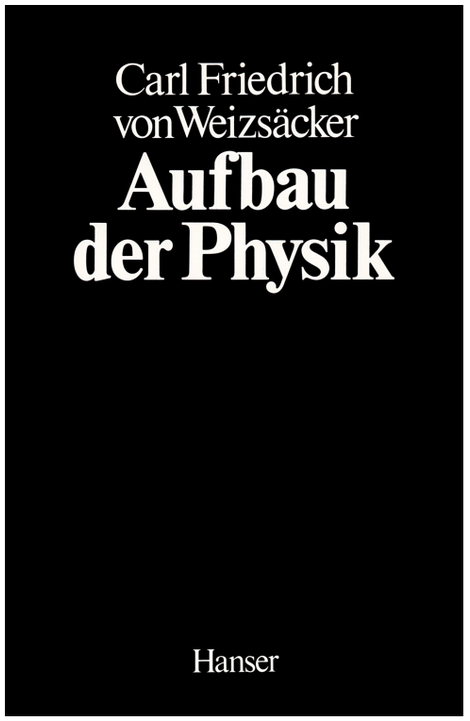
Von Weizsäcker gives the following definition of the central notion of "ur-alternative":
The binary alternative, out of which the state spaces of quantum theory can be built, is called ur-alternative. The subobject associated with an ur-alternative is called "ur".

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.

Von Weizsäcker's theory of "ur alternatives" (1955-58)



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".

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.

Now generally considered unsuccessful: details of approach are ad-hoc and complicated.

Bill Wootters: “statistical distance equals actual distance”



No-cloning theorem, Page-Wootters mechanism…

Bill Wootters: “statistical distance equals actual distance”



No-cloning theorem, Page-Wootters mechanism…

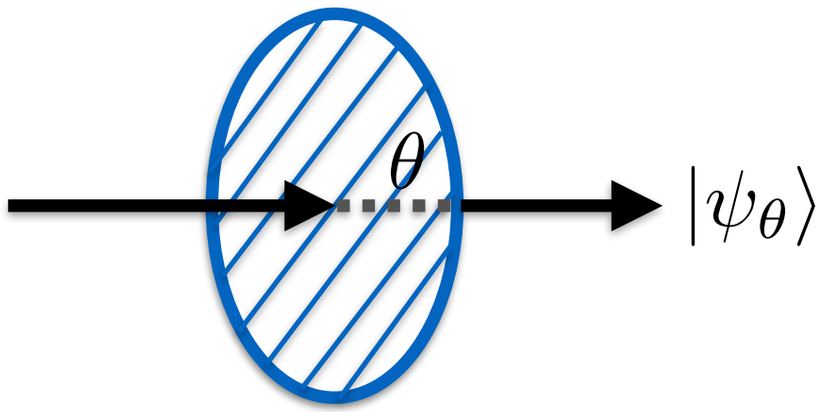
PhD thesis, 1980: “*The Acquisition of Information from Quantum Measurements”.*

Bill Wootters: “statistical distance equals actual distance”



No-cloning theorem, Page-Wootters mechanism…

PhD thesis, 1980: “*The Acquisition of Information from Quantum Measurements”.*



Bill Wootters: “statistical distance equals actual distance”



No-cloning theorem, Page-Wootters mechanism…

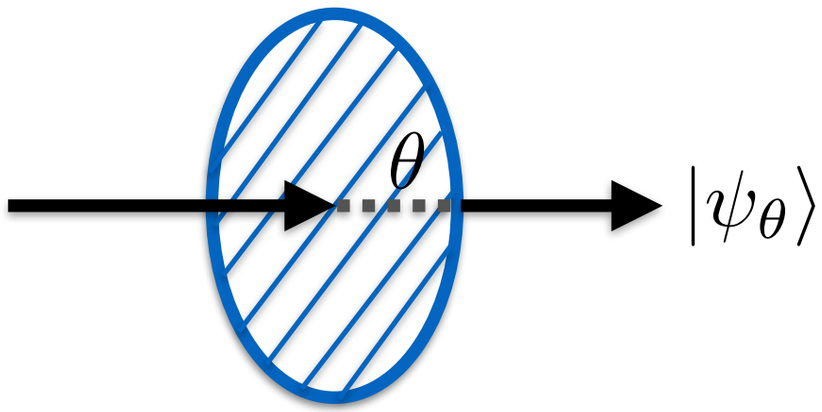
PhD thesis, 1980: “*The Acquisition of Information from Quantum Measurements”.*

Shown **without** assuming QM:

$$\underbrace{d(\psi_\theta, \psi_{\theta'})}_{\text{statistical distance for yes-no measurement}} = c \cdot \underbrace{|\theta - \theta'|}_{\text{“actual” distance of angles}}$$

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

characteristic of spin-*J* particles in QM



Bill Wootters: “statistical distance equals actual distance”



No-cloning theorem, Page-Wootters mechanism…

PhD thesis, 1980: “*The Acquisition of Information from Quantum Measurements”.*

Shown **without** assuming QM:

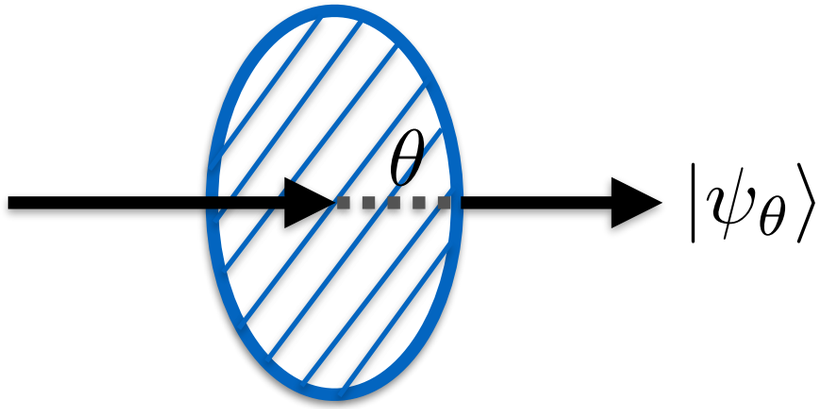
$$d(\psi_\theta, \psi_{\theta'}) = c \cdot |\theta - \theta'|$$

statistical distance for yes-no measurement

“actual” distance of angles

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

characteristic of spin-*J* particles in QM



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

Bill Wootters: “statistical distance equals actual distance”



No-cloning theorem, Page-Wootters mechanism…

PhD thesis, 1980: “*The Acquisition of Information from Quantum Measurements”.*

Shown **without** assuming QM:

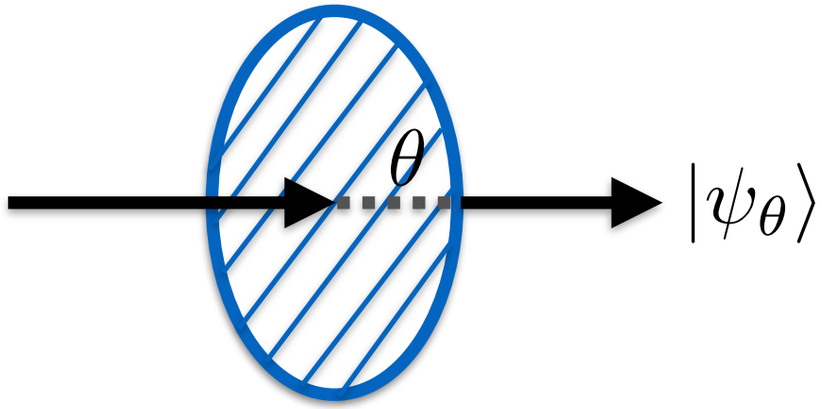
$$d(\psi_\theta, \psi_{\theta'}) = c \cdot |\theta - \theta'|$$

statistical distance for yes-no measurement

“actual” distance of angles

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

characteristic of spin-*J* particles in QM



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

Is this statistical-spatial correspondence characteristic of quantum theory?

Overview

1. Motivation (and some history)

2. “Rotation boxes” within and beyond QT

3. A metrological game and the (sub)optimality of QT

4. A theory-independent SDI randomness generator

5. Conclusions

Overview

1. Motivation (and some history)

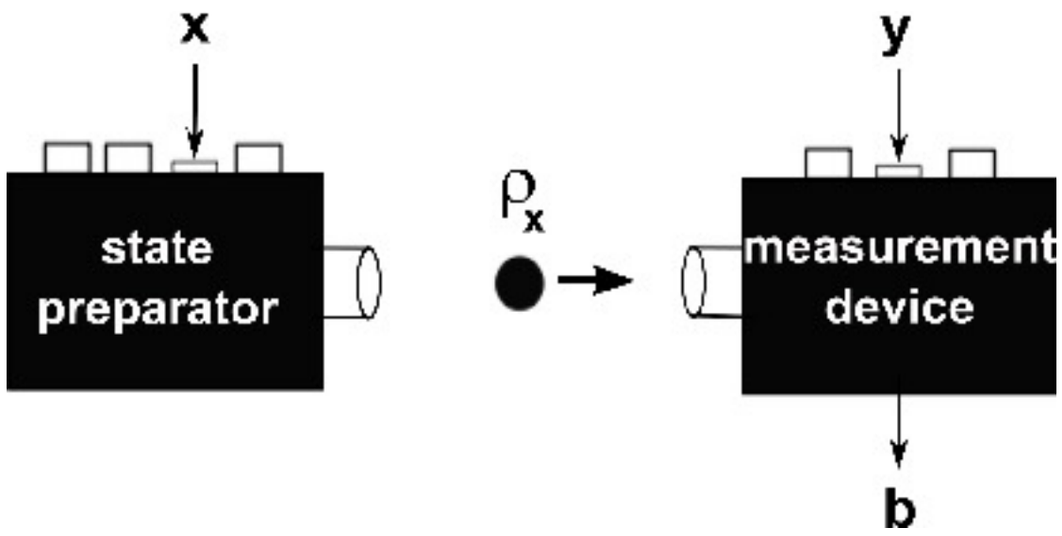
2. “Rotation boxes” within and beyond QT

3. A metrological game and the (sub)optimality of QT

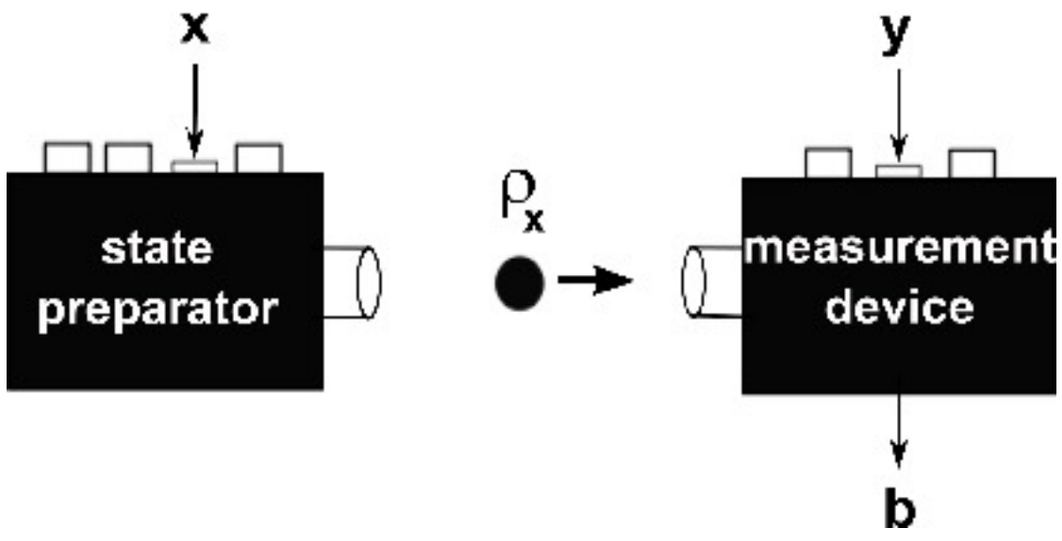
4. A theory-independent SDI randomness generator

5. Conclusions

What is a “prepare-and-measure scenario”?

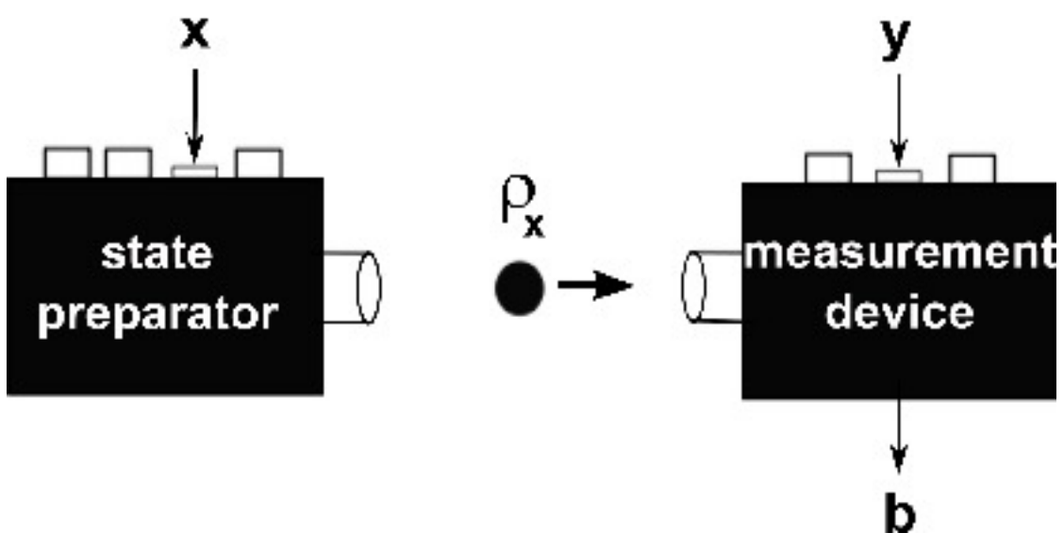


What is a “prepare-and-measure scenario”?



On input *x*, the preparation device prepares some physical system in some associated state.
The measurement device performs some measurement *y* and yields some outcome *b*.

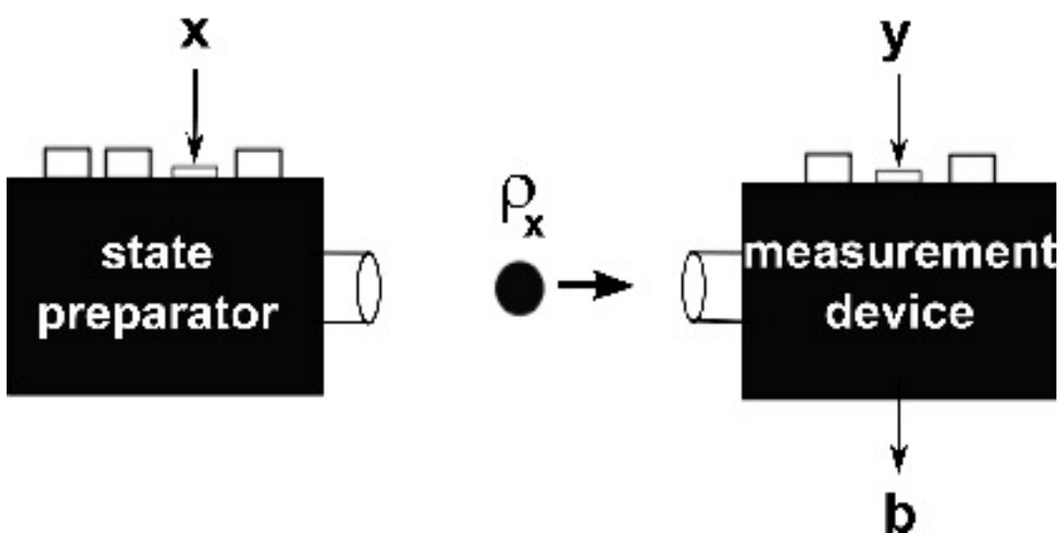
What is a “prepare-and-measure scenario”?



On input *x*, the preparation device prepares some physical system in some associated state.
The measurement device performs some measurement *y* and yields some outcome *b*.

Observed statistics: $\mathrm{Prob}(b|x,y).$

What is a “prepare-and-measure scenario”?

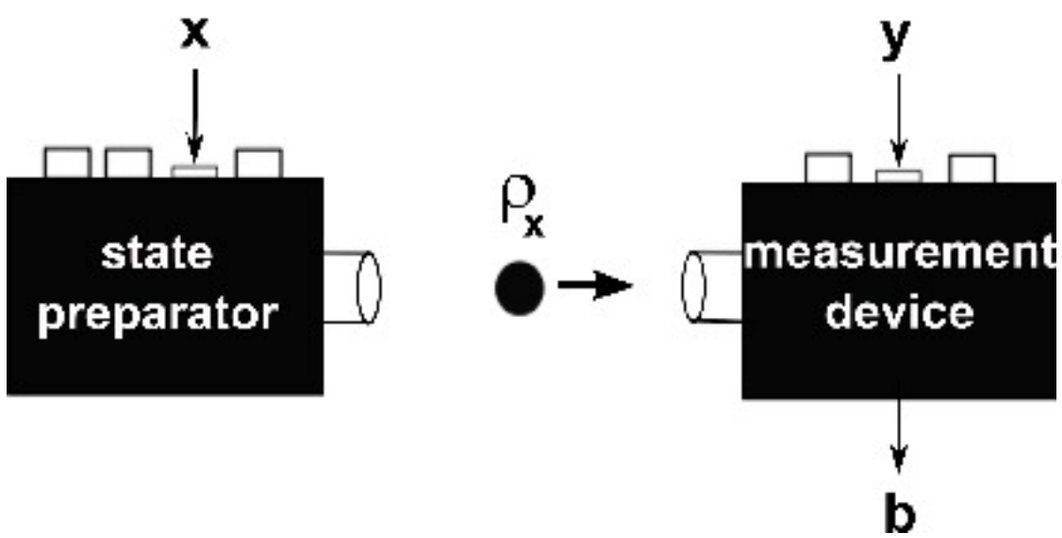


On input *x*, the preparation device prepares some physical system in some associated state.
The measurement device performs some measurement *y* and yields some outcome *b*.

Observed statistics: $\mathrm{Prob}(b|x,y).$

Often a goal: make only **minimal assumptions** (e.g. P, M devices **untrusted**; moderate assumptions on the transmitted physical system).
For example, for the generation of secure random numbers.

What is a “prepare-and-measure scenario”?



On input *x*, the preparation device prepares some physical system in some associated state.
The measurement device performs some measurement *y* and yields some outcome *b*.

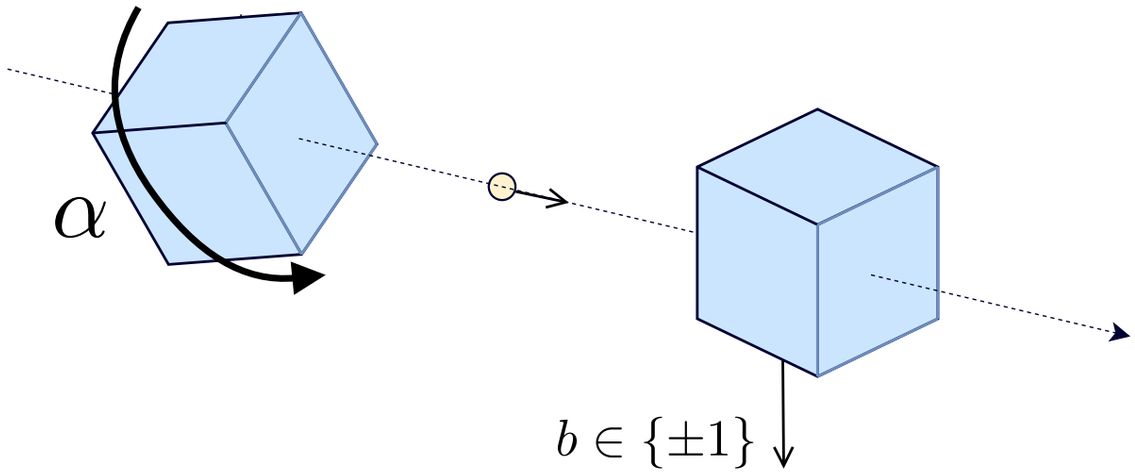
Observed statistics: $\mathrm{Prob}(b|x,y).$

Often a goal: make only **minimal assumptions** (e.g. P, M devices **untrusted**; moderate assumptions on the transmitted physical system).
For example, for the generation of secure random numbers.

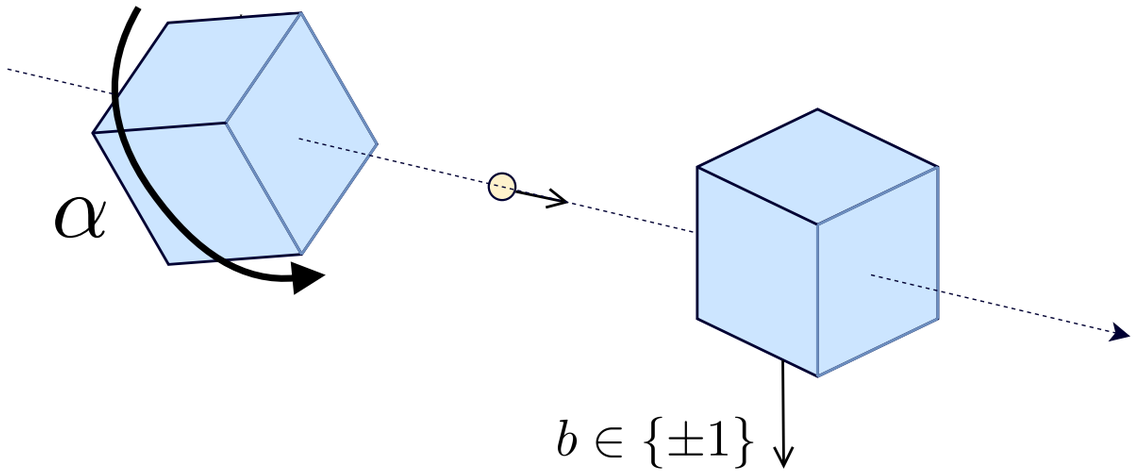
Let us assume quantum theory. Then there exists a complex Hilbert space $\mathcal{H}$ (in this talk finite-dim.), positive-semidefinite unit trace operators ρ_x and psd. measurement operators $M_y^{(b)}$ with $\sum_b M_y^{(b)} = \mathbf{1}$ such that

$$\mathrm{Prob}(b|x,y) = \mathrm{tr}(\rho_x M_y^{(b)}).$$

Quantum SO(2) prepare-and-measure



Quantum SO(2) prepare-and-measure

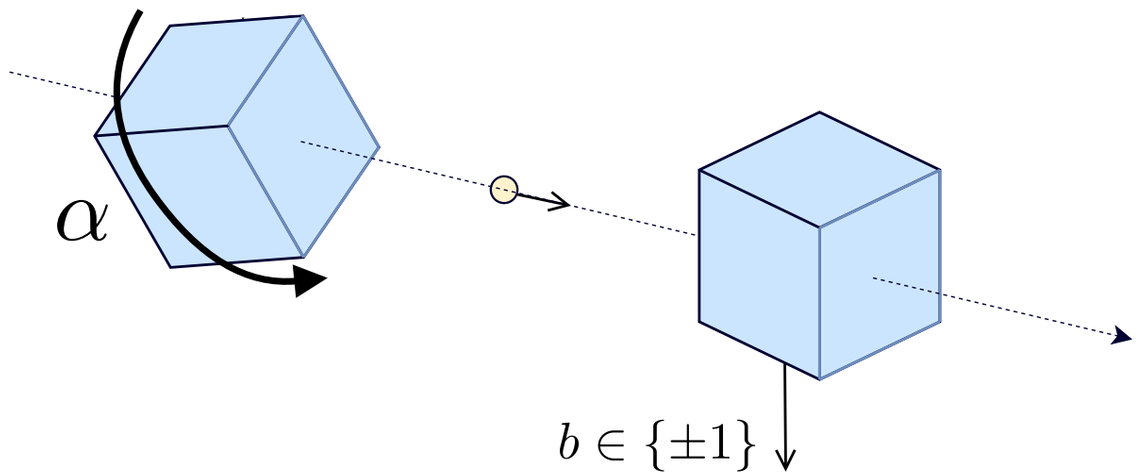


Observed statistics:

$$\mathrm{Prob}(b|\alpha)$$

$$\mathrm{Prob}(+1|\alpha) + \mathrm{Prob}(-1|\alpha) = 1.$$

Quantum SO(2) prepare-and-measure



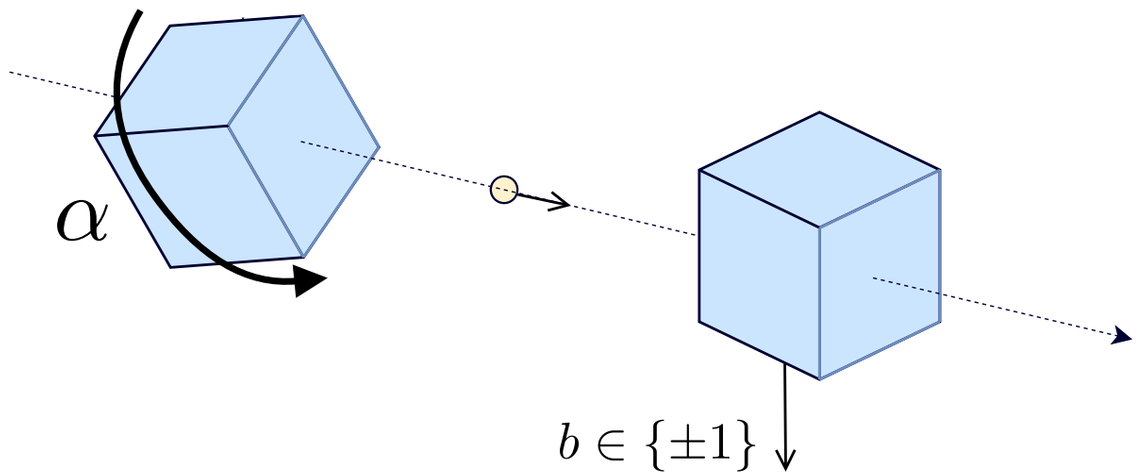
Observed statistics:

$$\mathrm{Prob}(b|\alpha)$$

$$\mathrm{Prob}(+1|\alpha) + \mathrm{Prob}(-1|\alpha) = 1.$$

Let state ρ be what is prepared without any rotation.

Quantum SO(2) prepare-and-measure



Observed statistics:

$$\mathrm{Prob}(b|\alpha)$$

$$\mathrm{Prob}(+1|\alpha) + \mathrm{Prob}(-1|\alpha) = 1.$$

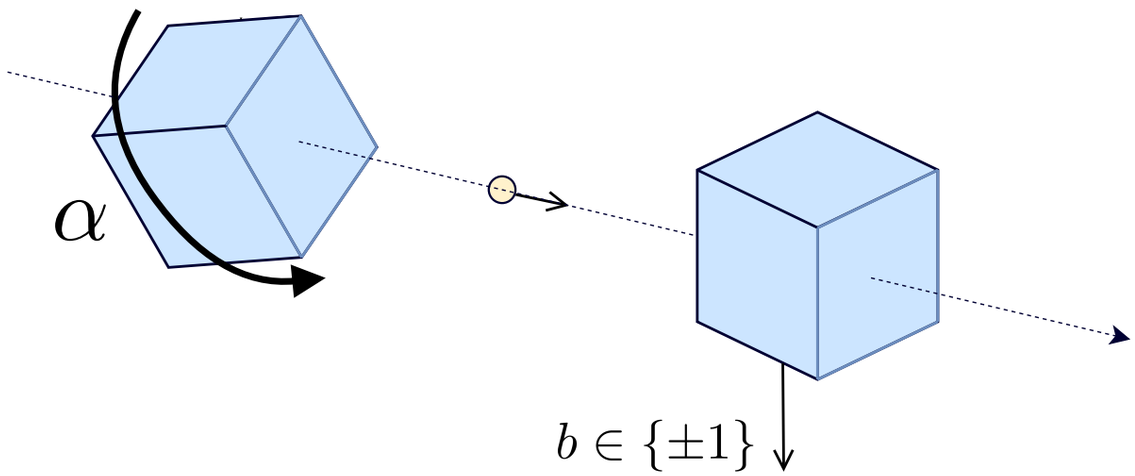
Let state ρ be what is prepared without any rotation.

What do rotations do to that state? Standard textbook arguments (via rotational covariance) imply that there is a continuous homomorphism

$$\mathrm{SO}(2) \to \mathrm{PU}(\mathcal{H}), \quad \alpha \mapsto U_\alpha$$

such that $\rho_\alpha := U_\alpha \rho U_\alpha^\dagger$ is prepared upon rotation by angle α.

Quantum SO(2) prepare-and-measure



Observed statistics:

$$\mathrm{Prob}(b|\alpha)$$

$$\mathrm{Prob}(+1|\alpha) + \mathrm{Prob}(-1|\alpha) = 1.$$

Let state ρ be what is prepared without any rotation.

What do rotations do to that state? Standard textbook arguments (via rotational covariance) imply that there is a continuous homomorphism

$$\mathrm{SO}(2) \to \mathrm{PU}(\mathcal{H}), \quad \alpha \mapsto U_\alpha$$

such that $\rho_\alpha := U_\alpha \rho U_\alpha^\dagger$ is prepared upon rotation by angle α.

If the Hilbert space $\mathcal{H}$ is finite-dimensional, this always has the form

$$U_\alpha = \bigoplus_{j=-J}^{J} \mathbb{I}_{n_j} e^{ij\alpha}$$

for some $J \in \{0, \frac{1}{2}, 1, \frac{3}{2}, 2, \ldots\}$.

Quantum spin-J boxes $\mathcal{Q}_J$

Quantum spin-J boxes $\mathcal{Q}_J$

Definition. The quantum spin-J correlations $\mathcal{Q}_J$ are the set of functions

$$P(+1|\alpha) = \mathrm{tr}(U_\alpha \rho U_\alpha^\dagger E),$$

where ρ is some quantum state, E some POVM element, and U_α is a projective representation of SO(2) of the form above.

Quantum spin-J boxes $\mathcal{Q}_J$

Definition. The quantum spin-J correlations $\mathcal{Q}_J$ are the set of functions

$$P(+1|\alpha) = \mathrm{tr}(U_\alpha \rho U_\alpha^\dagger E),$$

where ρ is some quantum state, E some POVM element, and U_α is a projective representation of SO(2) of the form above.

Via purification, one can show that every $\mathcal{Q}_J$ is a **convex** set.

Moreover, the Hilbert space can always be fixed as follows:

Quantum spin-J boxes $\mathcal{Q}_J$

Definition. The quantum spin-J correlations $\mathcal{Q}_J$ are the set of functions

$$P(+1|\alpha) = \mathrm{tr}(U_\alpha \rho U_\alpha^\dagger E),$$

where ρ is some quantum state, E some POVM element, and U_α is a projective representation of SO(2) of the form above.

Via purification, one can show that every $\mathcal{Q}_J$ is a **convex** set.

Moreover, the Hilbert space can always be fixed as follows:

Lemma. For every $P \in \mathcal{Q}_J$, there is a pure state $|\psi\rangle \in \mathbb{C}^{2J+1}$ and a POVM $\{E_b\}_{b\in\{+1,-1\}}$ such that $P(b|\alpha) = \langle\psi|U_\alpha^\dagger E_b U_\alpha|\psi\rangle$, where $U_\alpha := \exp(i\alpha Z)$, Z = $\mathrm{diag}(J, J-1, \ldots, -J)$.

Quantum spin-J boxes $\mathcal{Q}_J$

Definition. The quantum spin-J correlations $\mathcal{Q}_J$ are the set of functions

$$P(+1|\alpha) = \mathrm{tr}(U_\alpha \rho U_\alpha^\dagger E),$$

where ρ is some quantum state, E some POVM element, and U_α is a projective representation of SO(2) of the form above.

Via purification, one can show that every $\mathcal{Q}_J$ is a **convex** set.

Moreover, the Hilbert space can always be fixed as follows:

Lemma. For every $P \in \mathcal{Q}_J$, there is a pure state $|\psi\rangle \in \mathbb{C}^{2J+1}$ and a POVM $\{E_b\}_{b\in\{+1,-1\}}$ such that $P(b|\alpha) = \langle\psi|U_\alpha^\dagger E_b U_\alpha|\psi\rangle$, where $U_\alpha := \exp(i\alpha Z)$, Z = $\mathrm{diag}(J, J-1, \ldots, -J)$.

In particular, every $\mathcal{Q}_J$ is **compact**, and multiplying out the above shows that every function in $\mathcal{Q}_J$ is a trigonometric polynomial of degree $\leq 2J$.

Single-photon example

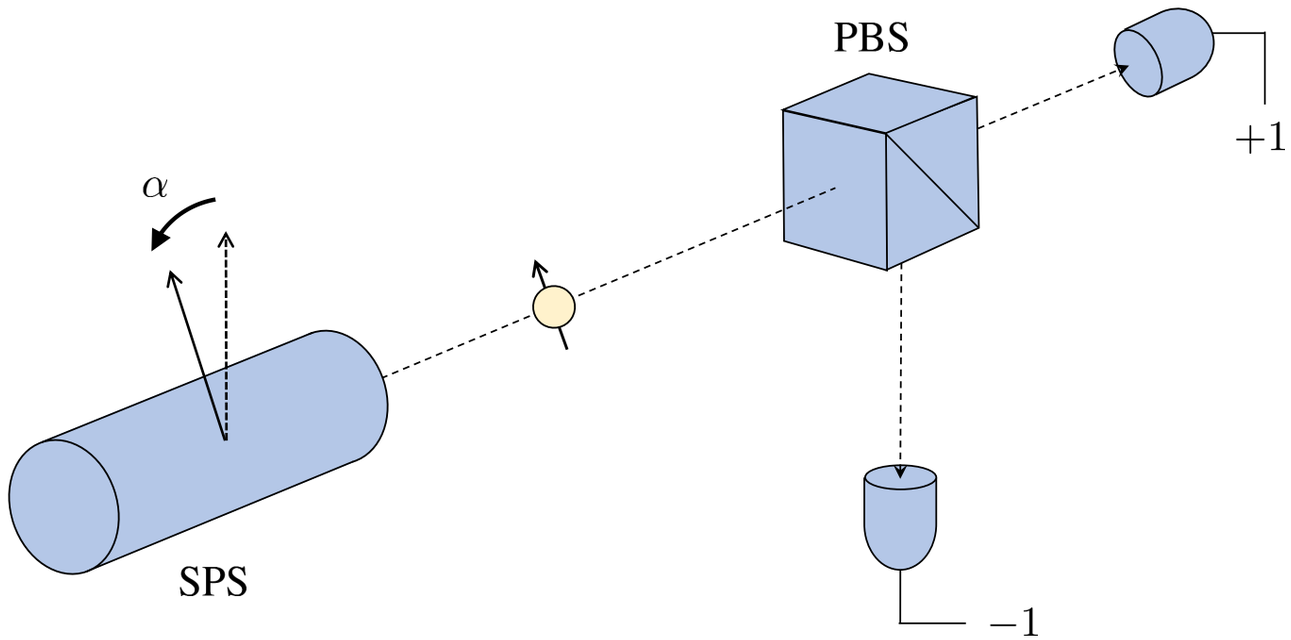


Figure 2: Illustration of a possible way to implement our prepare-and-measure scenario. The preparation consists of a single-photon source (SPS) which is rotated at angles 0 and α for inputs $x = 1$ and $x = 2$ respectively. This leaves the photon unchanged or rotates its polarization by α. The photon is then measured by a polarizing beam splitter (PBS) with two single-photon detectors corresponding to the binary outcomes $b \in \{+1, -1\}$. This setup realizes the $J = 1$ case of our framework, where the mechanical rotation implements the unitary $U_\alpha = \mathrm{diag}(e^{i\alpha}, e^{-i\alpha})$ to rotate the photon polarization.

Single-photon example

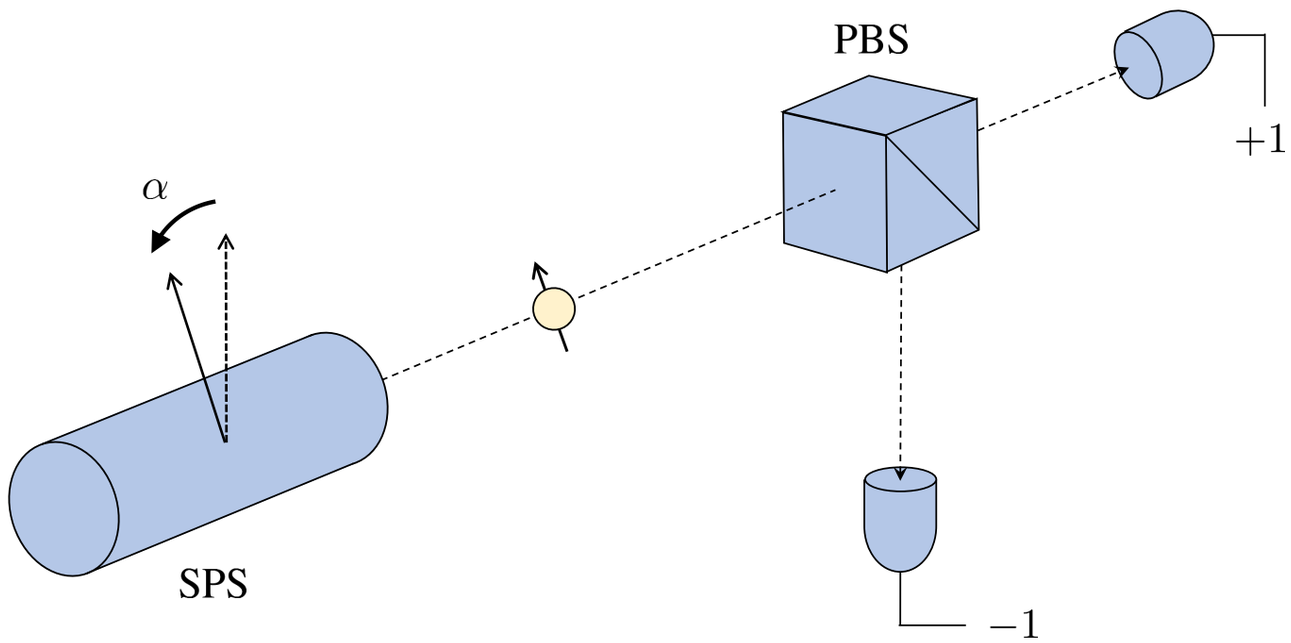


Figure 2: Illustration of a possible way to implement our prepare-and-measure scenario. The preparation consists of a single-photon source (SPS) which is rotated at angles 0 and α for inputs $x = 1$ and $x = 2$ respectively. This leaves the photon unchanged or rotates its polarization by α. The photon is then measured by a polarizing beam splitter (PBS) with two single-photon detectors corresponding to the binary outcomes $b \in \{+1, -1\}$. This setup realizes the $J = 1$ case of our framework, where the mechanical rotation implements the unitary $U_\alpha = \mathrm{diag}(e^{i\alpha}, e^{-i\alpha})$ to rotate the photon polarization.

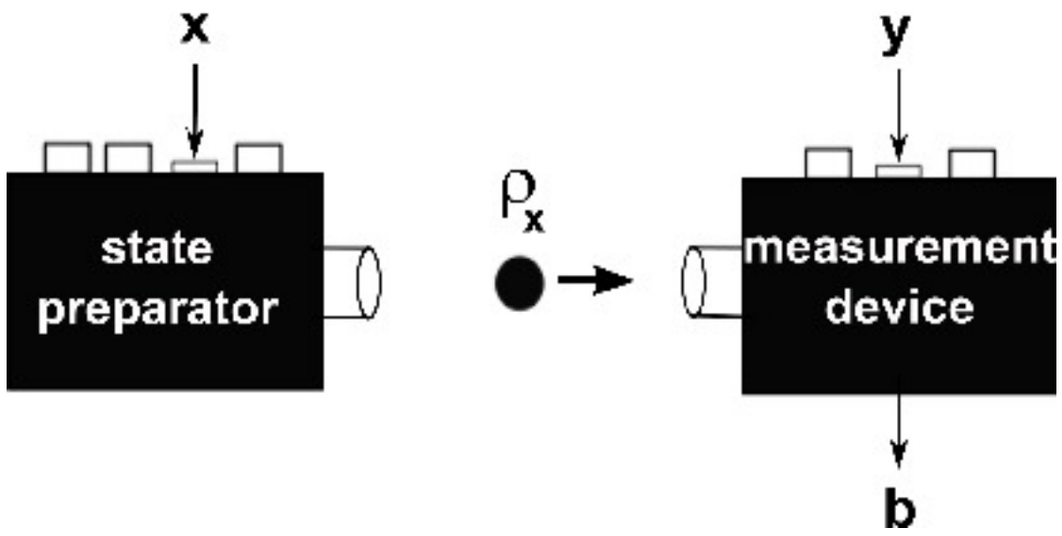
Photons are spin-1 particles.

Consistent with the previous slide, we have

$$P(+1|\alpha) = \frac{1}{2}\left(1 + \cos(2(\theta_0 + \alpha))\right)$$

(trig. polynomial of deg. $2J$)

Prepare-and-measure **in generalized prob. theories**

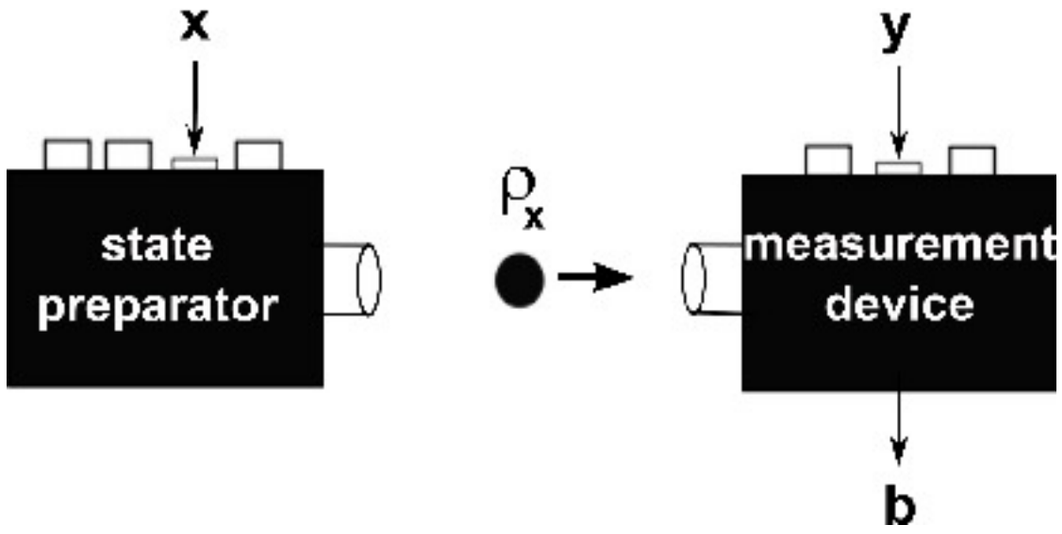


Quantum:

$$\mathrm{Prob}(b|x,y) = \mathrm{tr}(\rho_x M_y^{(b)}).$$

Quantum system

Prepare-and-measure **in generalized prob. theories**

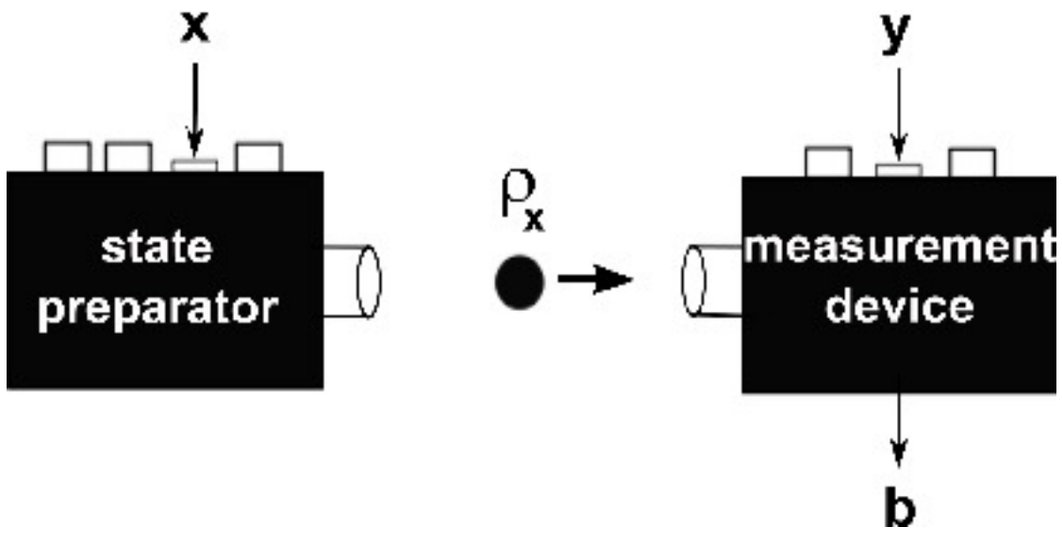


Quantum:

$$\mathrm{Prob}(b|x,y) = \mathrm{tr}(\rho_x M_y^{(b)}).$$
$$= (e_y^{(b)}, \omega_x)$$

Quantum system A **GPT system**

Prepare-and-measure **in generalized prob. theories**



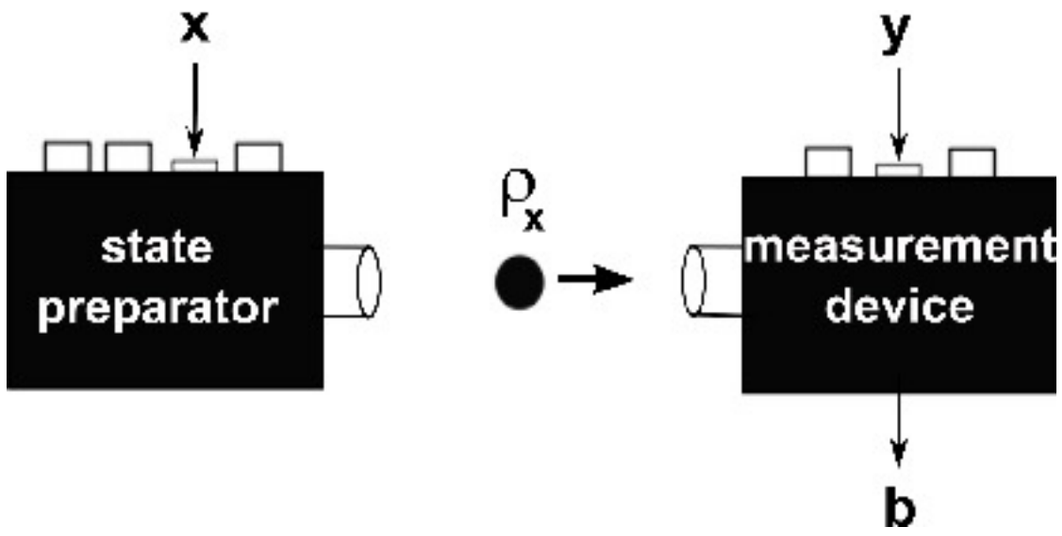
Quantum:

$$\mathrm{Prob}(b|x,y) = \mathrm{tr}(\rho_x M_y^{(b)}).$$
$$= (e_y^{(b)}, \omega_x)$$

Quantum system A **GPT system** is defined by:

- a finite-dimensional real vector space V_A;
- a closed convex cone ("unnormalized states") $A_+ \subset V_A$ that spans V_A;
- a "unit functional" $u_A \in V_A^*$ with $(u_A, \omega) > 0$ for all $\omega \in A_+ \setminus \{0\}$.

Prepare-and-measure **in generalized prob. theories**



Quantum:

$$\mathrm{Prob}(b|x,y) = \mathrm{tr}(\rho_x M_y^{(b)}).$$
$$= (e_y^{(b)}, \omega_x)$$

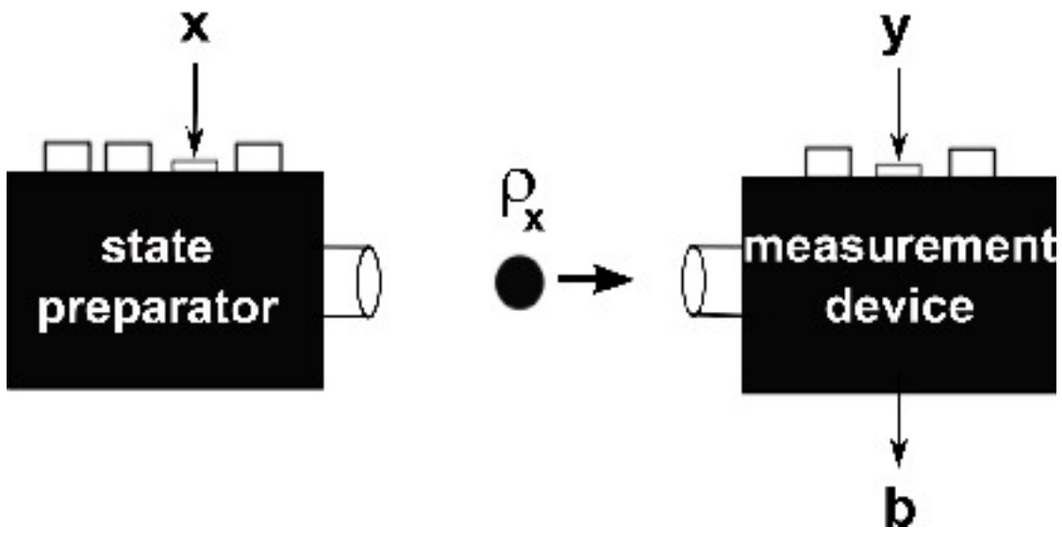
Quantum system A **GPT system** is defined by:

- a finite-dimensional real vector space V_A;
- a closed convex cone ("unnormalized states") $A_+ \subset V_A$ that spans V_A;
- a "unit functional" $u_A \in V_A^*$ with $(u_A, \omega) > 0$ for all $\omega \in A_+ \setminus \{0\}$.

The normalized states ω are the elements of

$$\Omega_A := \{\omega \in A_+ \mid u_A(\omega) = 1\},$$

Prepare-and-measure **in generalized prob. theories**



Quantum:

$$\mathrm{Prob}(b|x,y) = \mathrm{tr}(\rho_x M_y^{(b)}).$$
$$= (e_y^{(b)}, \omega_x)$$

Quantum system A **GPT system** is defined by:

- a finite-dimensional real vector space V_A;
- a closed convex cone ("unnormalized states") $A_+ \subset V_A$ that spans V_A;
- a "unit functional" $u_A \in V_A^*$ with $(u_A, \omega) > 0$ for all $\omega \in A_+ \setminus \{0\}$.

The normalized states ω are the elements of

$$\Omega_A := \{\omega \in A_+ \mid u_A(\omega) = 1\},$$

and measurement outcomes are characterized by **effects** e, elements of

$$A_+^* = \{e \in V_A^* \mid (e,\omega) \geq 0 \text{ for all } \omega \in A_+\}.$$

Examples of GPT systems

Classical n-level systems A:

Examples of GPT systems

Classical n-level systems A:

$$V_A = \mathbb{R}^n, \quad A_+ = \{(p_1, \ldots, p_n) \mid \text{all } p_i \geq 0\} = A_+^*,$$

Examples of GPT systems

Classical n-level systems A:

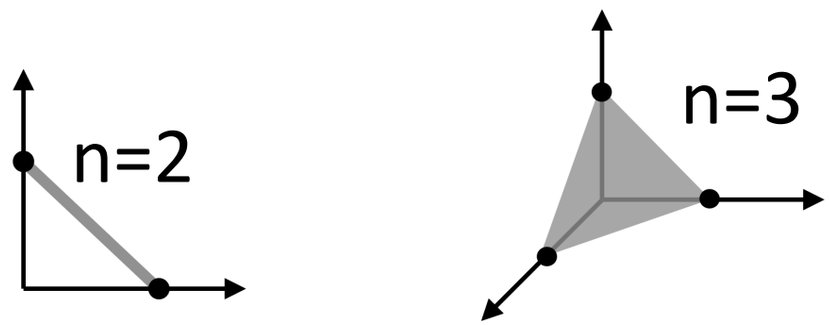
$$V_A = \mathbb{R}^n, \quad A_+ = \{(p_1, \ldots, p_n) \mid \text{all } p_i \geq 0\} = A_+^*,$$
$$u_A(p) = \sum_{k=1}^n p_k, \quad \Omega_A = \{(p_1, \ldots, p_n) \mid p_i \geq 0, \sum_k p_k = 1\}.$$

Examples of GPT systems

Classical n-level systems A:

$$V_A = \mathbb{R}^n, \quad A_+ = \{(p_1, \ldots, p_n) \mid \text{all } p_i \geq 0\} = A_+^*,$$
$$u_A(p) = \sum_{k=1}^n p_k, \quad \Omega_A = \{(p_1, \ldots, p_n) \mid p_i \geq 0, \sum_k p_k = 1\}.$$

States are discrete probability distributions, state spaces are **simplices**.

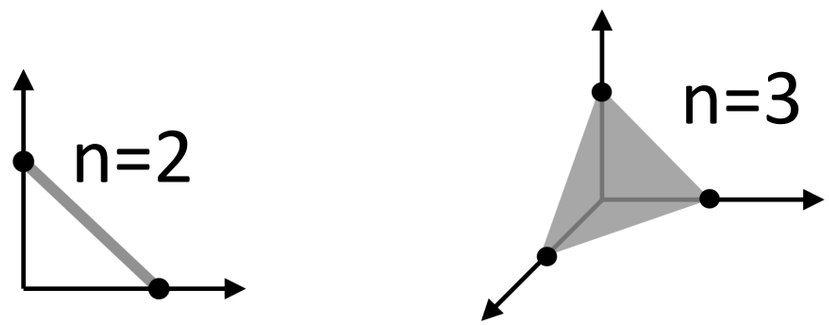


Examples of GPT systems

Classical n-level systems A:

$$V_A = \mathbb{R}^n, \quad A_+ = \{(p_1, \ldots, p_n) \mid \text{all } p_i \geq 0\} = A_+^*,$$
$$u_A(p) = \sum_{k=1}^n p_k, \quad \Omega_A = \{(p_1, \ldots, p_n) \mid p_i \geq 0, \sum_k p_k = 1\}.$$

States are discrete probability distributions, state spaces are **simplices**.



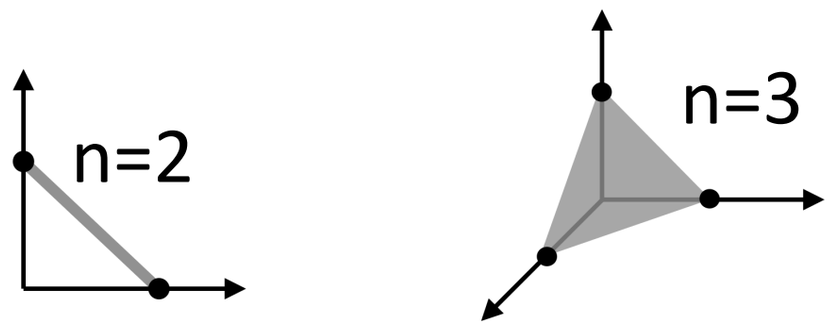
Quantum n-level systems B:

Examples of GPT systems

Classical n-level systems A:

$$V_A = \mathbb{R}^n, \quad A_+ = \{(p_1, \ldots, p_n) \mid \text{all } p_i \geq 0\} = A_+^*,$$
$$u_A(p) = \sum_{k=1}^n p_k, \quad \Omega_A = \{(p_1, \ldots, p_n) \mid p_i \geq 0, \sum_k p_k = 1\}.$$

States are discrete probability distributions, state spaces are **simplices**.



Quantum n-level systems B:

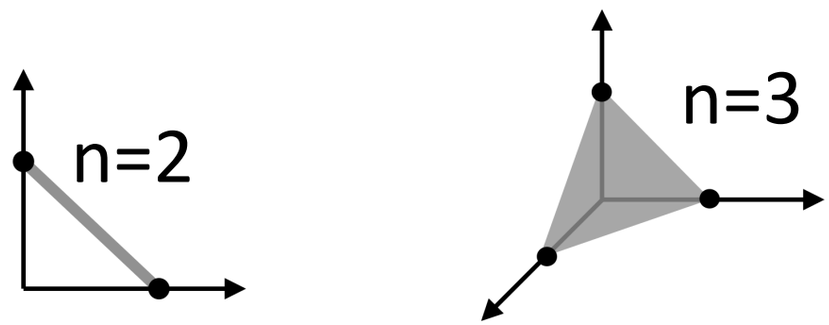
$V_B = \{M \in \mathcal{L}(\mathbb{C}^n) \mid M = M^\dagger\}$ (self-adjoint matrices)

Examples of GPT systems

Classical n-level systems A:

$$V_A = \mathbb{R}^n, \quad A_+ = \{(p_1, \ldots, p_n) \mid \text{all } p_i \geq 0\} = A_+^*,$$
$$u_A(p) = \sum_{k=1}^n p_k, \quad \Omega_A = \{(p_1, \ldots, p_n) \mid p_i \geq 0, \sum_k p_k = 1\}.$$

States are discrete probability distributions, state spaces are **simplices**.



Quantum n-level systems B:

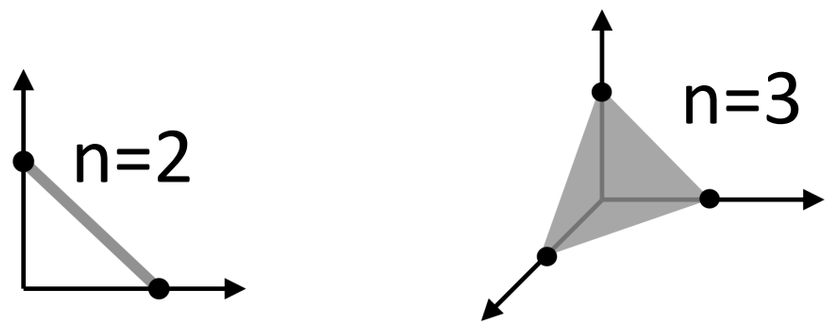
$$V_B = \{M \in \mathcal{L}(\mathbb{C}^n) \mid M = M^\dagger\} \quad \text{(self-adjoint matrices)}$$
$$B_+ = \{M \mid M \geq 0\} = B_+^* \quad \text{(positive semi-definite cone)}$$

Examples of GPT systems

Classical n-level systems A:

$$V_A = \mathbb{R}^n, \quad A_+ = \{(p_1, \ldots, p_n) \mid \text{all } p_i \geq 0\} = A_+^*,$$
$$u_A(p) = \sum_{k=1}^n p_k, \quad \Omega_A = \{(p_1, \ldots, p_n) \mid p_i \geq 0, \sum_k p_k = 1\}.$$

States are discrete probability distributions, state spaces are **simplices**.



Quantum n-level systems B:

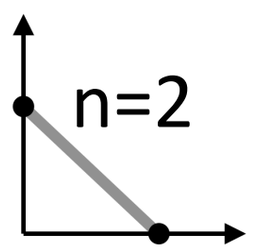
$$V_B = \{M \in \mathcal{L}(\mathbb{C}^n) \mid M = M^\dagger\} \quad \text{(self-adjoint matrices)}$$
$$B_+ = \{M \mid M \geq 0\} = B_+^* \quad \text{(positive semi-definite cone)}$$
$$u_B(M) = \mathrm{tr}(M), \quad \Omega_B = \{\rho \mid \rho \geq 0, \mathrm{tr}(\rho) = 1\} \quad \text{(density matrices)}$$

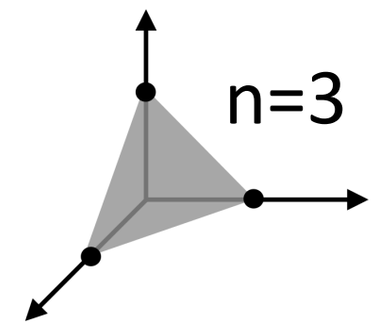
Examples of GPT systems

Classical n-level systems A:

$$V_A = \mathbb{R}^n, \quad A_+ = \{(p_1, \ldots, p_n) \mid \text{all } p_i \geq 0\} = A_+^*,$$
$$u_A(p) = \sum_{k=1}^n p_k, \quad \Omega_A = \{(p_1, \ldots, p_n) \mid p_i \geq 0, \sum_k p_k = 1\}.$$

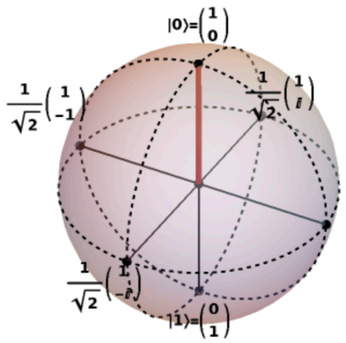
States are discrete probability distributions, state spaces are **simplices**.





Quantum n-level systems B:

$$V_B = \{M \in \mathcal{L}(\mathbb{C}^n) \mid M = M^\dagger\} \quad \text{(self-adjoint matrices)}$$
$$B_+ = \{M \mid M \geq 0\} = B_+^* \quad \text{(positive semi-definite cone)}$$
$$u_B(M) = \mathrm{tr}(M), \quad \Omega_B = \{\rho \mid \rho \geq 0, \mathrm{tr}(\rho) = 1\} \quad \text{(density matrices)}$$



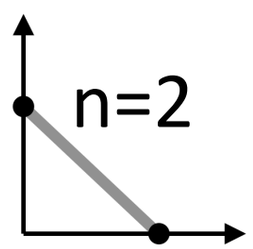
n=2

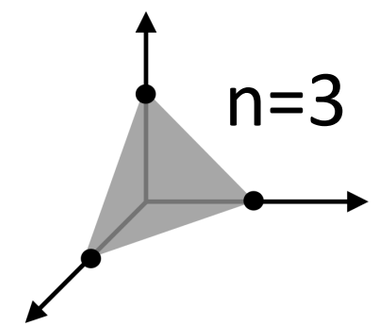
Examples of GPT systems

Classical n-level systems A:

$$V_A = \mathbb{R}^n, \quad A_+ = \{(p_1, \ldots, p_n) \mid \text{all } p_i \geq 0\} = A_+^*,$$
$$u_A(p) = \sum_{k=1}^n p_k, \quad \Omega_A = \{(p_1, \ldots, p_n) \mid p_i \geq 0, \sum_k p_k = 1\}.$$

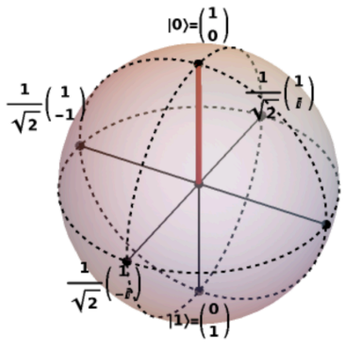
States are discrete probability distributions, state spaces are **simplices**.





Quantum n-level systems B:

$$V_B = \{M \in \mathcal{L}(\mathbb{C}^n) \mid M = M^\dagger\} \quad \text{(self-adjoint matrices)}$$
$$B_+ = \{M \mid M \geq 0\} = B_+^* \quad \text{(positive semi-definite cone)}$$
$$u_B(M) = \mathrm{tr}(M), \quad \Omega_B = \{\rho \mid \rho \geq 0, \mathrm{tr}(\rho) = 1\} \quad \text{(density matrices)}$$

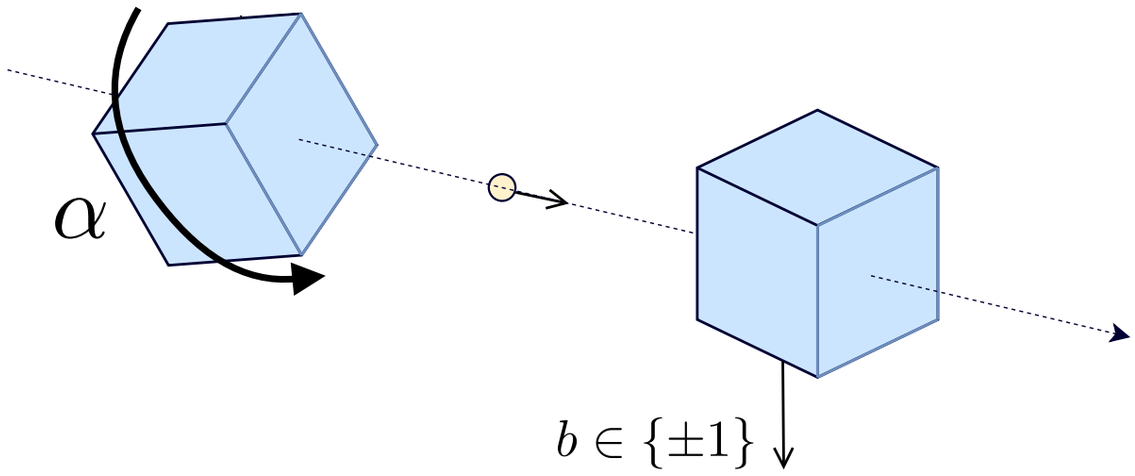


n=2

For larger n, these are (sort of complicated) **spectrahedra**.

Generalized SO(2) prepare-and-measure

Generalized SO(2) prepare-and-measure

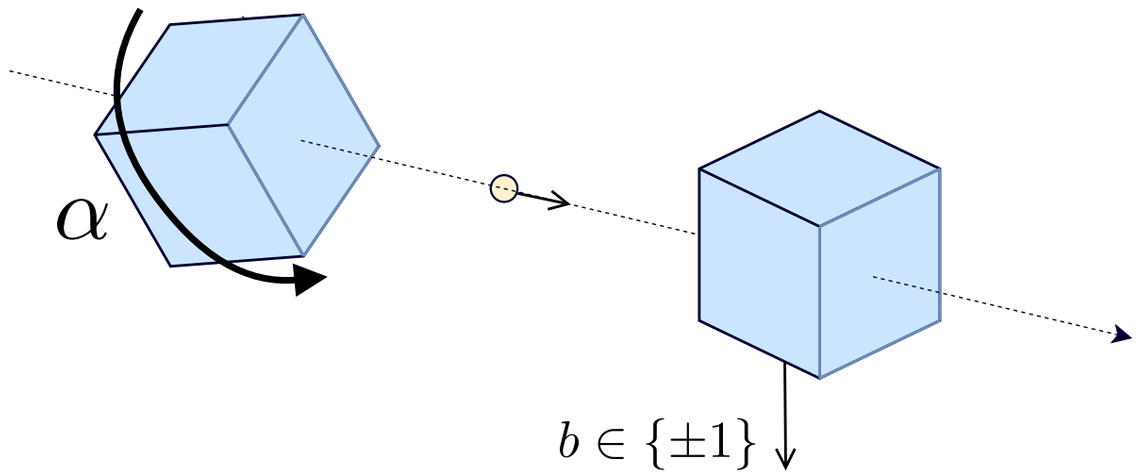


Observed statistics:

$$\mathrm{Prob}(b|\alpha)$$

$$\mathrm{Prob}(+1|\alpha) + \mathrm{Prob}(-1|\alpha) = 1.$$

Generalized SO(2) prepare-and-measure



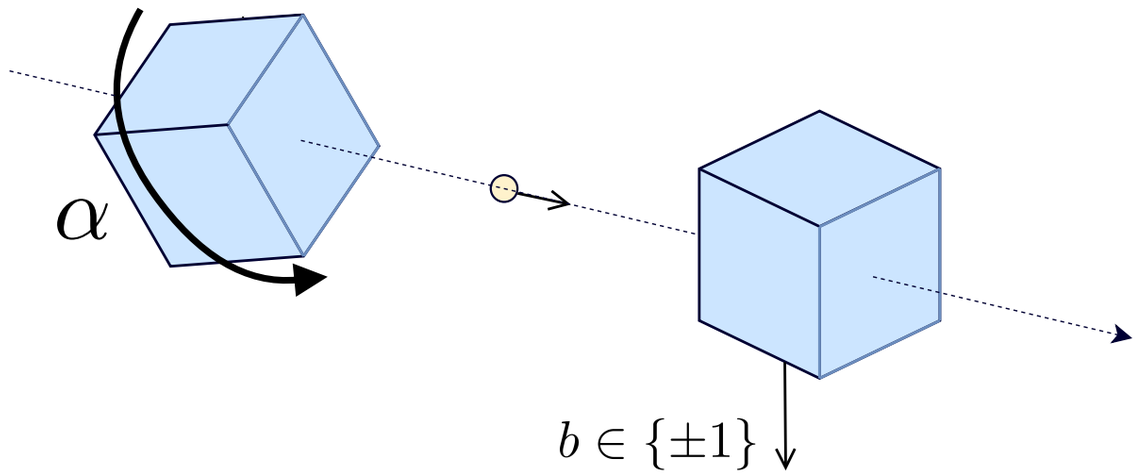
Observed statistics:

$$\mathrm{Prob}(b|\alpha)$$

$$\mathrm{Prob}(+1|\alpha) + \mathrm{Prob}(-1|\alpha) = 1.$$

Transformations T are linear maps $T \in \mathcal{L}(V_A)$ which are **positive**, i.e. $T(A_+) \subseteq A_+,$ and **normalization-preserving**, i.e. $u_A \circ T = u_A.$

Generalized SO(2) prepare-and-measure



Observed statistics:

$$\mathrm{Prob}(b|\alpha)$$

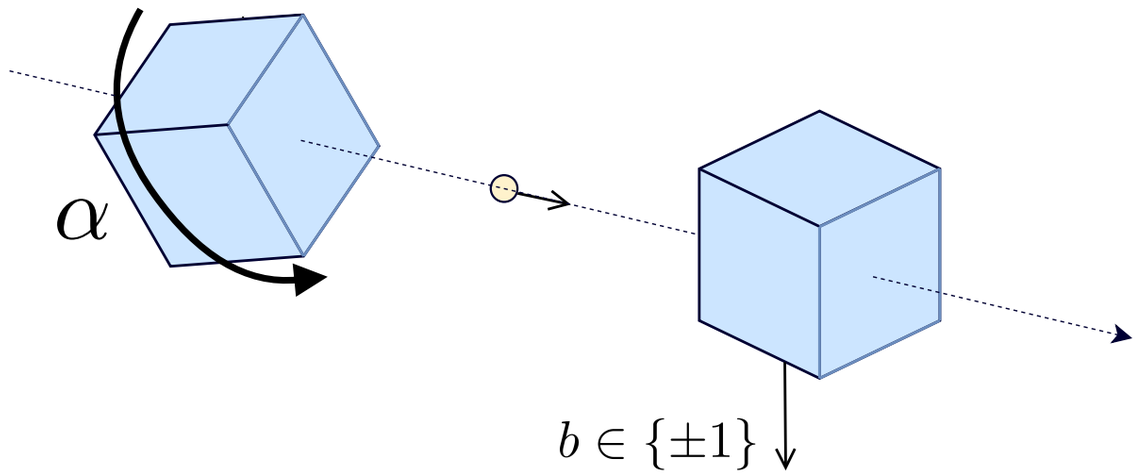
$$\mathrm{Prob}(+1|\alpha) + \mathrm{Prob}(-1|\alpha) = 1.$$

Transformations T are linear maps $T \in \mathcal{L}(V_A)$ which are **positive**, i.e. $T(A_+) \subseteq A_+,$ and **normalization-preserving**, i.e. $u_A \circ T = u_A.$

The standard textbook arguments still apply, and we get a continuous group homomorphism $\mathrm{SO}(2) \to \mathcal{L}(V_A), \quad \alpha \mapsto T_\alpha$

such that every T_α is a transformation, and $\omega_\alpha = T_\alpha \omega$ is prepared.

Generalized SO(2) prepare-and-measure



Observed statistics:

$$\mathrm{Prob}(b|\alpha)$$

$$\mathrm{Prob}(+1|\alpha) + \mathrm{Prob}(-1|\alpha) = 1.$$

Transformations T are linear maps $T \in \mathcal{L}(V_A)$ which are **positive**, i.e. $T(A_+) \subseteq A_+,$ and **normalization-preserving**, i.e. $u_A \circ T = u_A.$

The standard textbook arguments still apply, and we get a continuous group homomorphism $\mathrm{SO}(2) \to \mathcal{L}(V_A), \quad \alpha \mapsto T_\alpha$

such that every T_α is a transformation, and $\omega_\alpha = T_\alpha \omega$ is prepared.

Definition. The GPT system *A* is a spin-*J* system if, for $m_{2J} \neq 0,$

$$T_\alpha \simeq \mathbf{1}_{m_0} \oplus \bigoplus_{k=1}^{2J} \mathbf{1}_{m_k} \otimes \begin{pmatrix} \cos(k\alpha) & -\sin(k\alpha) \\ \sin(k\alpha) & \cos(k\alpha) \end{pmatrix}$$

Rotation boxes $\mathcal{R}_J$

Rotation boxes $\mathcal{R}_J$

Definition. The set $\mathcal{R}_J$ of spin-J correlations is the set of all functions $P(+1|\alpha)$ arising from *some* GPT system of spin *J* or less, i.e.

$$P(+1|\alpha) = (e, T_\alpha \omega)$$

where $\omega \in \Omega_A$, $0 \leq e \leq u_A$ and $\alpha \mapsto T_\alpha$ is the associated representation of SO(2).

Rotation boxes $\mathcal{R}_J$

Definition. The set $\mathcal{R}_J$ of spin-J correlations is the set of all functions $P(+1|\alpha)$ arising from *some* GPT system of spin *J* or less, i.e.

$$P(+1|\alpha) = (e, T_\alpha \omega)$$

where $\omega \in \Omega_A$, $0 \leq e \leq u_A$ and $\alpha \mapsto T_\alpha$ is the associated representation of SO(2).

The form of the T_α implies that every such function is a trigonometric polynomial of degree at most 2J. Moreover, we can show:

Rotation boxes $\mathcal{R}_J$

Definition. The set $\mathcal{R}_J$ of spin-J correlations is the set of all functions $P(+1|\alpha)$ arising from *some* GPT system of spin *J* or less, i.e.

$$P(+1|\alpha) = (e, T_\alpha \omega)$$

where $\omega \in \Omega_A$, $0 \leq e \leq u_A$ and $\alpha \mapsto T_\alpha$ is the associated representation of SO(2).

The form of the T_α implies that every such function is a trigonometric polynomial of degree at most 2J. Moreover, we can show:

Lemma. $\mathcal{R}_J$ is *exactly* the set of all trigonometric polynomials of degree at most 2J with $0 \leq P(+1|\alpha) \leq 1$ for all α.

Rotation boxes $\mathcal{R}_J$

Definition. The set $\mathcal{R}_J$ of spin-J correlations is the set of all functions $P(+1|\alpha)$ arising from *some* GPT system of spin *J* or less, i.e.

$$P(+1|\alpha) = (e, T_\alpha \omega)$$

where $\omega \in \Omega_A$, $0 \leq e \leq u_A$ and $\alpha \mapsto T_\alpha$ is the associated representation of SO(2).

The form of the T_α implies that every such function is a trigonometric polynomial of degree at most 2J. Moreover, we can show:

Lemma. $\mathcal{R}_J$ is *exactly* the set of all trigonometric polynomials of degree at most 2J with $0 \leq P(+1|\alpha) \leq 1$ for all α.

It describes how any conceivable statistical physical system of spin J (quantum or not) could respond to spatial rotations around a single axis.

Quantum vs. general rotation boxes

Quantum vs. general rotation boxes

- Definition of **quantum spin-J boxes**:

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

Quantum vs. general rotation boxes

- Definition of **quantum spin-J boxes**:

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

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

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

Quantum vs. general rotation boxes

- Definition of **quantum spin-J boxes**:

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

- 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 $\mathcal{Q}_J \subseteq \mathcal{R}_J$.

Quantum vs. general rotation boxes

- Definition of **quantum spin-J boxes**:

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

- 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 $\mathcal{Q}_J \subseteq \mathcal{R}_J$.

For $J = 0$, we obtain the constant probability functions:

$$\mathcal{Q}_0 = \mathcal{R}_0 = \{P(+1|\alpha) = c \mid 0 \leq c \leq 1\}.$$

Quantum vs. general rotation boxes

- Definition of **quantum spin-J boxes**:

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

- 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 $\mathcal{Q}_J \subseteq \mathcal{R}_J.$ $\mathcal{Q}_0 = \mathcal{R}_0$

Quantum vs. general rotation boxes

- Definition of **quantum spin-J boxes**:

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

- 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 $\mathcal{Q}_J \subseteq \mathcal{R}_J$. $\quad \mathcal{Q}_0 = \mathcal{R}_0$

For $J = \frac{1}{2}$, all rotation boxes can be realized on a qubit, hence $\mathcal{Q}_{1/2} = \mathcal{R}_{1/2}$.

Quantum vs. general rotation boxes

- Definition of **quantum spin-J boxes**:

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

- 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 $\mathcal{Q}_J \subseteq \mathcal{R}_J$. $\mathcal{Q}_0 = \mathcal{R}_0$

For $J = \frac{1}{2}$, all rotation boxes can be realized on a qubit, hence $\mathcal{Q}_{1/2} = \mathcal{R}_{1/2}$.

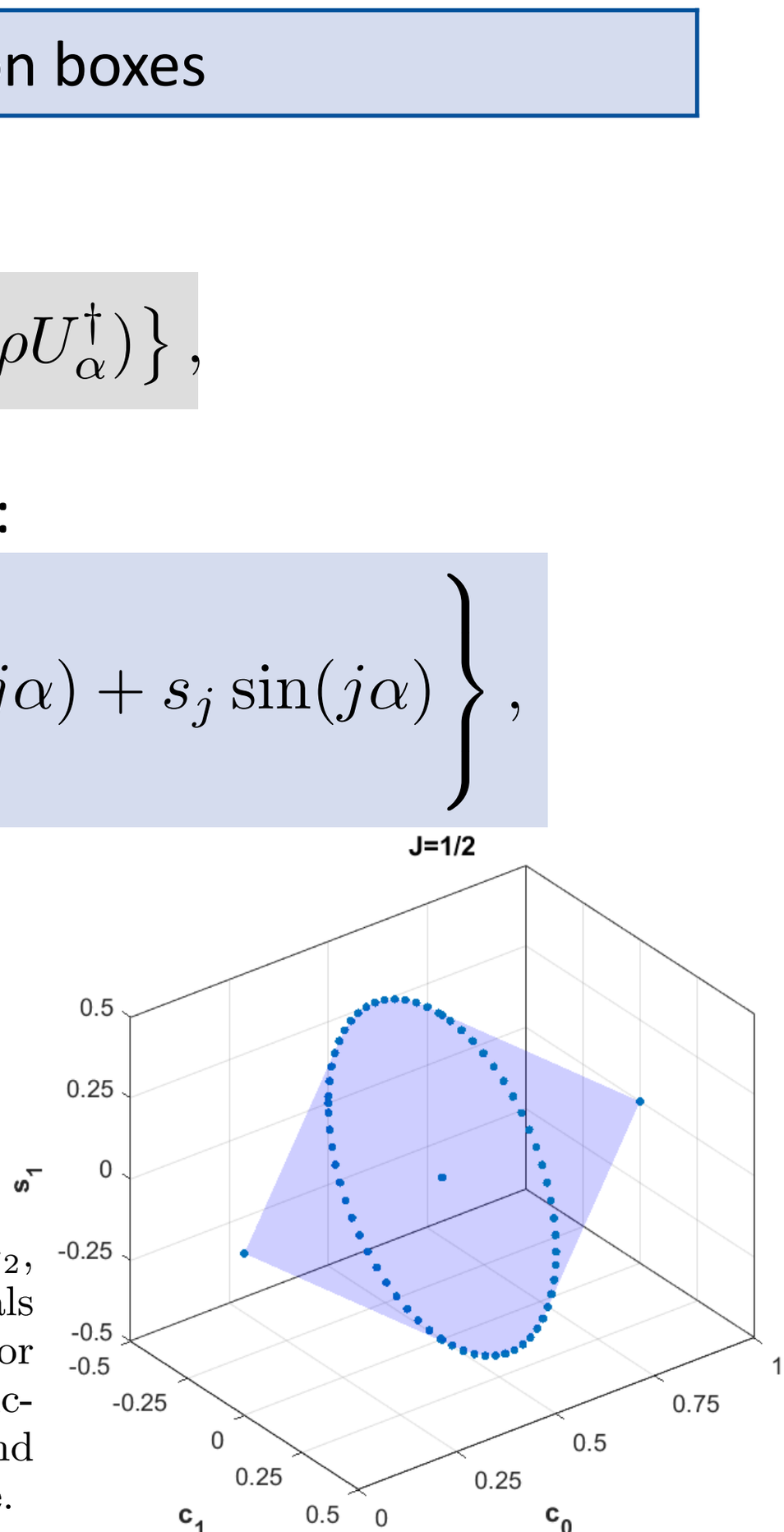


FIG. 4. The binary quantum spin-1/2 correlations $\mathcal{Q}_{1/2}$, which happens to be the set of trigonometric polynomials $P(+|\theta) = c_0 + c_1 \cos\theta + s_1 \sin\theta$ with $0 \leq P(+|\theta) \leq 1$ for all θ. The two endpoints are the constant zero and one functions, and the other extremal points on the circle correspond to functions $\theta \mapsto \frac{1}{2} + \frac{1}{2}\cos(\theta - \varphi)$, with φ some fixed angle.

Classification of the spin-1 correlations

Classification of the spin-1 correlations

The spin-1 rotation boxes are the trigonometric polynomials with

$$0 \leq c_0 + c_1 \cos\alpha + s_1 \sin\alpha + c_2 \cos(2\alpha) + s_2 \sin(2\alpha) \leq 1,$$

with coefficients $(c_0, c_1, s_1, c_2, s_2) \in \mathbb{R}^5$.

Classification of the spin-1 correlations

The spin-1 rotation boxes are the trigonometric polynomials with

$$0 \leq c_0 + c_1 \cos\alpha + s_1 \sin\alpha + c_2 \cos(2\alpha) + s_2 \sin(2\alpha) \leq 1,$$

with coefficients $(c_0, c_1, s_1, c_2, s_2) \in \mathbb{R}^5$.

Task: classify the **extremal points** $p(\alpha)$ of the compact convex set $\mathcal{R}_1$.

Each one attains the value zero somewhere. Shifting the angle, we can restrict our attention to those with $p(0) = 0 \Rightarrow p'(0) = 0$.

Classification of the spin-1 correlations

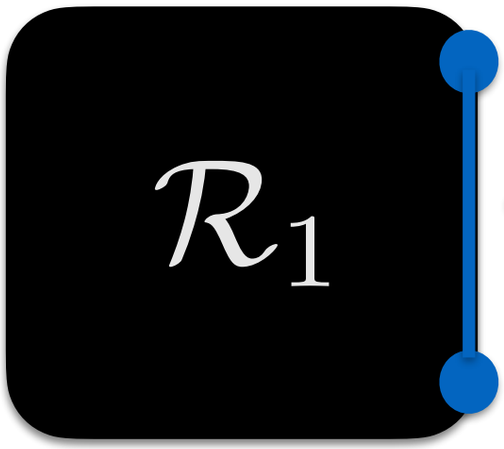
The spin-1 rotation boxes are the trigonometric polynomials with

$$0 \leq c_0 + c_1 \cos\alpha + s_1 \sin\alpha + c_2 \cos(2\alpha) + s_2 \sin(2\alpha) \leq 1,$$

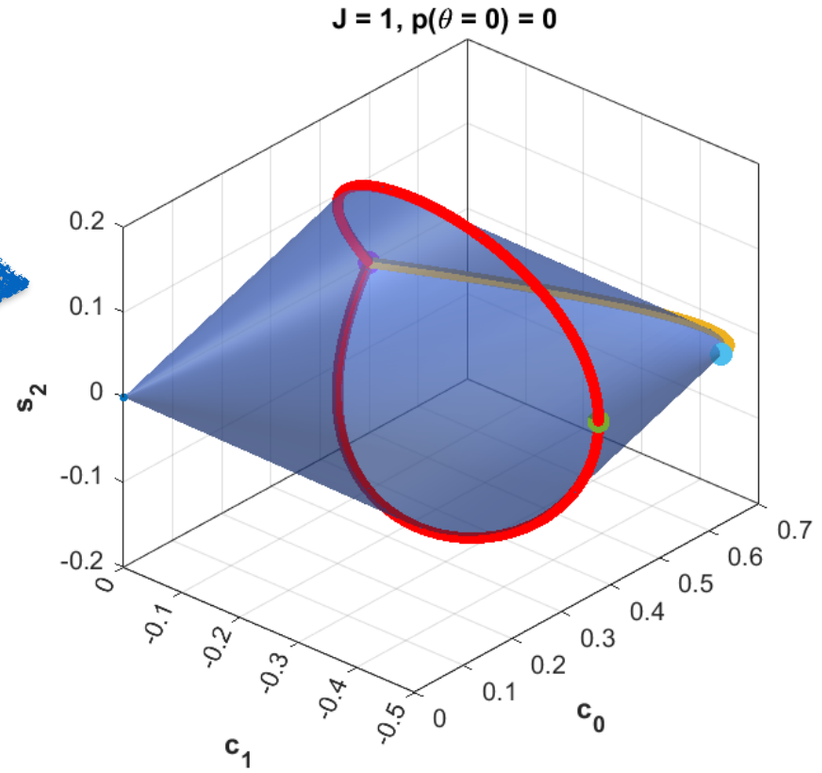
with coefficients $(c_0, c_1, s_1, c_2, s_2) \in \mathbb{R}^5$.

Task: classify the **extremal points** $p(\alpha)$ of the compact convex set $\mathcal{R}_1$.

Each one attains the value zero somewhere. Shifting the angle, we can restrict our attention to those with $p(0) = 0 \Rightarrow p'(0) = 0$.



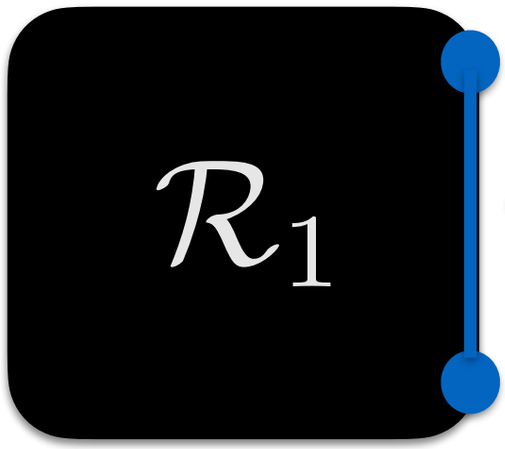
5-dimensional



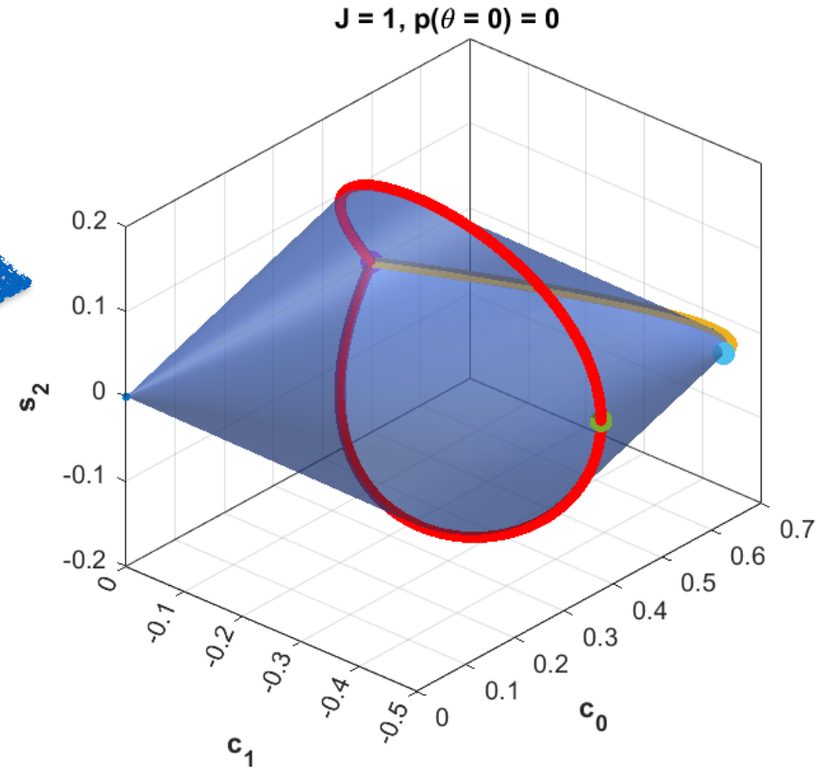
3-dimensional face

$\{p \in \mathcal{R}_1 \mid p(0) = 0\}$

Classification of the spin-1 correlations



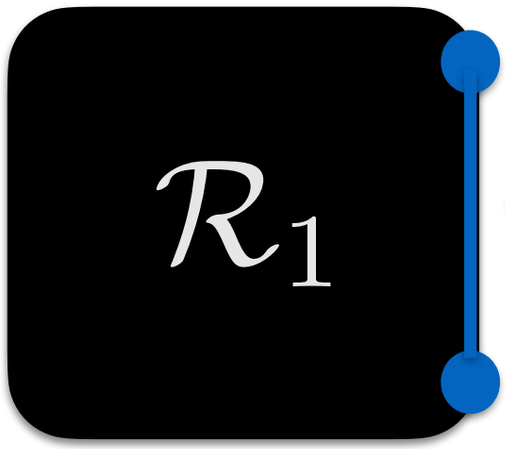
5-dimensional



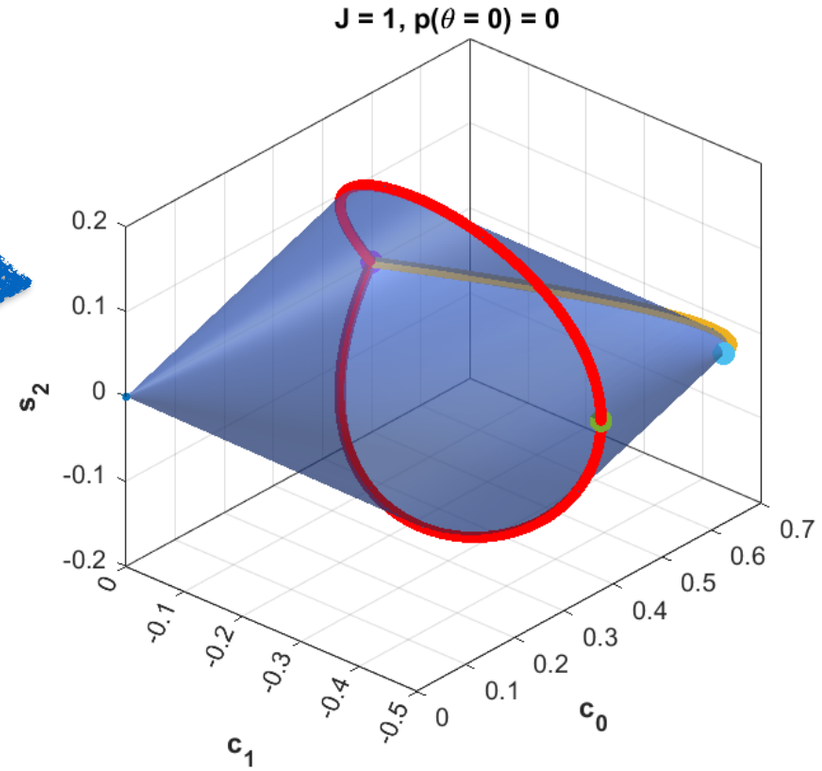
3-dimensional face

$\{p \in \mathcal{R}_1 \mid p(0) = 0\}$

Classification of the spin-1 correlations



5-dimensional



3-dimensional face

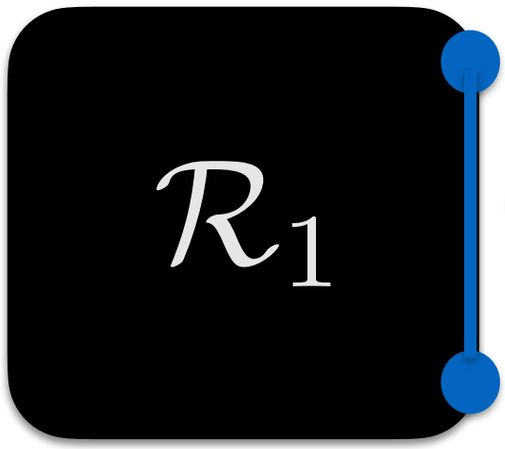
$$\{p \in \mathcal{R}_1 \mid p(0) = 0\}$$

We can give the extremal points explicitly:

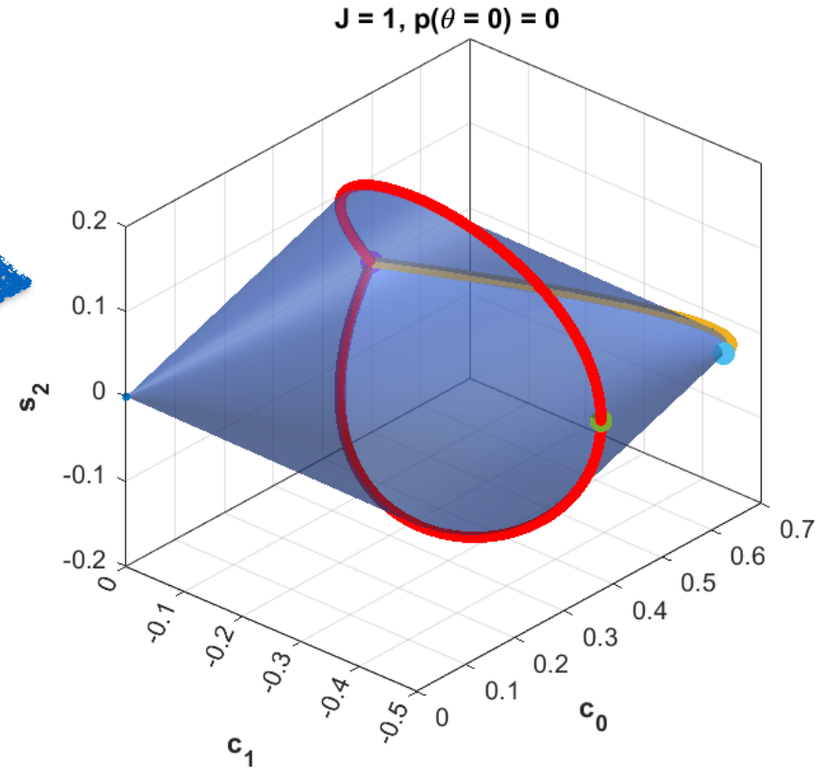
$$\begin{aligned}
p_0(\alpha) &= 0 \\
p_1(\alpha) &= \sin^2 \alpha \\
p_2(\alpha) &= \sin^4 \frac{\alpha}{2} \\
p_3(\alpha) &= \frac{1}{4}(1-\cos\alpha)(3+\cos\alpha) \\
p_4(\alpha) &= c(1-\cos\alpha)(1-\cos(\alpha-\alpha_0)) \\
p_5(\alpha) &= 1 - p_4(\alpha_1 - \alpha).
\end{aligned}$$

Main math. tool: Fejér-Riesz theorem.

Classification of the spin-1 correlations



5-dimensional



3-dimensional face

$$\{p \in \mathcal{R}_1 \mid p(0) = 0\}$$

We can give the extremal points explicitly:

$$\begin{aligned}
p_0(\alpha) &= 0 \\
p_1(\alpha) &= \sin^2 \alpha \\
p_2(\alpha) &= \sin^4 \frac{\alpha}{2} \\
p_3(\alpha) &= \frac{1}{4}(1-\cos\alpha)(3+\cos\alpha) \\
p_4(\alpha) &= c(1-\cos\alpha)(1-\cos(\alpha-\alpha_0)) \\
p_5(\alpha) &= 1 - p_4(\alpha_1 - \alpha).
\end{aligned}$$

Main math. tool: Fejér-Riesz theorem.

For all of these, we can construct spin-1 quantum realizations! This proves

$$\partial\mathcal{R}_1 \subseteq \partial\mathcal{Q}_1$$

and then by convexity

$$\mathcal{Q}_1 = \mathcal{R}_1.$$

Overview

1. Motivation (and some history)

2. “Rotation boxes” within and beyond QT

3. A metrological game and the (sub)optimality of QT

4. A theory-independent SDI randomness generator

5. Conclusions

Overview

1. Motivation (and some history)

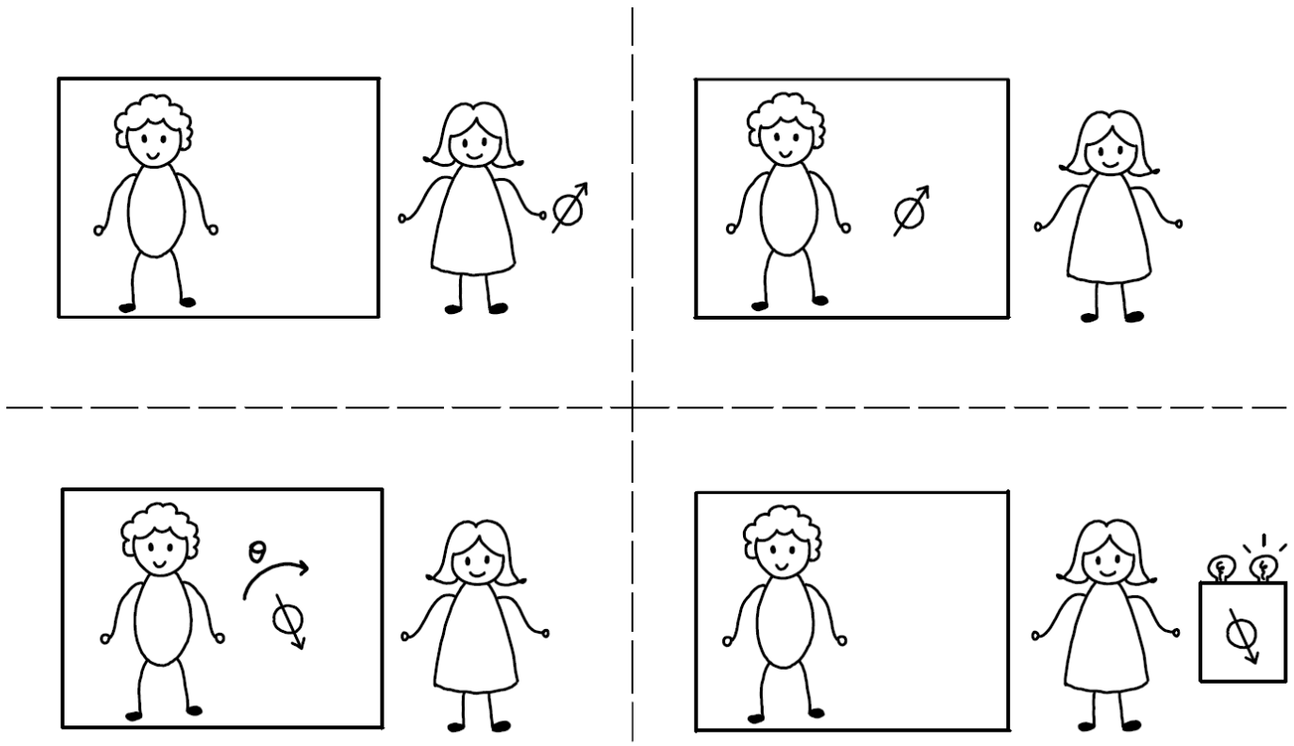
2. “Rotation boxes” within and beyond QT

3. A metrological game and the (sub)optimality of QT

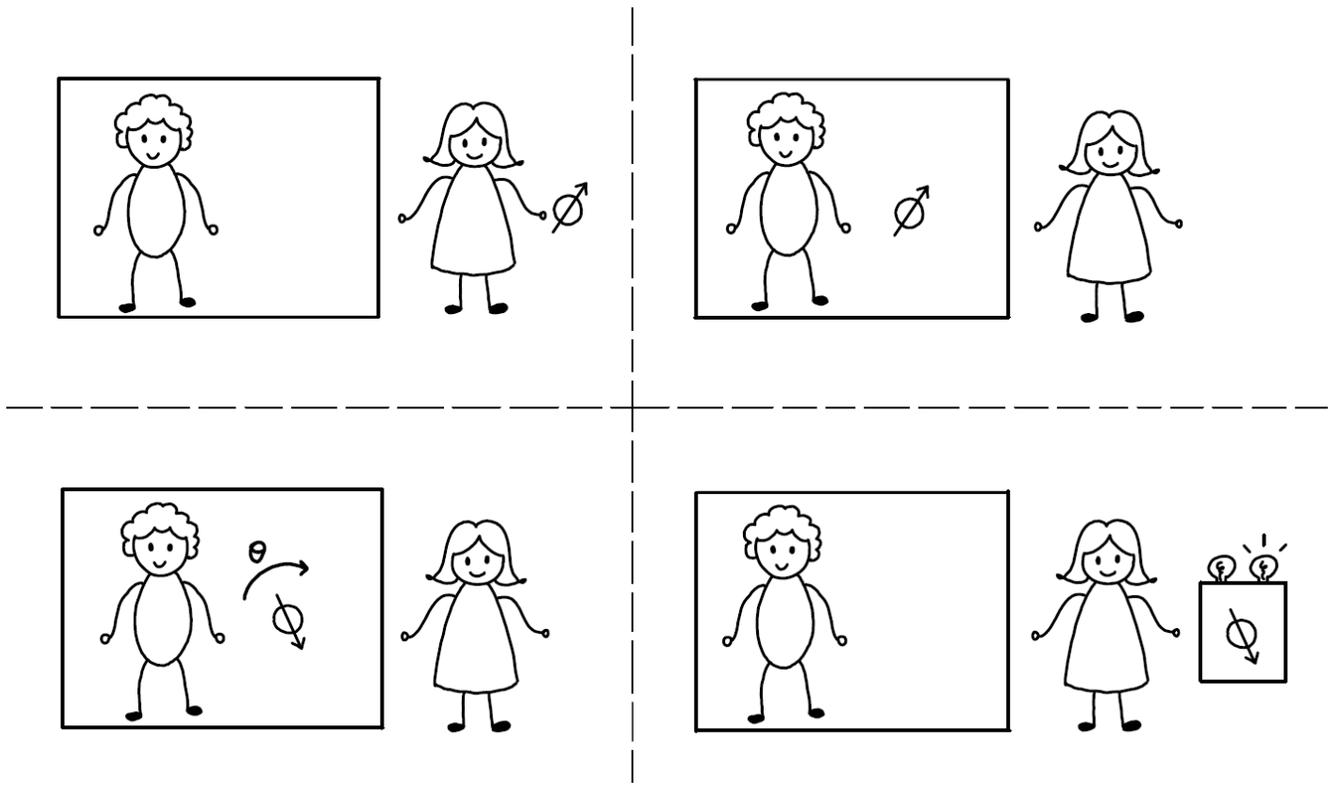
4. A theory-independent SDI randomness generator

5. Conclusions

A metrological game

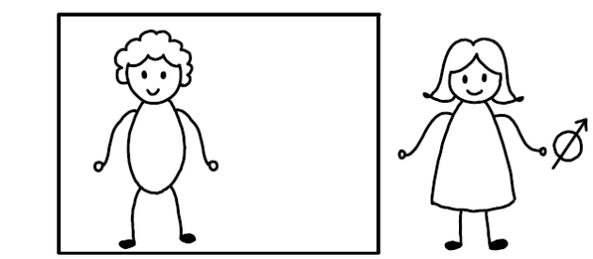


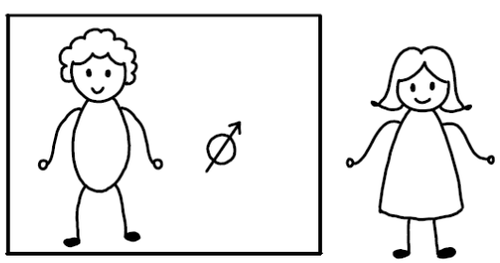
A metrological game

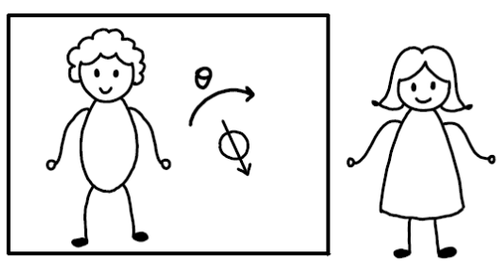


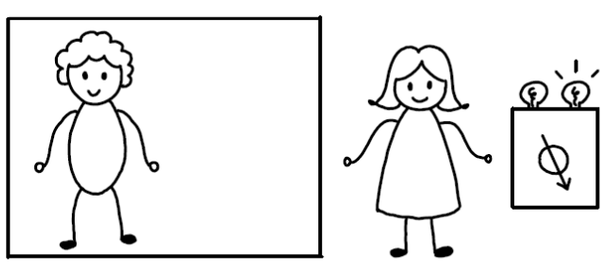
- Alice prepares a spin-J system of her probabilistic theory.
- She hands it over to Bob, who performs a rotation by θ. His angle is chosen at random with $\mu(\theta) := n^{-1}|\cos(2\theta) + \sin(3\theta)|$.

A metrological game

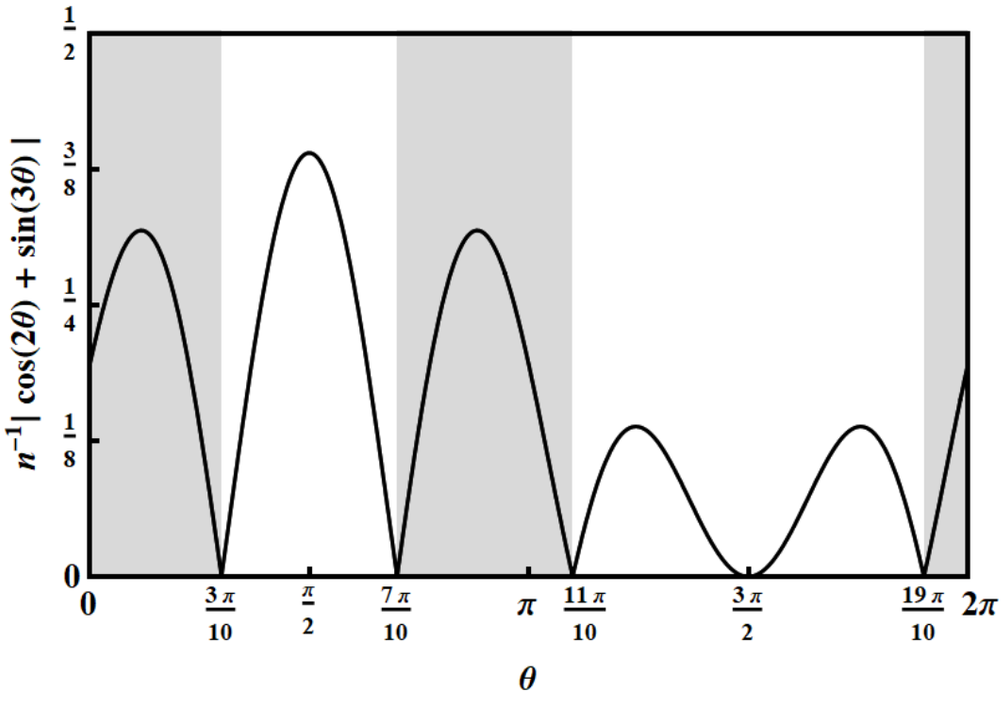




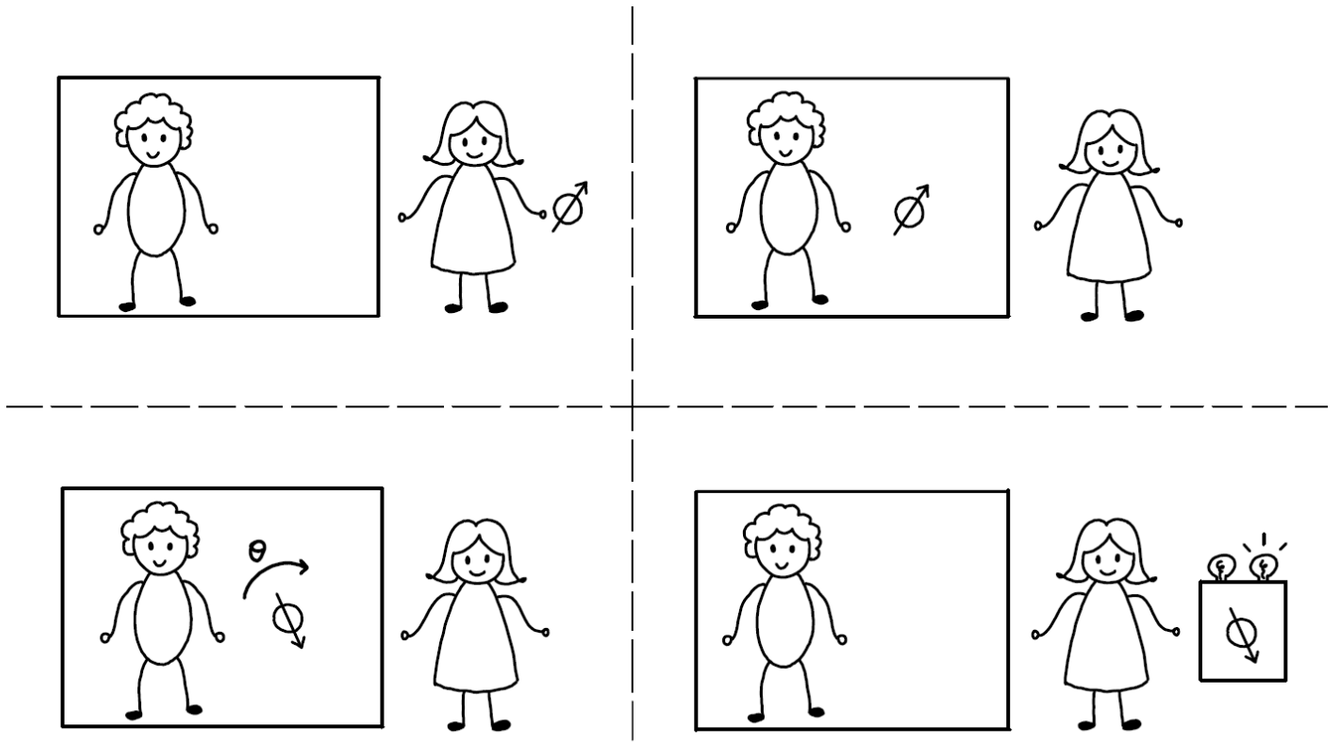




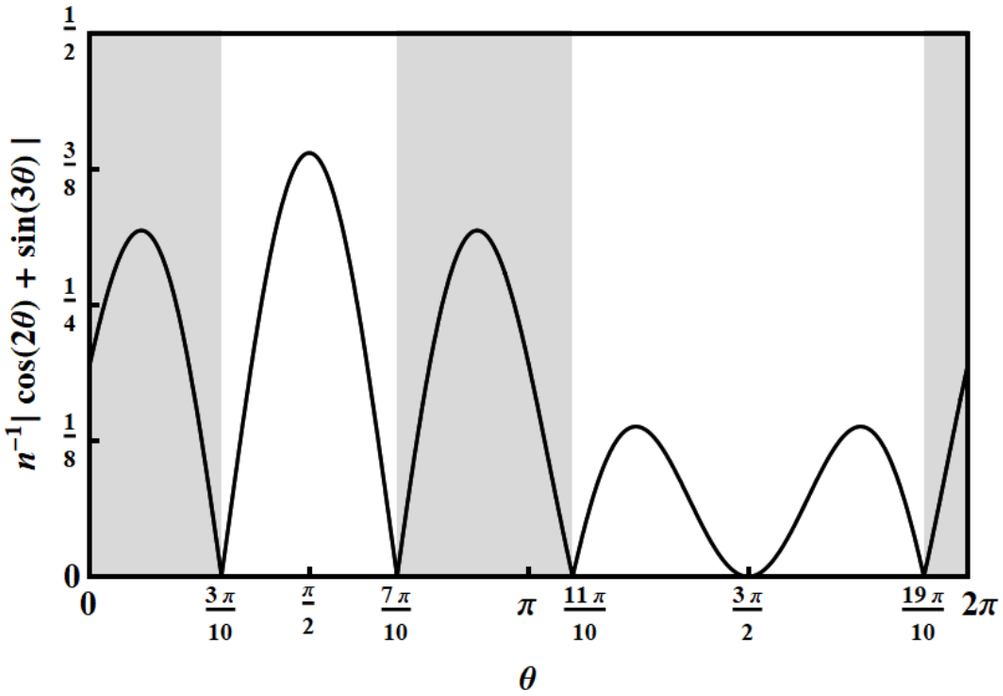
- Alice prepares a spin-J system of her probabilistic theory.
- She hands it over to Bob, who performs a rotation by θ. His angle is chosen at random with $\mu(\theta) := n^{-1}|\cos(2\theta) + \sin(3\theta)|$.
- Alice's task: decide whether θ is in the gray or the white set of angles (has prob. 1/2 each).



A metrological game



- Alice prepares a spin-J system of her probabilistic theory.
- She hands it over to Bob, who performs a rotation by θ. His angle is chosen at random with $\mu(\theta) := n^{-1}|\cos(2\theta) + \sin(3\theta)|$.
- Alice's task: decide whether θ is in the gray or the white set of angles (has prob. 1/2 each).



For spin $J \in \{0, \frac{1}{2}, 1\}$, quantum systems are optimal for winning such games. But for $J = \frac{3}{2}$, the maximal quantum winning probability is $P^{\mathrm{Q}}_{\mathrm{succ}} \approx 85\%$, whereas some rotation boxes allow Alice to win it with $P^{\mathrm{R}}_{\mathrm{succ}} \approx 88\%$.

A metrological game

This is because $\mathcal{Q}_{3/2} \subsetneq \mathcal{R}_{3/2}$:

A metrological game

This is because $\mathcal{Q}_{3/2} \subsetneq \mathcal{R}_{3/2}$:

$$\begin{aligned} p(\theta) \;=\; & c_0 + c_1\cos\theta + s_1\sin\theta + c_2\cos(2\theta) + s_2\sin(2\theta) \\ & + c_3\cos(3\theta) + s_3\sin(3\theta), \end{aligned} \tag{31}$$

A metrological game

This is because $\mathcal{Q}_{3/2} \subsetneq \mathcal{R}_{3/2}$:

$$\begin{aligned} p(\theta) \;=\; & c_0 + c_1\cos\theta + s_1\sin\theta + c_2\cos(2\theta) + s_2\sin(2\theta) \\ & + c_3\cos(3\theta) + s_3\sin(3\theta), \end{aligned} \tag{31}$$

Theorem 6. *If $p \in \mathcal{Q}_{3/2}$, then its trigonometric coefficients, as taken from representation (31), satisfy*

$$c_2 + s_3 \leq \frac{1}{\sqrt{3}} \lesssim 0.5774.$$

On the other hand, the trigonometric polynomial

$$p^\star(\theta) := \frac{2}{5} + \frac{1}{4}\sin\theta + \frac{7}{20}\cos(2\theta) + \frac{1}{4}\sin(3\theta)$$

satisfies $0 \leq p^\star(\theta) \leq 1$ for all θ, hence $p^\star \in \mathcal{R}_{3/2}$, but $c_2 + s_3 = 0.6$, i.e. $p^\star \notin \mathcal{Q}_{3/2}$. In particular, $\mathcal{Q}_{3/2} \subsetneq \mathcal{R}_{3/2}$.

A metrological game

This is because $\mathcal{Q}_{3/2} \subsetneq \mathcal{R}_{3/2}$:

$$\begin{aligned} p(\theta) \;=\; & c_0 + c_1\cos\theta + s_1\sin\theta + c_2\cos(2\theta) + s_2\sin(2\theta) \\ & + c_3\cos(3\theta) + s_3\sin(3\theta), \end{aligned} \tag{31}$$

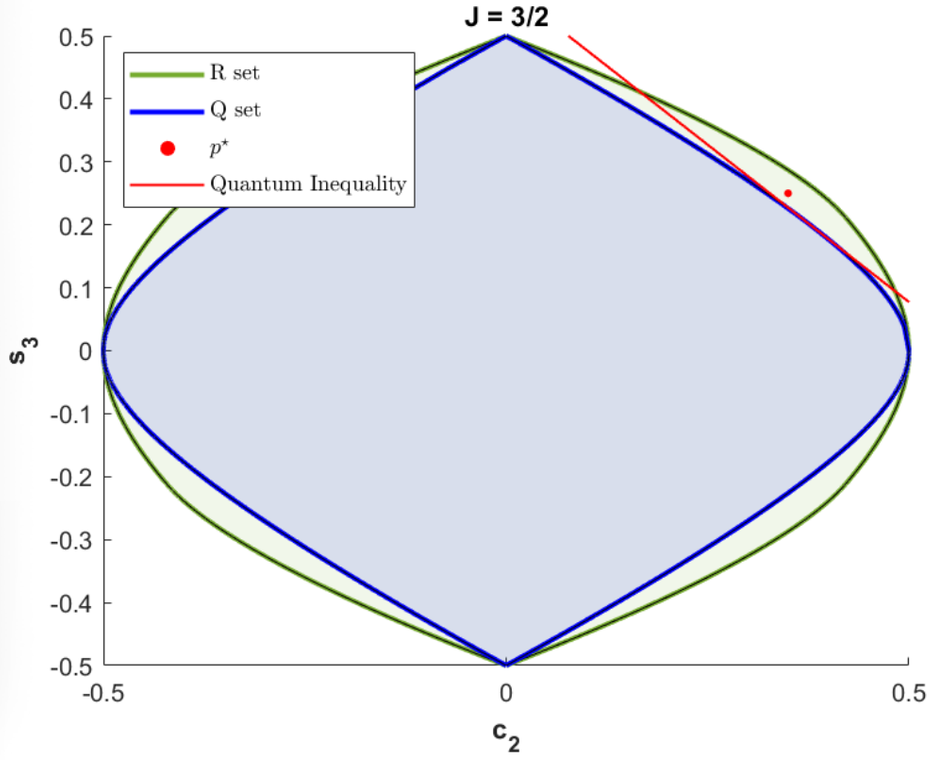
Theorem 6. *If $p \in \mathcal{Q}_{3/2}$, then its trigonometric coefficients, as taken from representation (31), satisfy*

$$c_2 + s_3 \leq \frac{1}{\sqrt{3}} \lesssim 0.5774.$$

On the other hand, the trigonometric polynomial

$$p^\star(\theta) := \frac{2}{5} + \frac{1}{4}\sin\theta + \frac{7}{20}\cos(2\theta) + \frac{1}{4}\sin(3\theta)$$

satisfies $0 \leq p^\star(\theta) \leq 1$ for all θ, hence $p^\star \in \mathcal{R}_{3/2}$, but $c_2 + s_3 = 0.6$, i.e. $p^\star \notin \mathcal{Q}_{3/2}$. In particular, $\mathcal{Q}_{3/2} \subsetneq \mathcal{R}_{3/2}$.



A metrological game

This is because $\mathcal{Q}_{3/2} \subsetneq \mathcal{R}_{3/2}$:

$$p(\theta) = c_0 + c_1 \cos\theta + s_1 \sin\theta + c_2 \cos(2\theta) + s_2 \sin(2\theta) + c_3 \cos(3\theta) + s_3 \sin(3\theta), \quad (31)$$

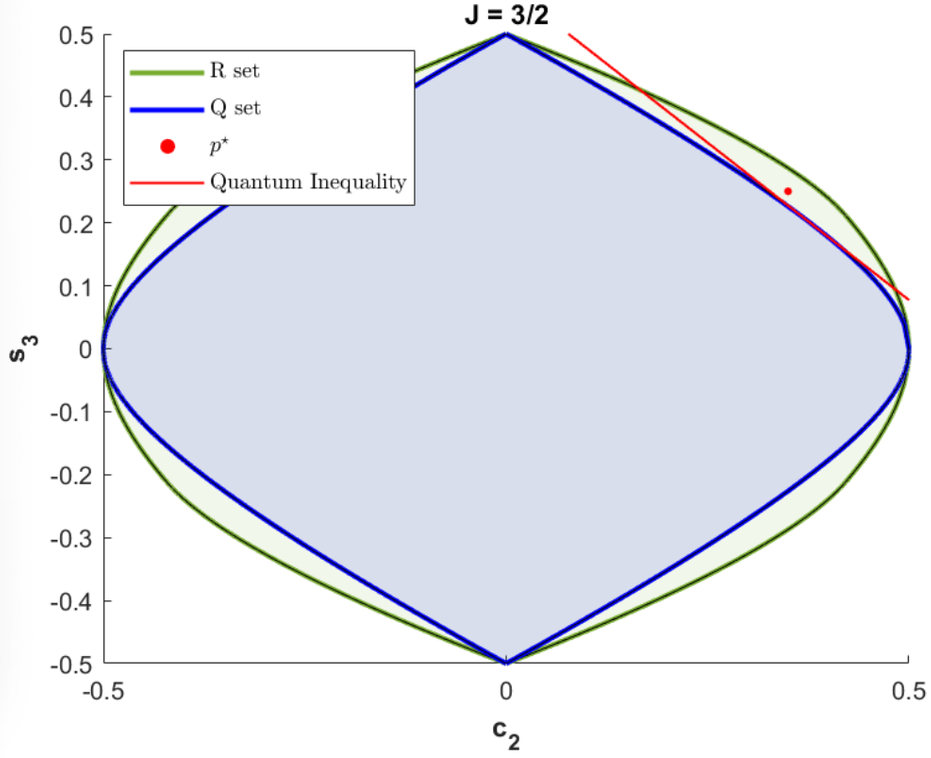
Theorem 6. *If $p \in \mathcal{Q}_{3/2}$, then its trigonometric coefficients, as taken from representation (31), satisfy*

$$c_2 + s_3 \leq \frac{1}{\sqrt{3}} \lesssim 0.5774.$$

On the other hand, the trigonometric polynomial

$$p^\star(\theta) := \frac{2}{5} + \frac{1}{4}\sin\theta + \frac{7}{20}\cos(2\theta) + \frac{1}{4}\sin(3\theta)$$

satisfies $0 \leq p^\star(\theta) \leq 1$ for all θ, hence $p^\star \in \mathcal{R}_{3/2}$, but $c_2 + s_3 = 0.6$, i.e. $p^\star \notin \mathcal{Q}_{3/2}$. In particular, $\mathcal{Q}_{3/2} \subsetneq \mathcal{R}_{3/2}$.



A similar gap can be demonstrated for all $J \geq 2$.

The large-J limit

The large-J limit

The trigonometric polynomials are uniformly dense in the continuous functions, hence, trivially,

$$\overline{\bigcup_J \mathcal{R}_J} = \mathcal{R}_\infty$$

(closure with respect to the uniform norm $\|\cdot\|_\infty$), where

$$\mathcal{R}_\infty := \{f \in \mathcal{C}(\mathrm{SO}(2)) \mid 0 \leq f(\theta) \leq 1 \text{ for all } \theta \in [0, 2\pi)\}.$$

The large-J limit

The trigonometric polynomials are uniformly dense in the continuous functions, hence, trivially,

$$\overline{\bigcup_J \mathcal{R}_J} = \mathcal{R}_\infty$$

(closure with respect to the uniform norm $\|\cdot\|_\infty$), where

$$\mathcal{R}_\infty := \{f \in \mathcal{C}(\mathrm{SO}(2)) \mid 0 \leq f(\theta) \leq 1 \text{ for all } \theta \in [0, 2\pi)\}.$$

But we also have

Theorem 8. *The set of continuous rotational correlations $\mathcal{R}_\infty$ is the closure of the union of all sets of spin-J quantum boxes $\mathcal{Q}_J$ with finite $J < \infty$, i.e.*

$$\mathcal{R}_\infty = \overline{\bigcup_J \mathcal{Q}_J} \tag{40}$$

The large-J limit

The trigonometric polynomials are uniformly dense in the continuous functions, hence, trivially,

$$\overline{\bigcup_J \mathcal{R}_J} = \mathcal{R}_\infty$$

(closure with respect to the uniform norm $\|\cdot\|_\infty$), where

$$\mathcal{R}_\infty := \{f \in \mathcal{C}(\mathrm{SO}(2)) \mid 0 \leq f(\theta) \leq 1 \text{ for all } \theta \in [0, 2\pi)\}.$$

But we also have

Theorem 8. *The set of continuous rotational correlations $\mathcal{R}_\infty$ is the closure of the union of all sets of spin-J quantum boxes $\mathcal{Q}_J$ with finite $J < \infty$, i.e.*

$$\mathcal{R}_\infty = \overline{\bigcup_J \mathcal{Q}_J} \tag{40}$$

Quantum rotation boxes can approximate every continuous prob. function.

The large-J limit

The trigonometric polynomials are uniformly dense in the continuous functions, hence, trivially,

$$\overline{\bigcup_J \mathcal{R}_J} = \mathcal{R}_\infty$$

(closure with respect to the uniform norm $\|\cdot\|_\infty$), where

$$\mathcal{R}_\infty := \{f \in \mathcal{C}(\mathrm{SO}(2)) \mid 0 \leq f(\theta) \leq 1 \text{ for all } \theta \in [0, 2\pi)\}.$$

But we also have

Theorem 8. *The set of continuous rotational correlations $\mathcal{R}_\infty$ is the closure of the union of all sets of spin-J quantum boxes $\mathcal{Q}_J$ with finite $J < \infty$, i.e.*

$$\mathcal{R}_\infty = \overline{\bigcup_J \mathcal{Q}_J} \tag{40}$$

Quantum rotation boxes can approximate every continuous prob. function.

Proof: via Peter-Weyl theorem + truncation of infinite-dim. Hilbert space.

Overview

1. Motivation (and some history)

2. “Rotation boxes” within and beyond QT

3. A metrological game and the (sub)optimality of QT

4. A theory-independent SDI randomness generator

5. Conclusions

Overview

1. Motivation (and some history)

2. “Rotation boxes” within and beyond QT

3. A metrological game and the (sub)optimality of QT

4. A theory-independent SDI randomness generator

5. Conclusions

A simple observation

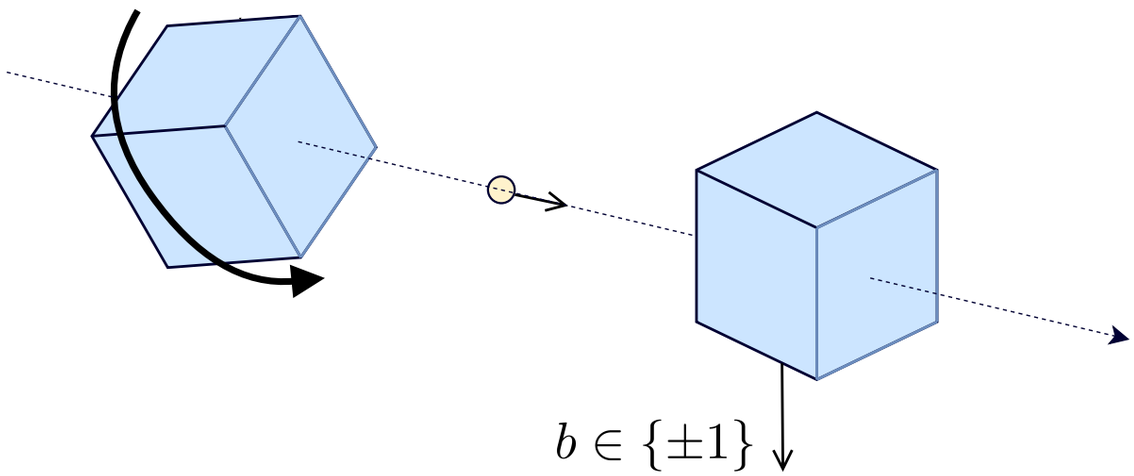
A simple observation

If we consider two fixed angles only, then quantum and general spin-J rotation boxes turn out to admit identical statistical behavior.

A simple observation

If we consider two fixed angles only, then quantum and general spin-J rotation boxes turn out to admit identical statistical behavior.

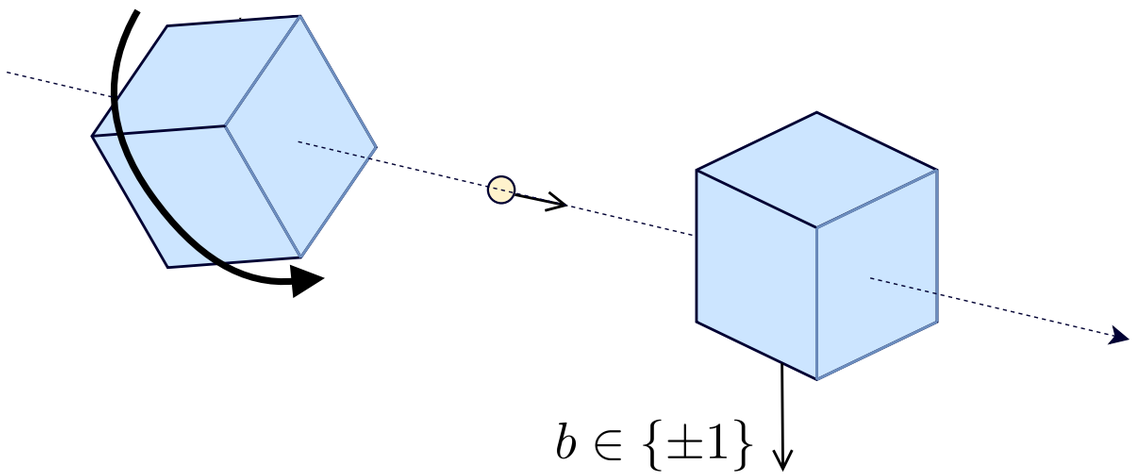
Example. It is well-known in quantum theory that we have to rotate a system by angle at least $\alpha \geq \pi/(2J)$ to obtain an orthogonal state, i.e. to have $\rho_a \perp \rho_0$.



A simple observation

If we consider two fixed angles only, then quantum and general spin-J rotation boxes turn out to admit identical statistical behavior.

Example. It is well-known in quantum theory that we have to rotate a system by angle at least $\alpha \geq \pi/(2J)$ to obtain an orthogonal state, i.e. to have $\rho_a \perp \rho_0$.

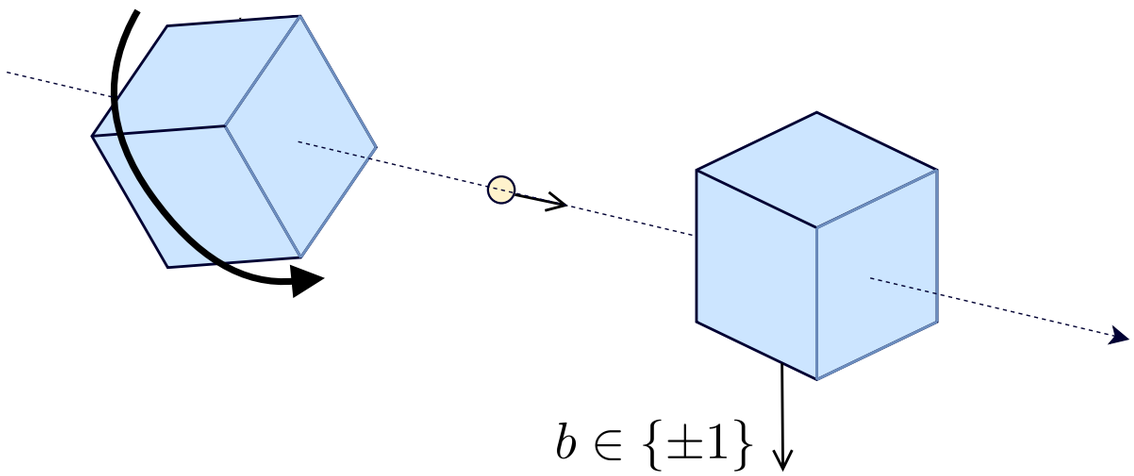


Theorem. Let $p \in \mathcal{R}_J$ with $p(+1|0) = 0$ and $p(+1|\alpha) = 1$.
Then $\alpha \geq \pi/(2J)$.

A simple observation

If we consider two fixed angles only, then quantum and general spin-J rotation boxes turn out to admit identical statistical behavior.

Example. It is well-known in quantum theory that we have to rotate a system by angle at least $\alpha \geq \pi/(2J)$ to obtain an orthogonal state, i.e. to have $\rho_a \perp \rho_0$.



Theorem. Let $p \in \mathcal{R}_J$ with $p(+1|0) = 0$ and $p(+1|\alpha) = 1$.
Then $\alpha \geq \pi/(2J)$.

In spirit, this is related to quantum speed limits / metrology.
But the equivalence goes much further, as we know show.

Motivation: (semi-)device-independent QIT

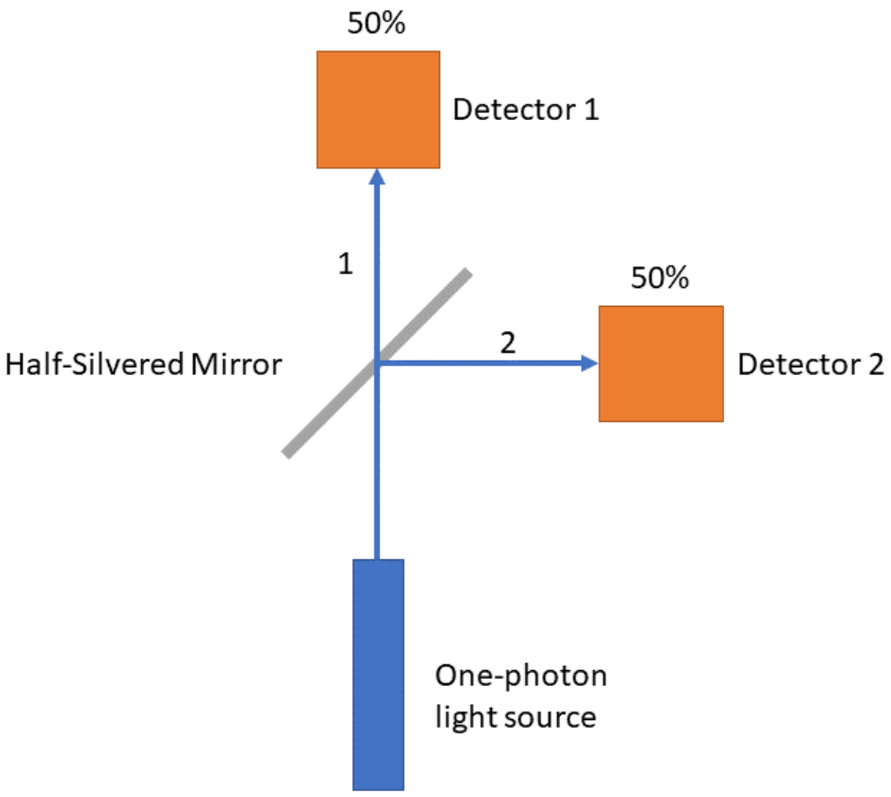
Motivation: (semi-)device-independent QIT

Goal: Generate certified random bits.

Motivation: (semi-)device-independent QIT

Goal: Generate certified random bits.

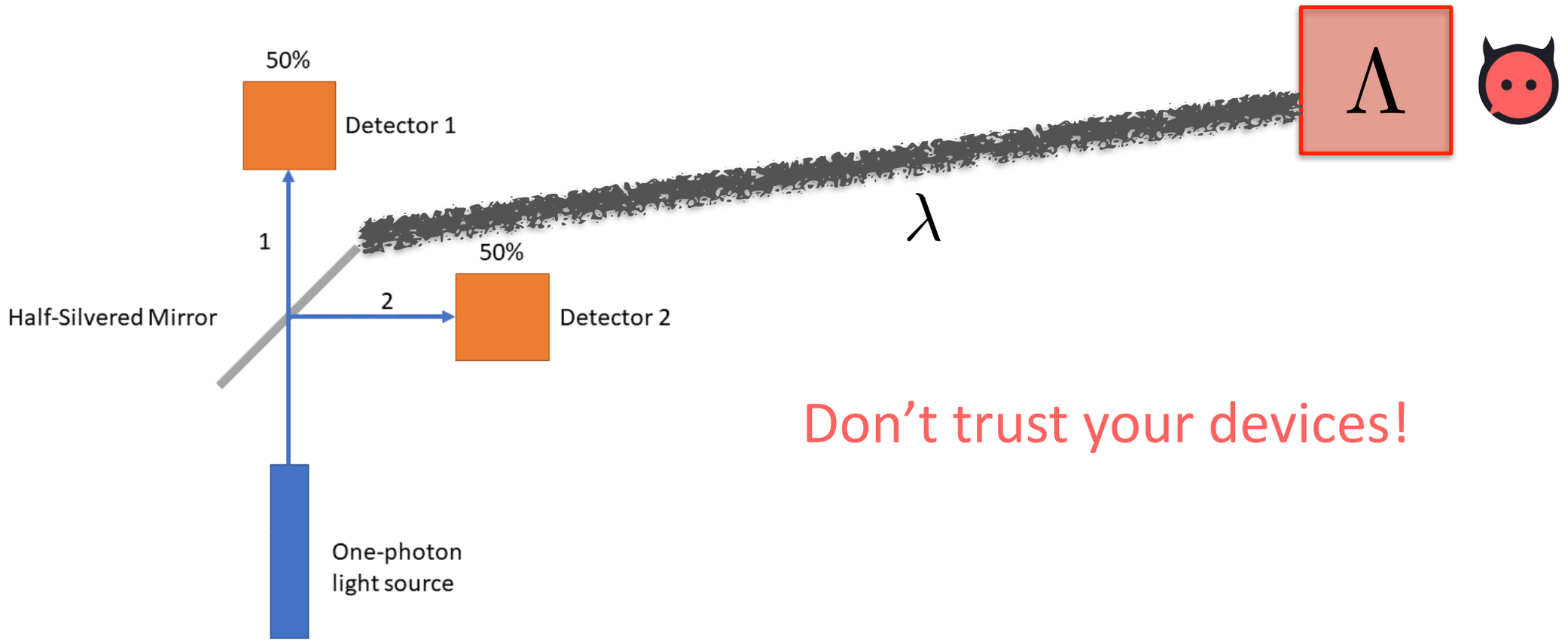
Why not just send single photons on a half-silvered mirror?



Motivation: (semi-)device-independent QIT

Goal: Generate certified random bits.

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

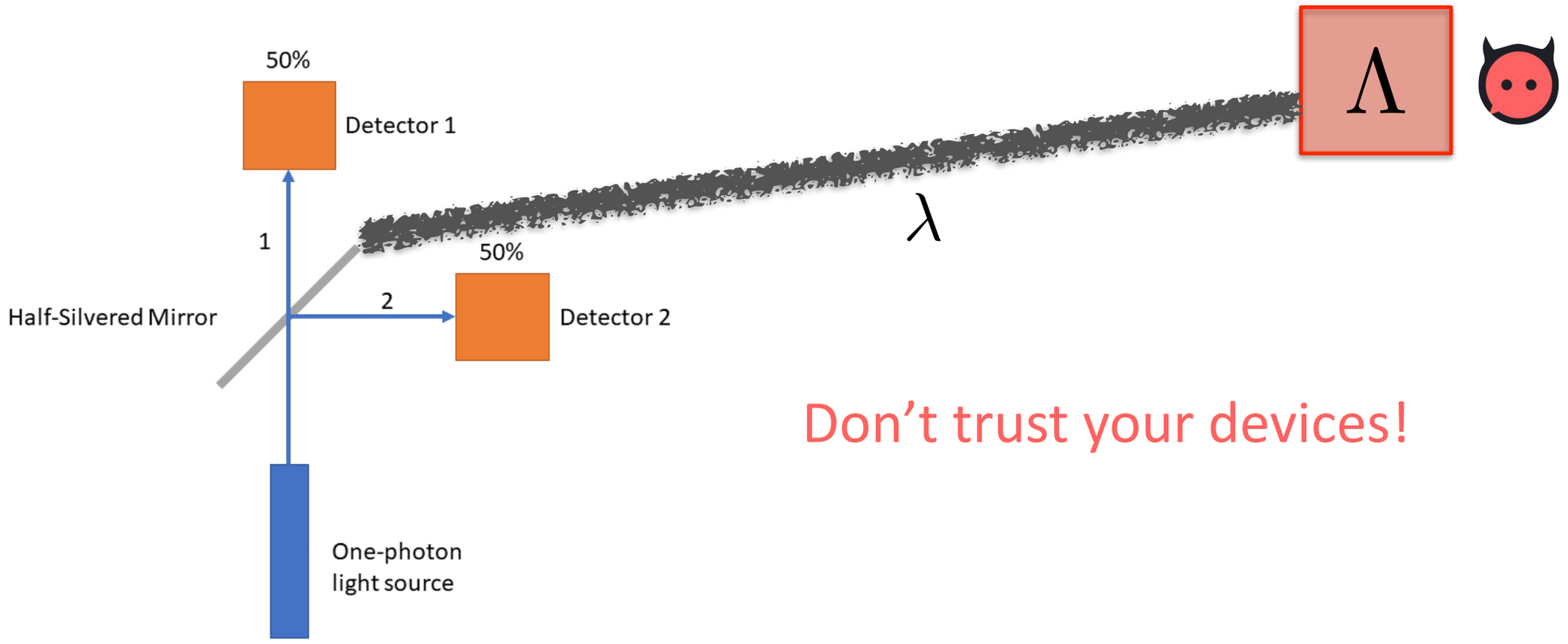


Don’t trust your devices!

Motivation: (semi-)device-independent QIT

Goal: Generate certified random bits.

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



Don’t trust your devices!

Device-independent randomness expansion:

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

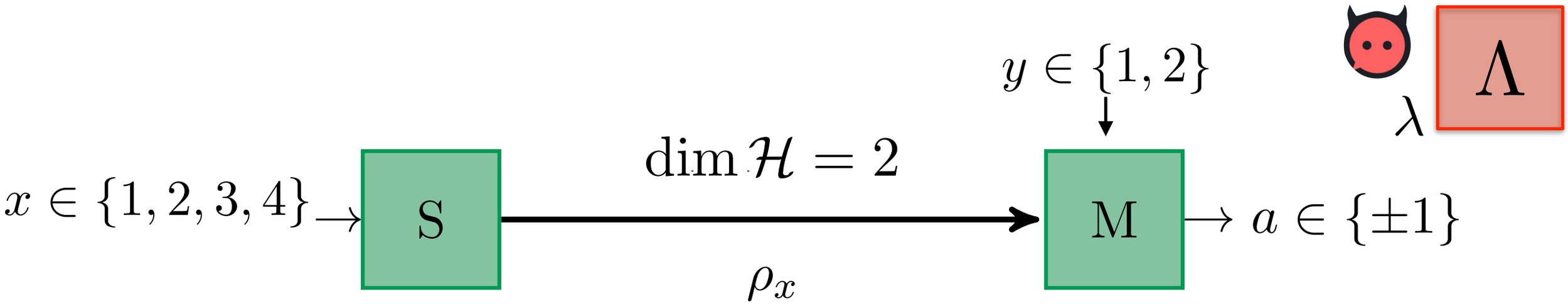
See e.g.: A. Acín, *Randomness and quantum non-locality*, QCRYPT 2012 talk.
V. Scarani, *Bell nonlocality*, Oxford Graduate Texts (2019).

Motivation: (semi-)device-independent QIT

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

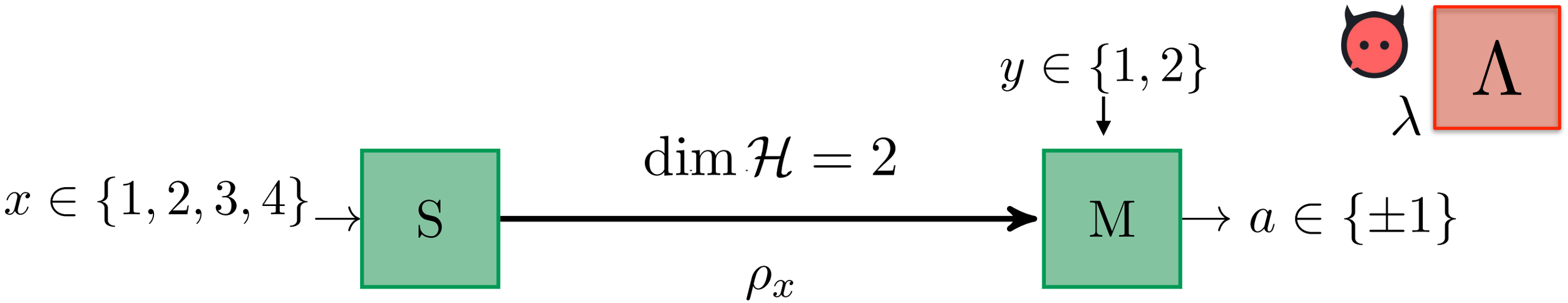
Motivation: (semi-)device-independent QIT

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



Motivation: (semi-)device-independent QIT

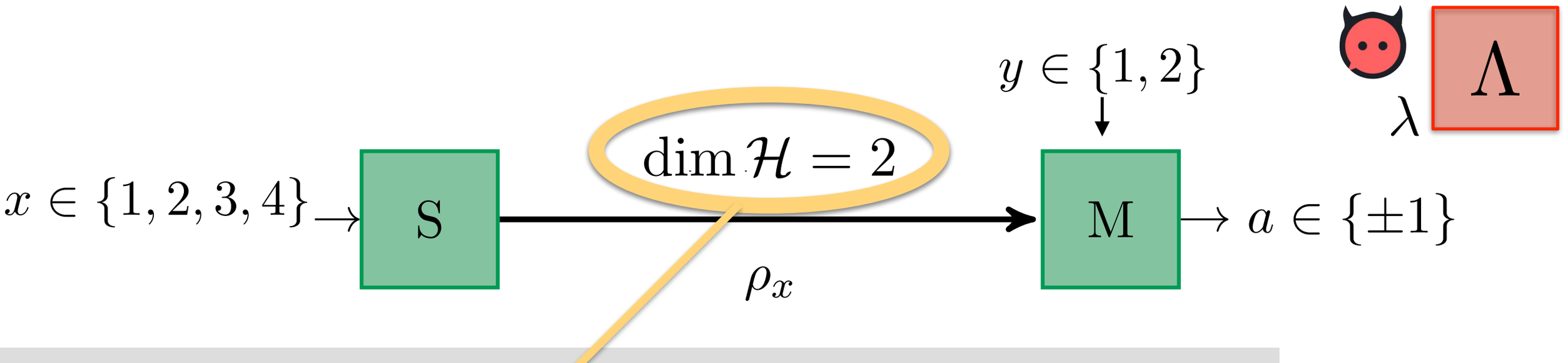
Semi-device-independent (SDI): allow communication, add assumption.



Observed correlations $p(a|x,y)$ imply $H(A|X,Y,\Lambda) \gg 0.$

Motivation: (semi-)device-independent QIT

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

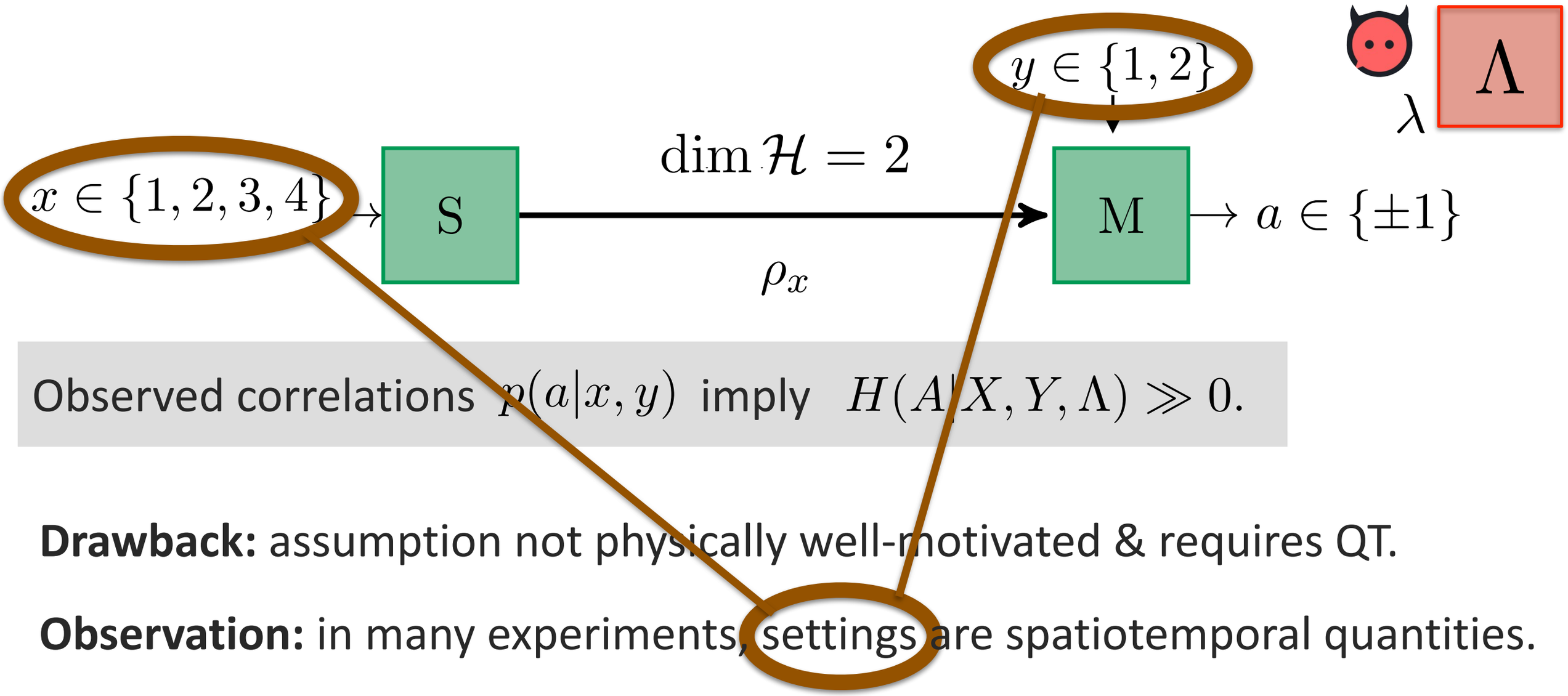


Observed correlations $p(a|x,y)$ imply $H(A|X,Y,\Lambda) \gg 0$.

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

Motivation: (semi-)device-independent QIT

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



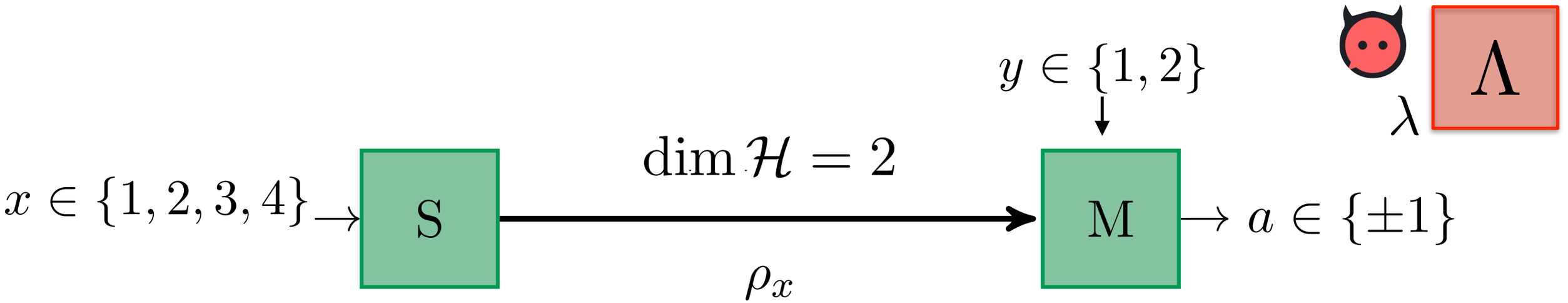
Observed correlations $p(a|x,y)$ imply $H(A|X,Y,\Lambda) \gg 0.$

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

Observation: in many experiments, settings are spatiotemporal quantities.

Motivation: (semi-)device-independent QIT

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



Observed correlations $p(a|x,y)$ imply $H(A|X,Y,\Lambda) \gg 0.$

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

Observation: in many experiments, settings are spatiotemporal quantities.

Idea: use the formalism of rotation boxes; replace dim bound by spin bound.
Slightly more physical; does not assume the validity of quantum theory.

A theory-independent SDI randomness generator

Suppose we only have **two possible** choices of **angles** — say, 0 and α.

A theory-independent SDI randomness generator

Suppose we only have **two possible** choices of **angles** — say, 0 and α.

Gives two probabilities

$$P(+1|x) = \begin{cases} P(+1|0) & \text{if } x = 1 \\ P(+1|\alpha) & \text{if } x = 2. \end{cases}$$

A theory-independent SDI randomness generator

Suppose we only have **two possible** choices of **angles** — say, 0 and α.

Gives two probabilities

$$P(+1|x) = \begin{cases} P(+1|0) & \text{if } x = 1 \\ P(+1|\alpha) & \text{if } x = 2. \end{cases}$$

Equivalently characterized by the correlations $E_x = P(+1|x) - P(-1|x)$

A theory-independent SDI randomness generator

Suppose we only have **two possible** choices of **angles** — say, 0 and α.

Gives two probabilities

$$P(+1|x) = \begin{cases} P(+1|0) & \text{if } x = 1 \\ P(+1|\alpha) & \text{if } x = 2. \end{cases}$$

Equivalently characterized by the correlations $E_x = P(+1|x) - P(-1|x)$

"**Two settings**" quantum and rotation box correlations:

$$\mathcal{Q}_{J,\alpha} = \{(E_1, E_2) \mid P \in \mathcal{Q}_J\}$$
$$\mathcal{R}_{J,\alpha} = \{(E_1, E_2) \mid P \in \mathcal{R}_J\}$$

(Recall $\mathcal{Q}_J \subsetneq \mathcal{R}_J$ for $J \geq 3/2$)

A theory-independent SDI randomness generator

Suppose we only have **two possible** choices of **angles** — say, 0 and α.

Gives two probabilities

$$P(+1|x) = \begin{cases} P(+1|0) & \text{if } x = 1 \\ P(+1|\alpha) & \text{if } x = 2. \end{cases}$$

Equivalently characterized by the correlations $E_x = P(+1|x) - P(-1|x)$

"**Two settings**" quantum and rotation box correlations:

$$\mathcal{Q}_{J,\alpha} = \{(E_1, E_2) \mid P \in \mathcal{Q}_J\}$$
$$\mathcal{R}_{J,\alpha} = \{(E_1, E_2) \mid P \in \mathcal{R}_J\}$$

(Recall $\mathcal{Q}_J \subsetneq \mathcal{R}_J$ for $J \geq 3/2$)

Theorem: $\mathcal{Q}_{J,\alpha} = \mathcal{R}_{J,\alpha}$ for all J, α.

A theory-independent SDI randomness generator

Suppose we only have **two possible** choices of **angles** — say, 0 and α.

Gives two probabilities

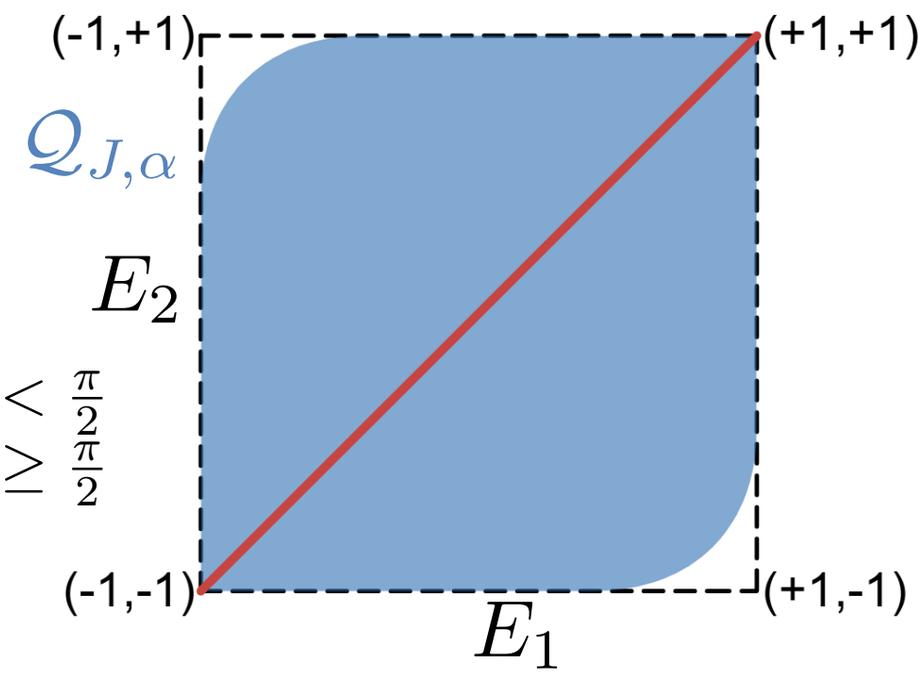
$$P(+1|x) = \begin{cases} P(+1|0) & \text{if } x = 1 \\ P(+1|\alpha) & \text{if } x = 2. \end{cases}$$

Equivalently characterized by the correlations $E_x = P(+1|x) - P(-1|x)$

"**Two settings**" quantum and rotation box correlations:

$$\mathcal{Q}_{J,\alpha} = \{(E_1, E_2) \mid P \in \mathcal{Q}_J\}$$
$$\mathcal{R}_{J,\alpha} = \{(E_1, E_2) \mid P \in \mathcal{R}_J\}$$

(Recall $\mathcal{Q}_J \subsetneq \mathcal{R}_J$ for $J \geq 3/2$)



Theorem: $\mathcal{Q}_{J,\alpha} = \mathcal{R}_{J,\alpha}$ for all J, α.

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

A theory-independent SDI randomness generator

Suppose we only have **two possible** choices of **angles** — say, 0 and α.

Gives two probabilities

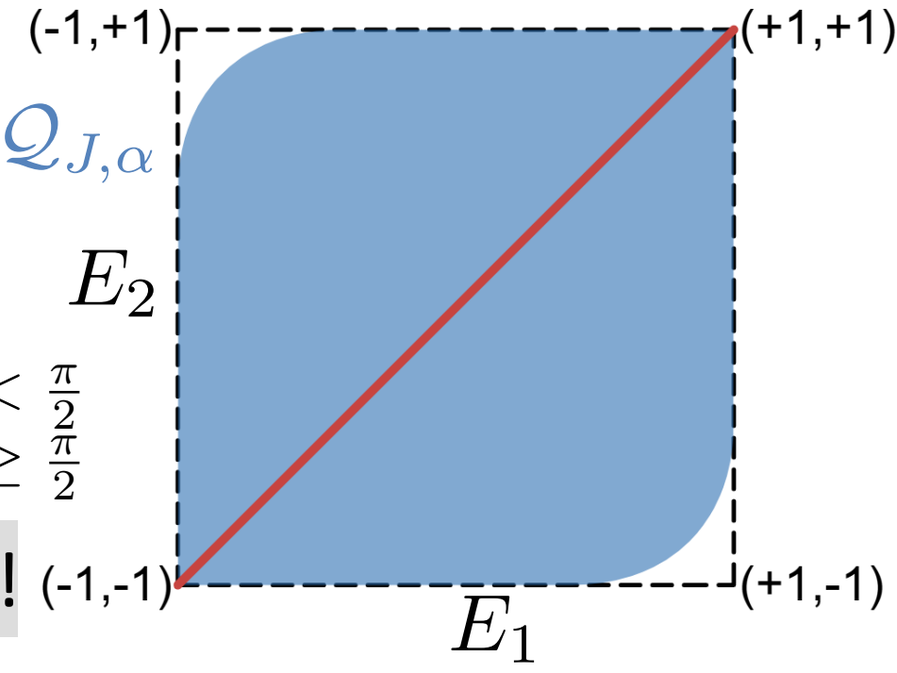
$$P(+1|x) = \begin{cases} P(+1|0) & \text{if } x = 1 \\ P(+1|\alpha) & \text{if } x = 2. \end{cases}$$

Equivalently characterized by the correlations $E_x = P(+1|x) - P(-1|x)$

"**Two settings**" quantum and rotation box correlations:

$$\mathcal{Q}_{J,\alpha} = \{(E_1, E_2) \mid P \in \mathcal{Q}_J\}$$
$$\mathcal{R}_{J,\alpha} = \{(E_1, E_2) \mid P \in \mathcal{R}_J\}$$

(Recall $\mathcal{Q}_J \subsetneq \mathcal{R}_J$ for $J \geq 3/2$)



Theorem: $\mathcal{Q}_{J,\alpha} = \mathcal{R}_{J,\alpha}$ for all J, α.

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

Correlations characterized by rotational symmetry!

A theory-independent SDI randomness generator

Main proof ingredient:

Thm. 1.1]: If T is a trigonometric polynomial of degree n with $-1 \leq T(x) \leq 1 \; \forall x$, then

$$T'(x)^2 + n^2 T(x)^2 \leq n^2. \tag{17}$$

A theory-independent SDI randomness generator

Main proof ingredient:

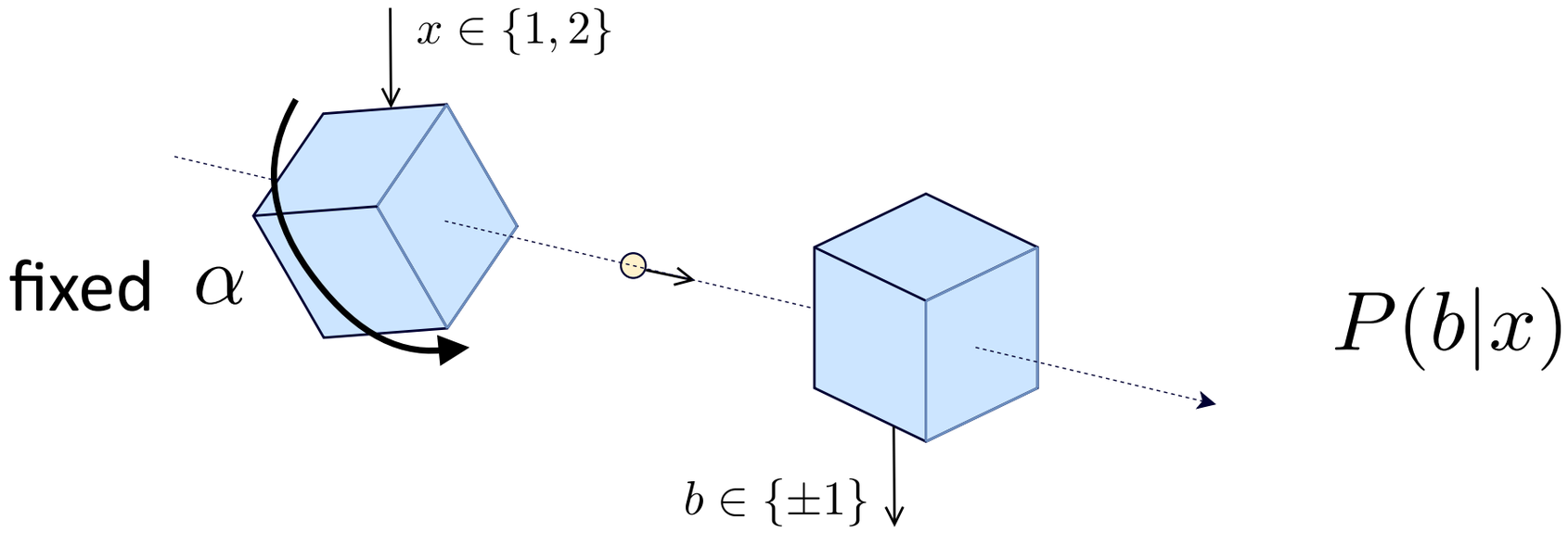
Thm. 1.1]: If T is a trigonometric polynomial of degree n with $-1 \leq T(x) \leq 1 \; \forall x$, then

$$T'(x)^2 + n^2 T(x)^2 \leq n^2. \tag{17}$$

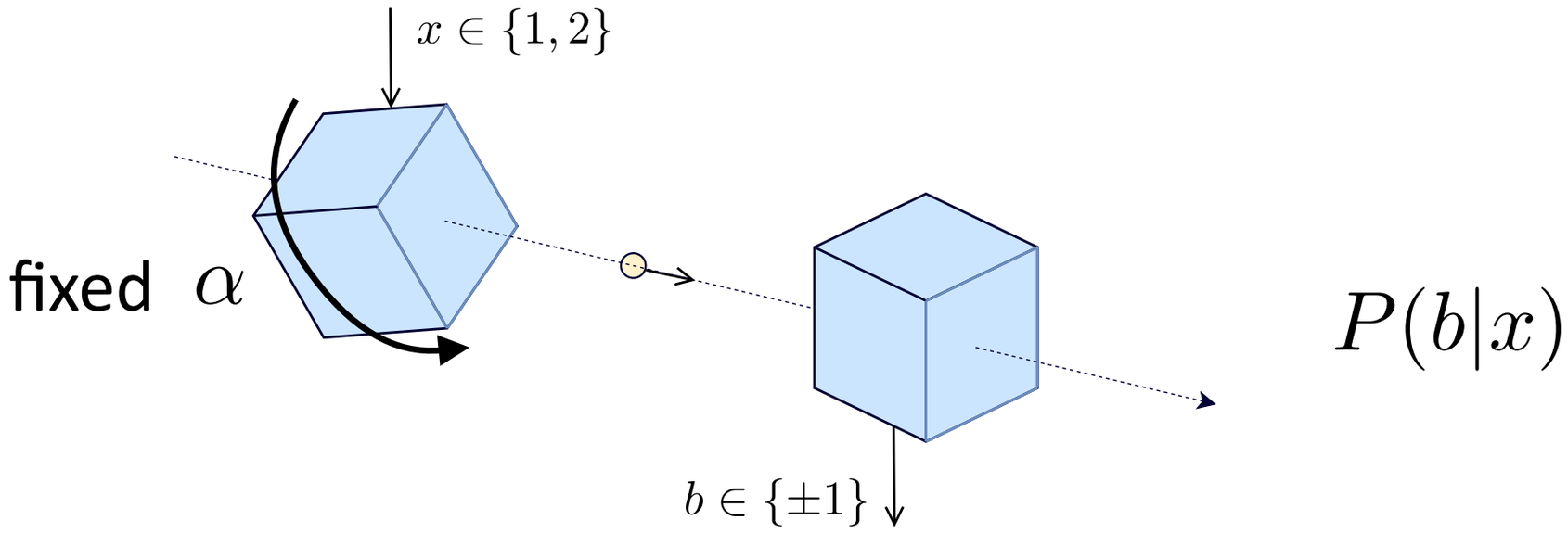
This is sufficient to reproduce the quantum boundary for all *J*:

$$\begin{aligned}
\alpha_\varepsilon = \int_0^{\alpha_\varepsilon} d\alpha &\geq \int_0^{\alpha_\varepsilon} \frac{T'(\alpha) d\alpha}{2J\sqrt{1 - T(\alpha)^2}} \\
&= \frac{1}{2J} \int_{E_x}^{E_{x'}} \frac{dy}{\sqrt{1-y^2}} \\
&= \frac{1}{2J} \left(\arcsin E_{x'} - \arcsin E_x \right)
\end{aligned}$$

A theory-independent SDI randomness generator



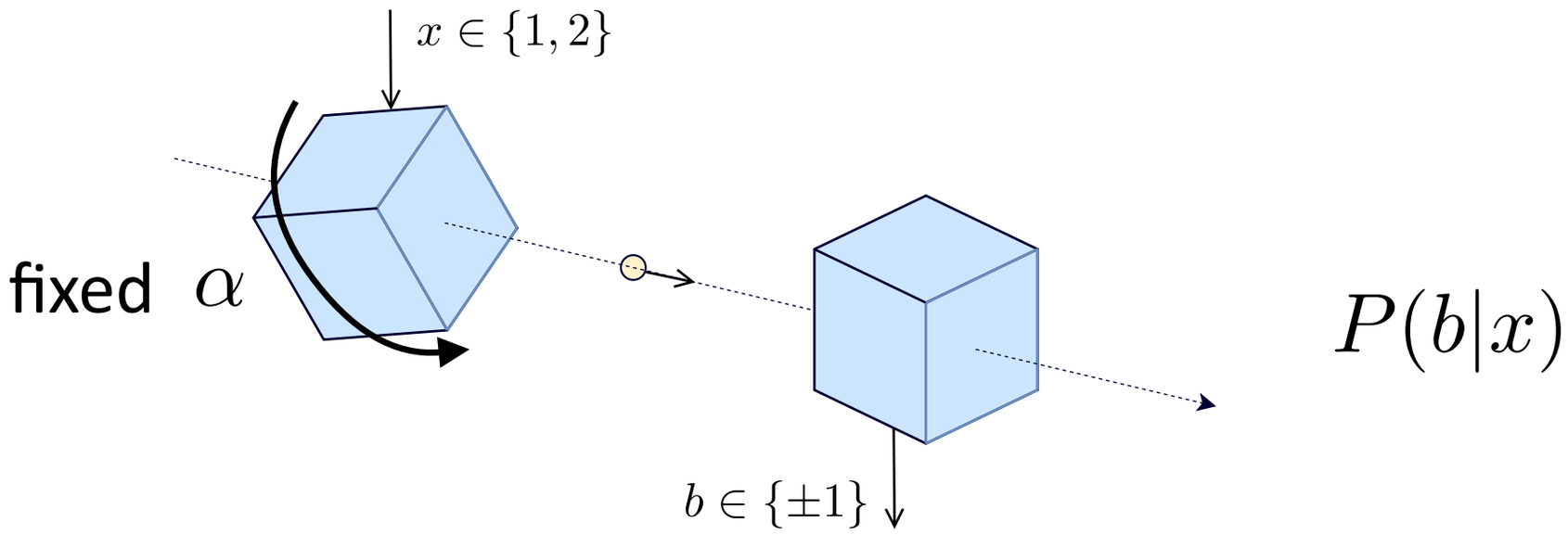
A theory-independent SDI randomness generator



If input is x=1: do nothing to preparation device;

if x=2: **rotate it** (relative to measurement device) **by angle α**.

A theory-independent SDI randomness generator



If input is x=1: do nothing to preparation device;

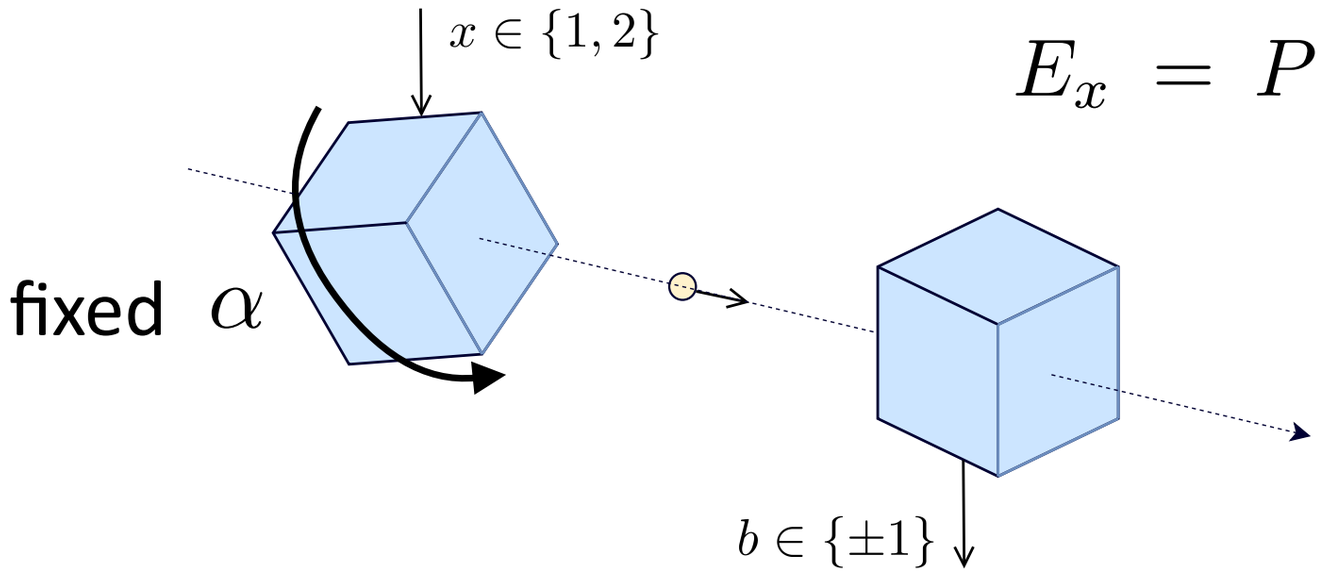
if x=2: **rotate it** (relative to measurement device) **by angle α**.

SDI assumption: "spin" of system ≤ **J**

No further assumptions on devices / system.

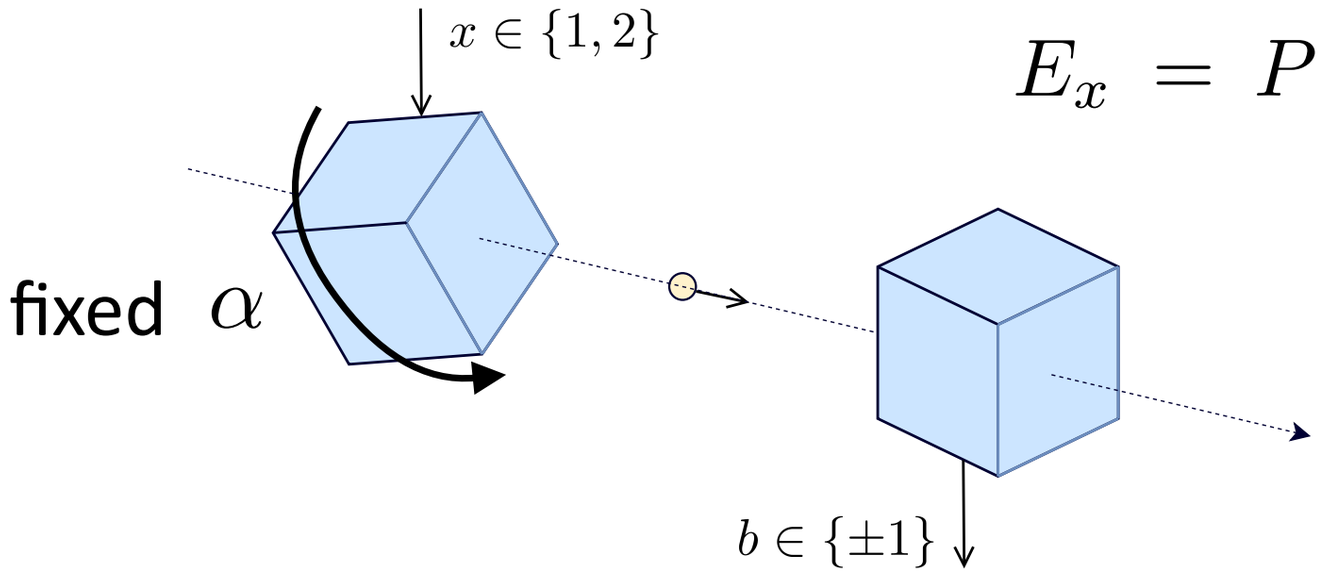
Do not need to assume the validity of quantum theory.

A theory-independent SDI randomness generator

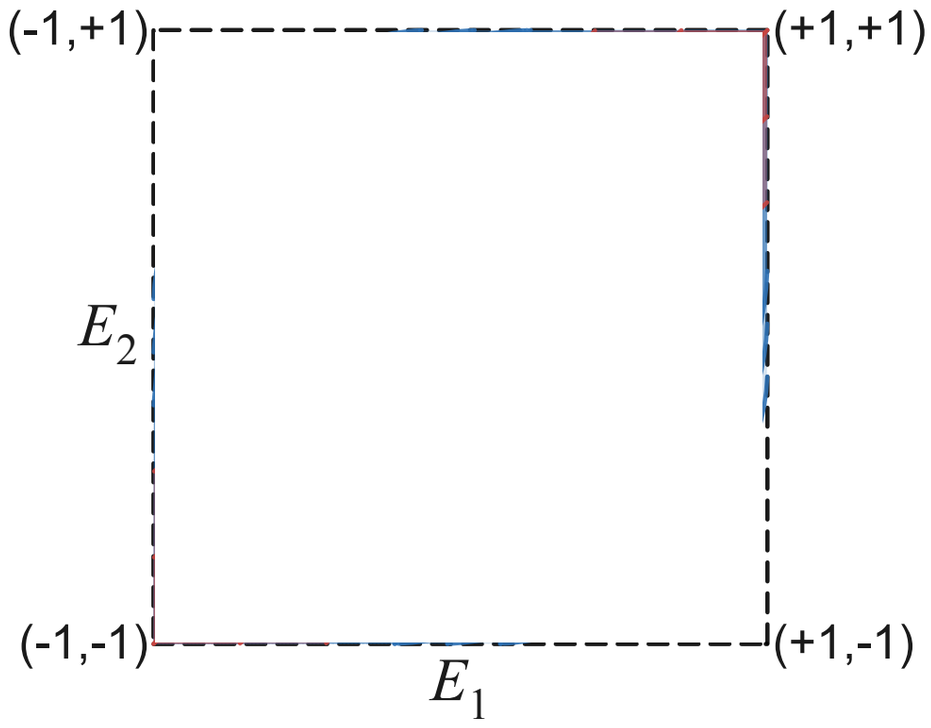


$$E_x \;=\; P(+1|x) \;-\; P(-1|x)$$

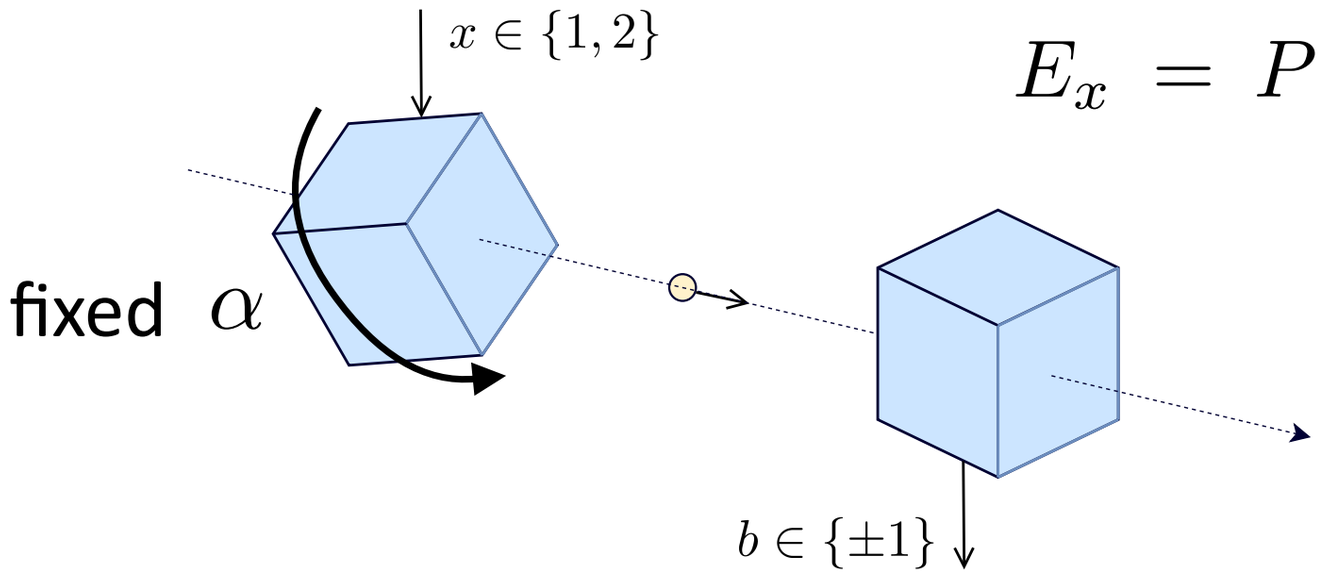
A theory-independent SDI randomness generator



$$E_x \;=\; P(+1|x) \,-\, P(-1|x)$$

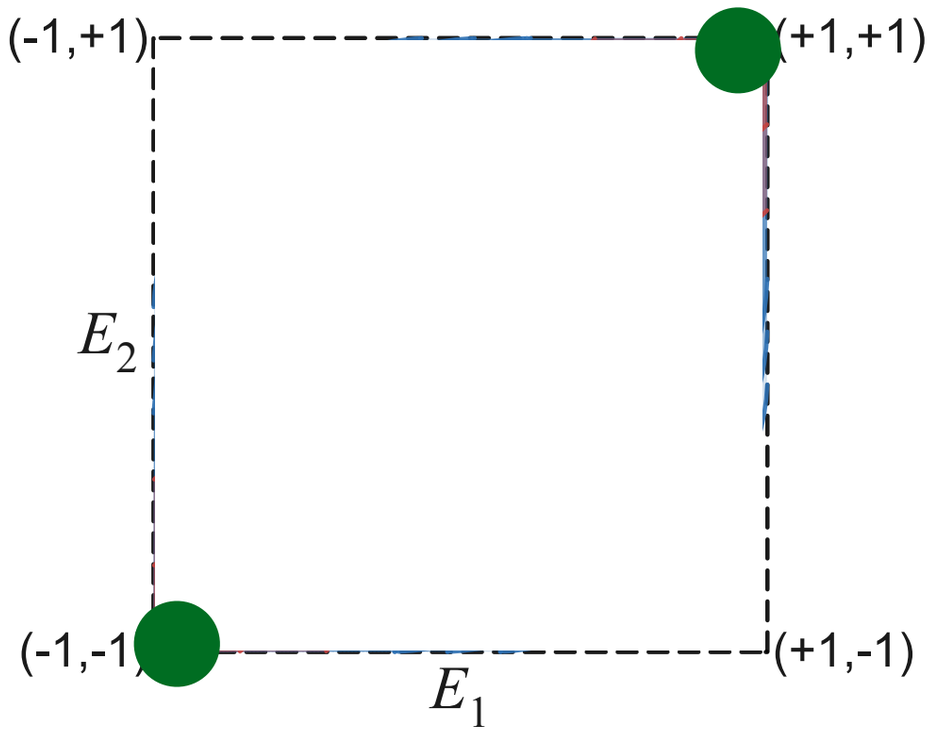


A theory-independent SDI randomness generator

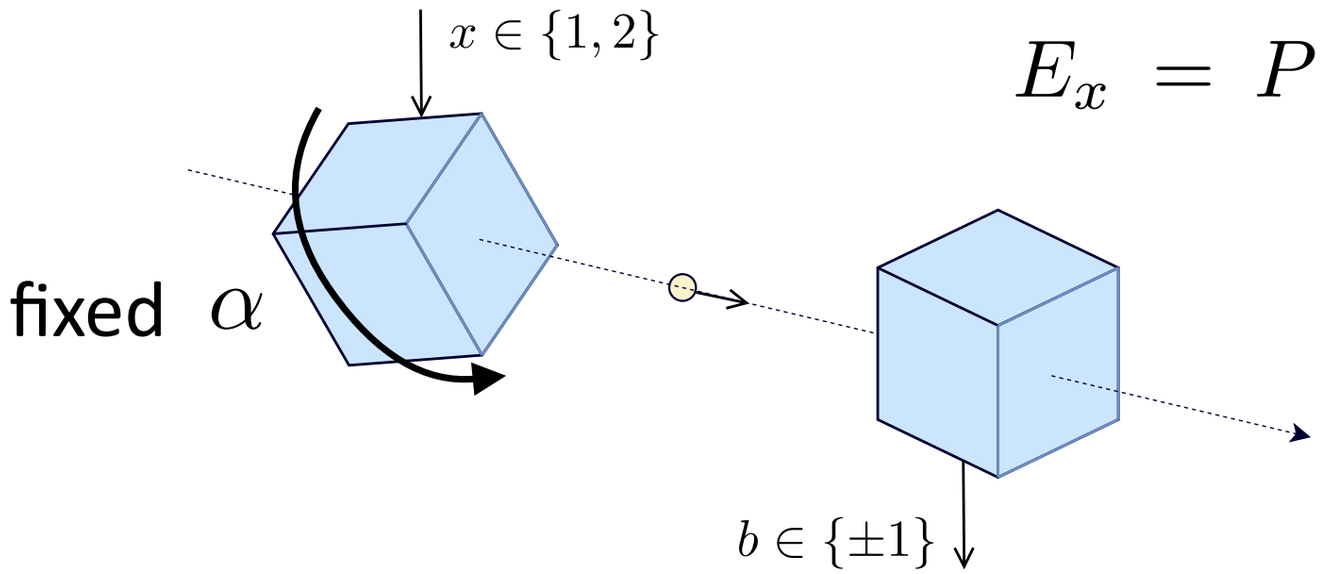


$$E_x \;=\; P(+1|x) \,-\, P(-1|x)$$

- "Boring" deterministic correlations: outcome *b* independent of *x*



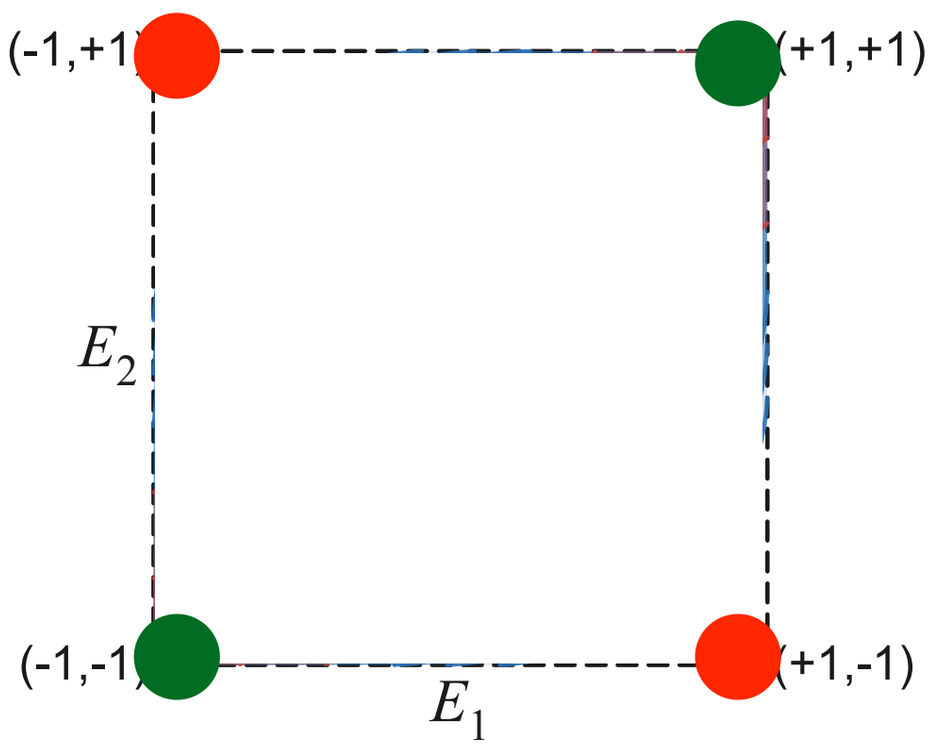
A theory-independent SDI randomness generator



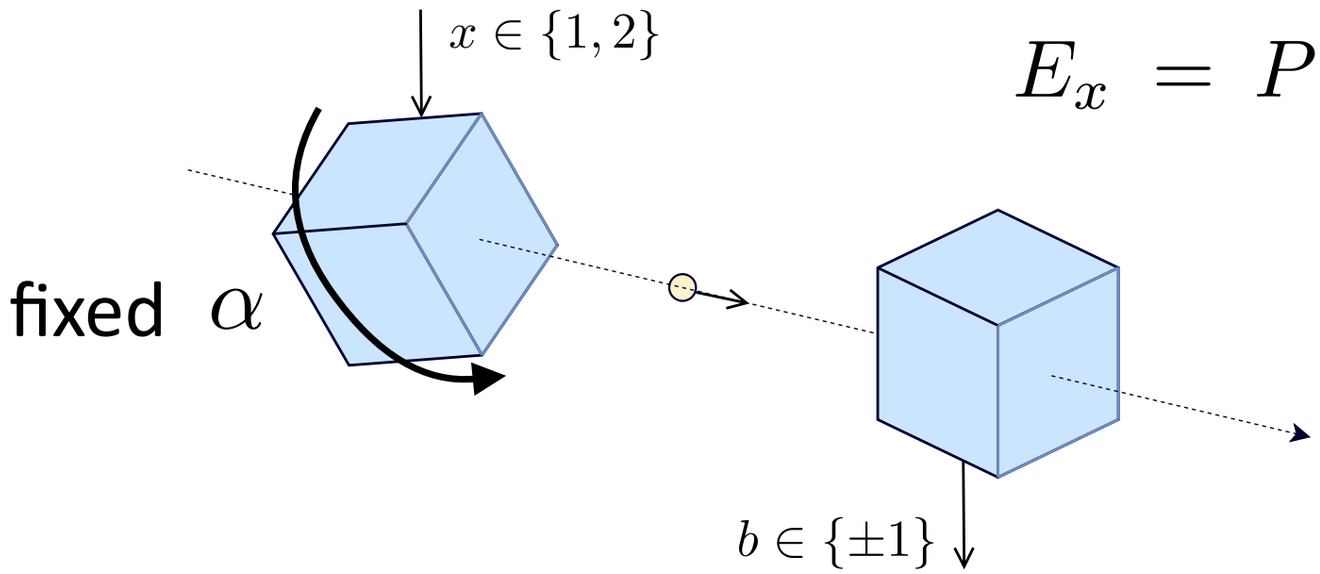
$$E_x \;=\; P(+1|x) \;-\; P(-1|x)$$

- "Boring" deterministic correlations: outcome *b* independent of *x*

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



A theory-independent SDI randomness generator



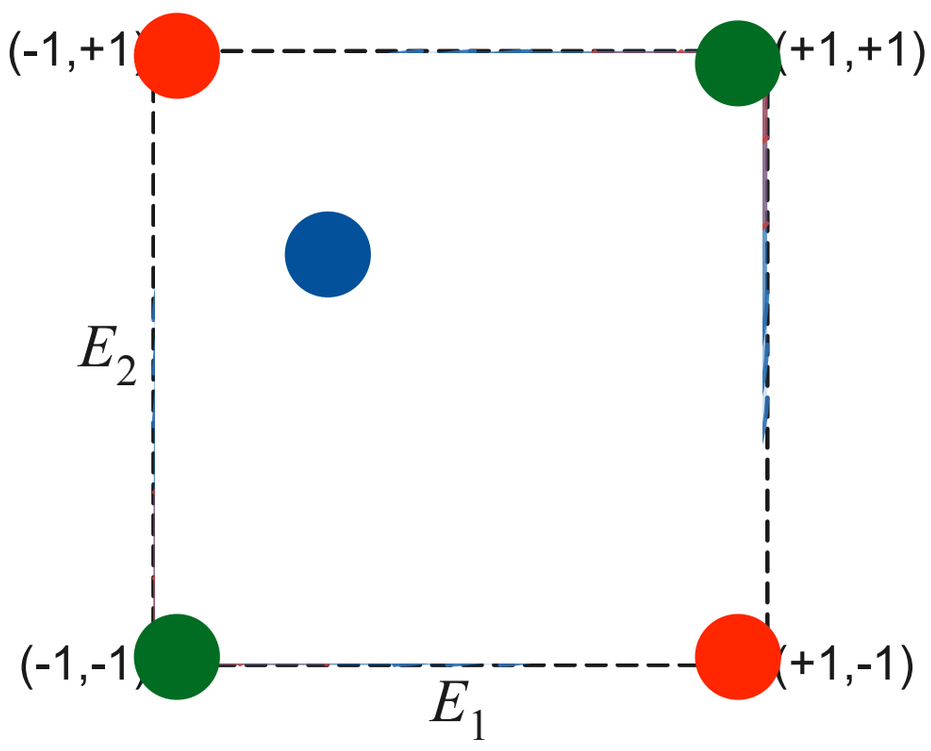
$$E_x \;=\; P(+1|x) \,-\, P(-1|x)$$

- "Boring" deterministic correlations: outcome *b* independent of *x*

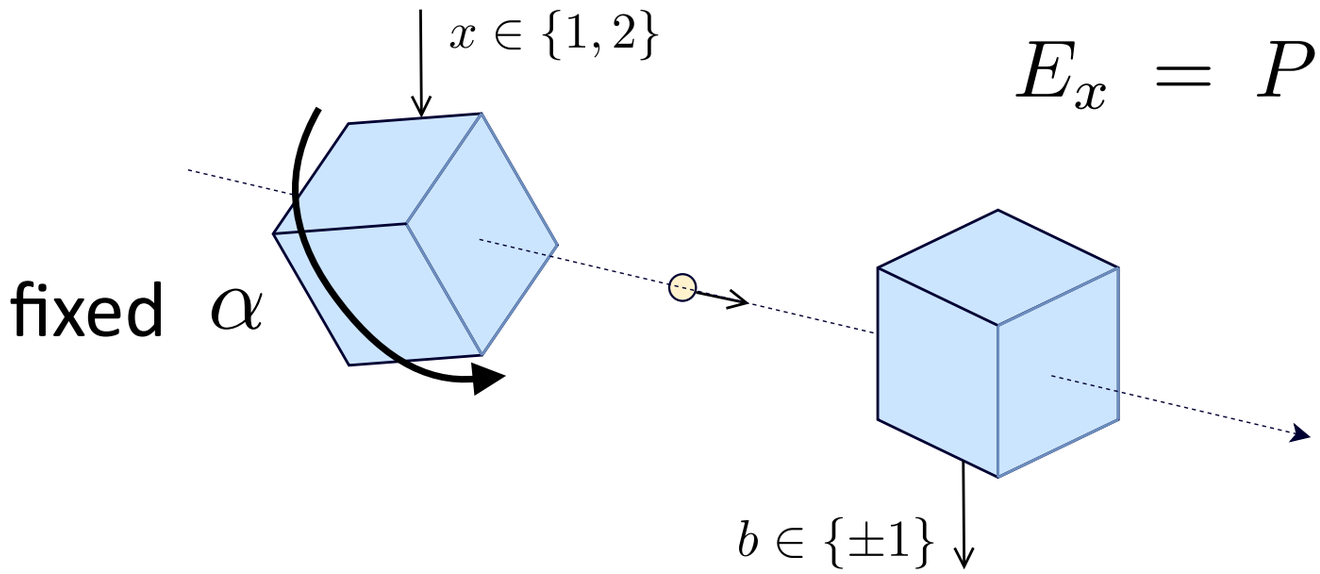
- "Interesting" deterministic correlations: outcome *b* is a function of *x*

Suppose (E_1, E_2) observed. Looks random.

But:



A theory-independent SDI randomness generator



$$E_x \;=\; P(+1|x) \,-\, P(-1|x)$$

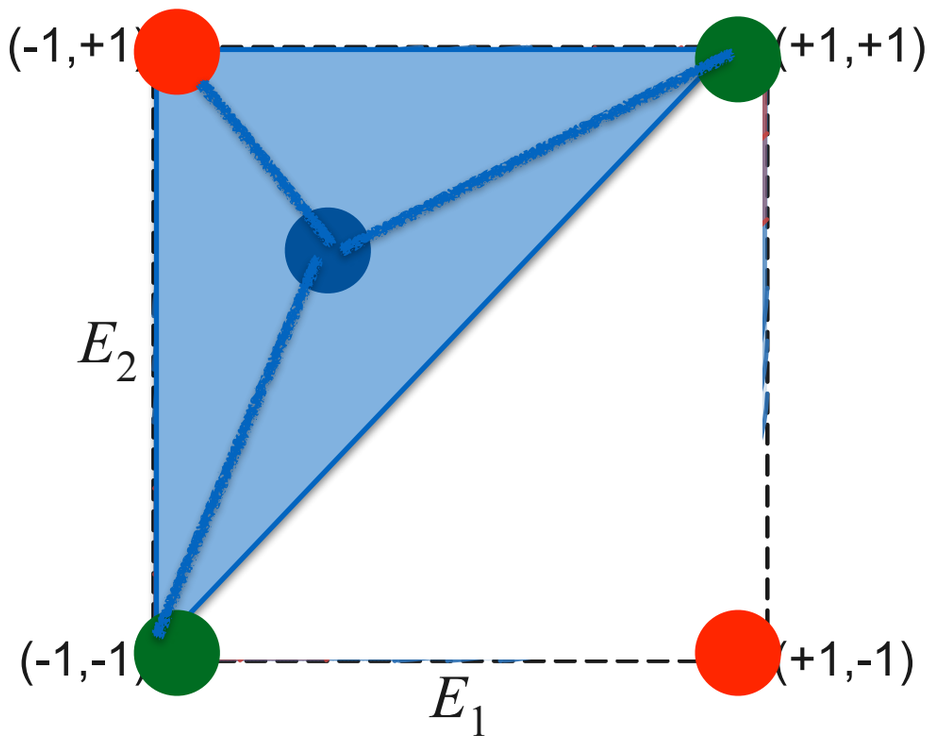
- "Boring" deterministic correlations: outcome *b* independent of *x*

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

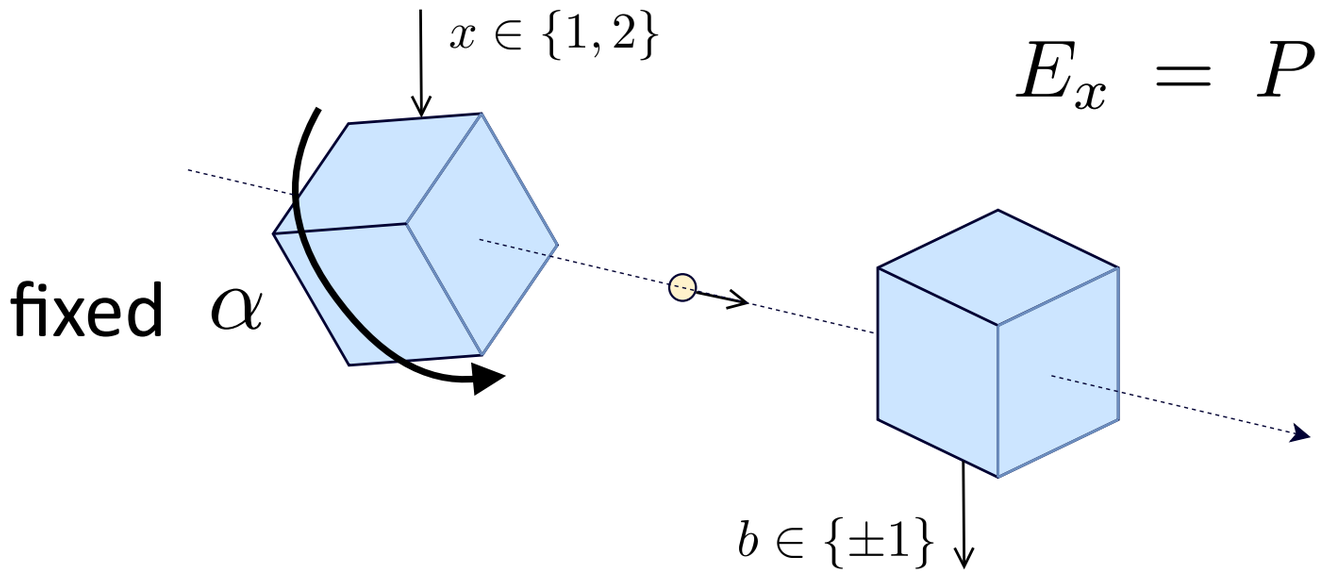
Suppose (E_1, E_2) observed. Looks random.

But:

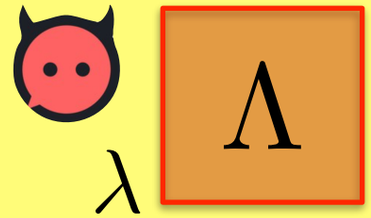
$$(E_1, E_2) = \sum_\lambda p(\lambda)(E_1^{(\lambda)}, E_2^{(\lambda)})_{\rm det}$$



A theory-independent SDI randomness generator



$$E_x \;=\; P(+1|x) \,-\, P(-1|x)$$



Can predict outcome!

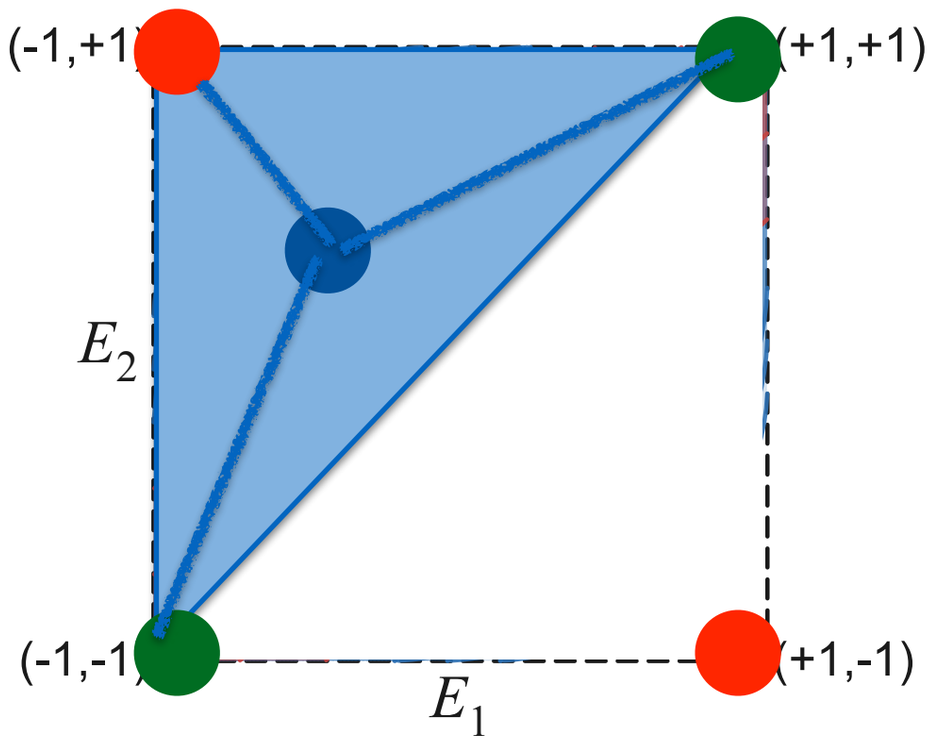
- "Boring" deterministic correlations: outcome *b* independent of *x*

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

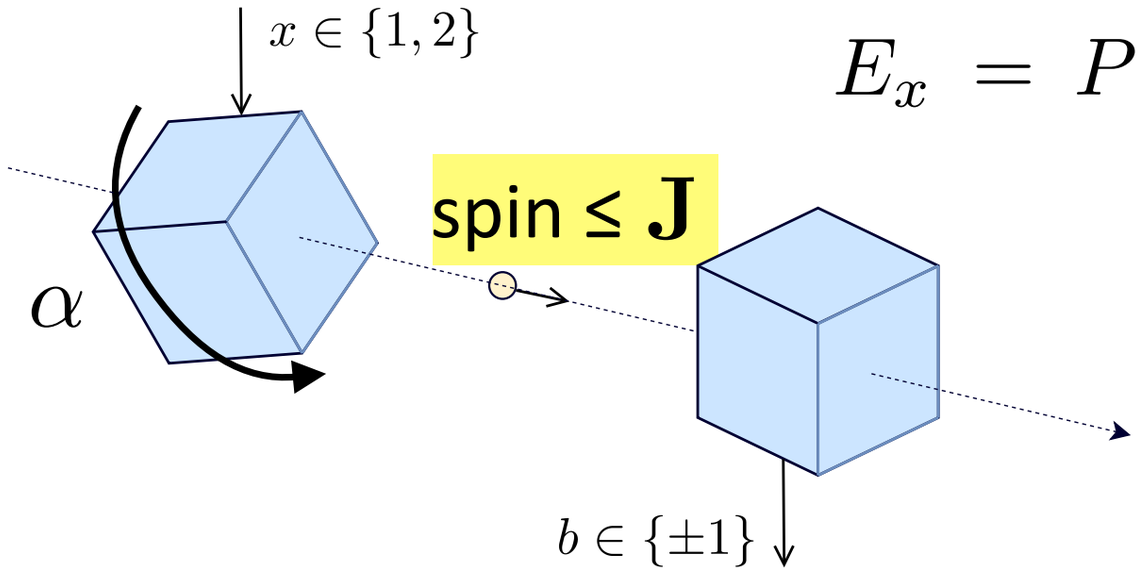
Suppose (E_1, E_2) observed. Looks random.

But:

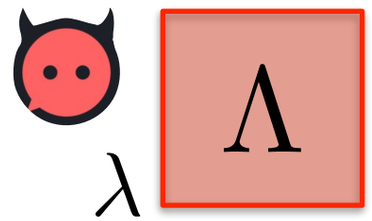
$$(E_1, E_2) = \sum_{\lambda} p(\lambda)(E_1^{(\lambda)}, E_2^{(\lambda)})_{\text{det}}$$



A theory-independent SDI randomness generator

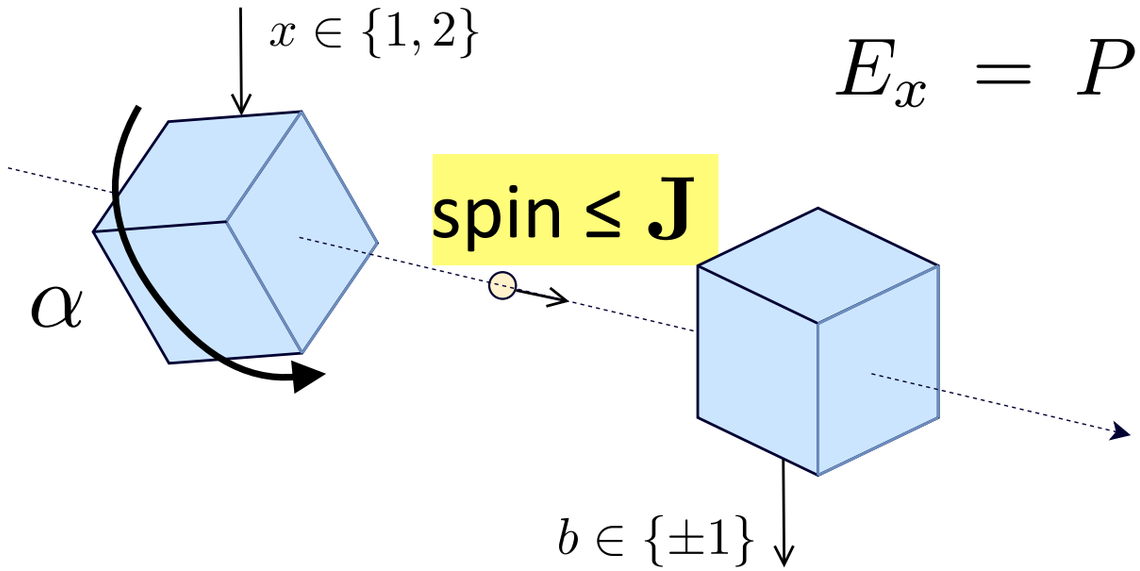


$$E_x = P(+1|x) - P(-1|x)$$

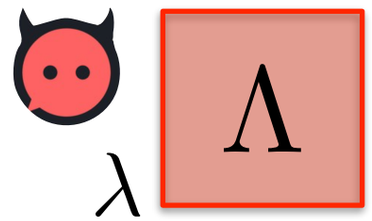


Which correlations are possible?

A theory-independent SDI randomness generator



$$E_x \;=\; P(+1|x) \,-\, P(-1|x)$$



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

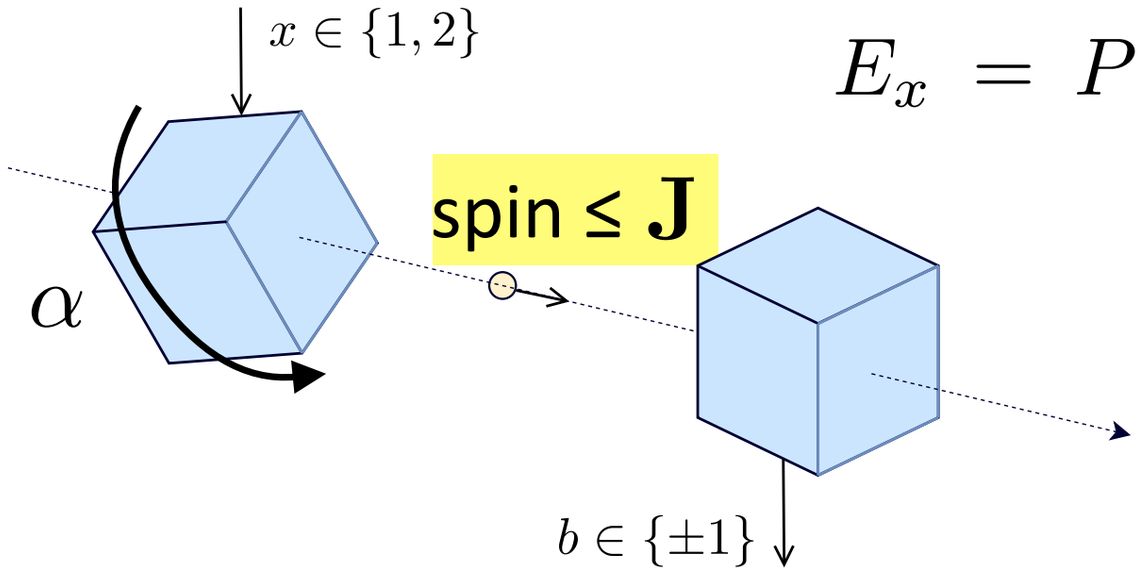
$$\frac{1}{2}\left(\sqrt{1+E_1}\sqrt{1+E_2}+\sqrt{1-E_1}\sqrt{1-E_2}\right) \geq \begin{cases} \cos(J\alpha) & \text{if } |J\alpha| < \frac{\pi}{2} \\ 0 & \text{if } |J\alpha| \geq \frac{\pi}{2} \end{cases}$$

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

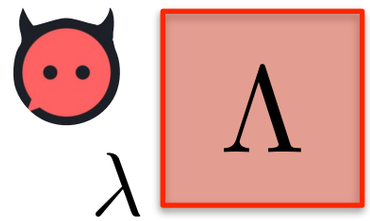
using results of

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

A theory-independent SDI randomness generator

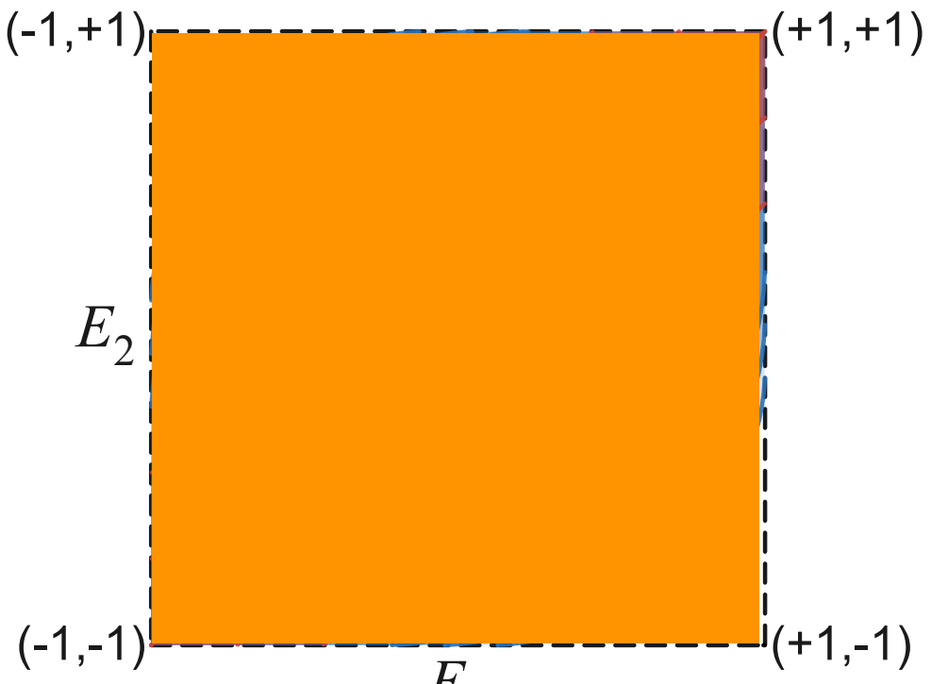


$$E_x \;=\; P(+1|x) \,-\, P(-1|x)$$



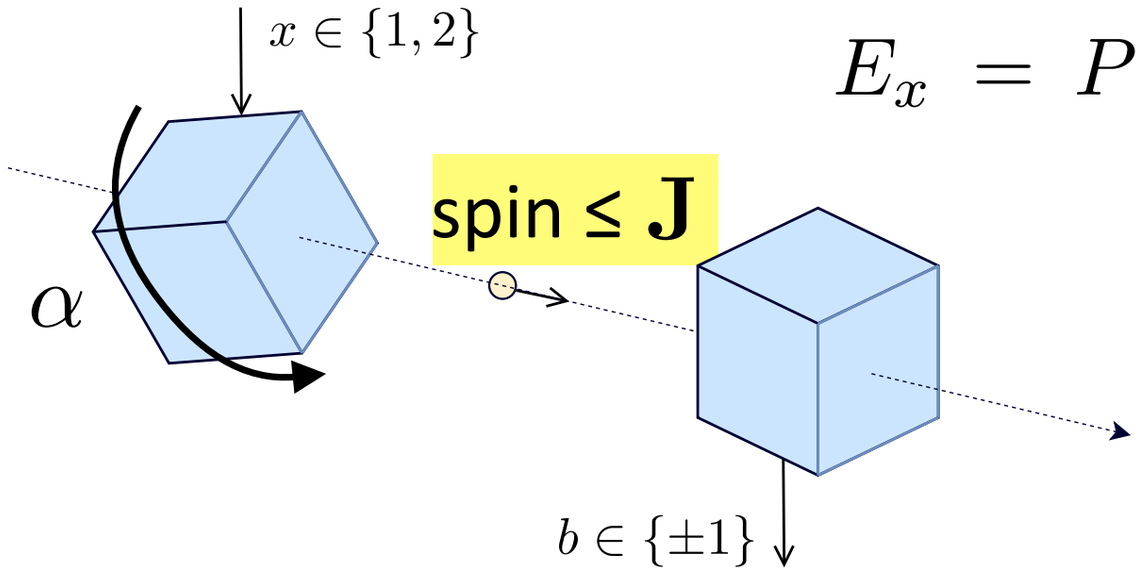
Which correlations are possible? **Theorem:** exactly those:

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

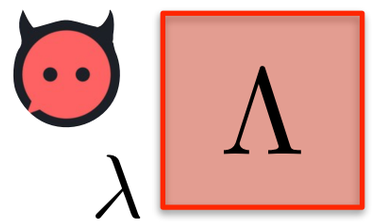


Angle $\alpha \geq \pi/(2J)$:
no certifiable randomness.

A theory-independent SDI randomness generator

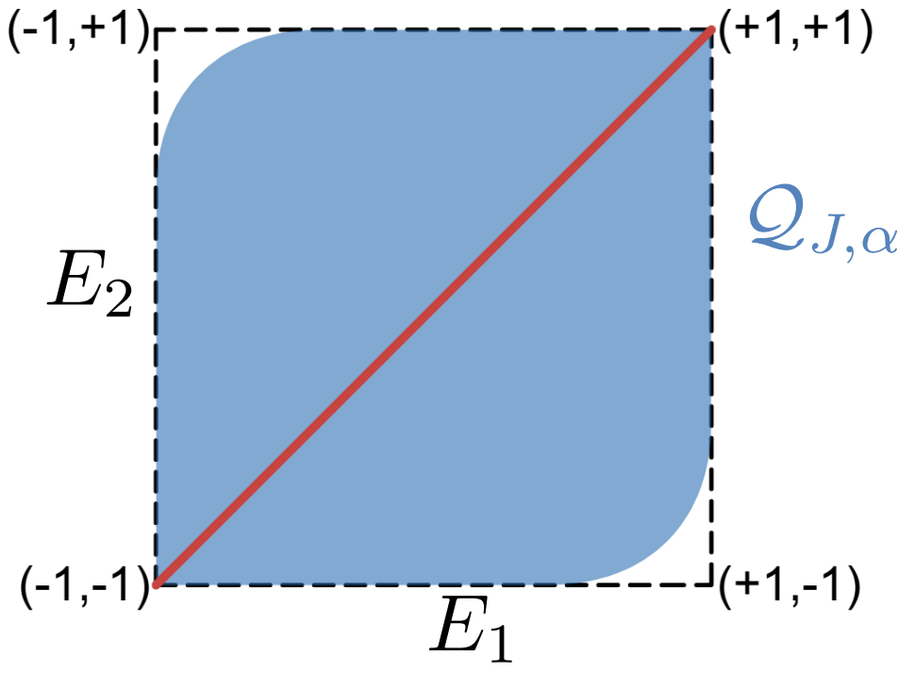


$$E_x \;=\; P(+1|x) \,-\, P(-1|x)$$



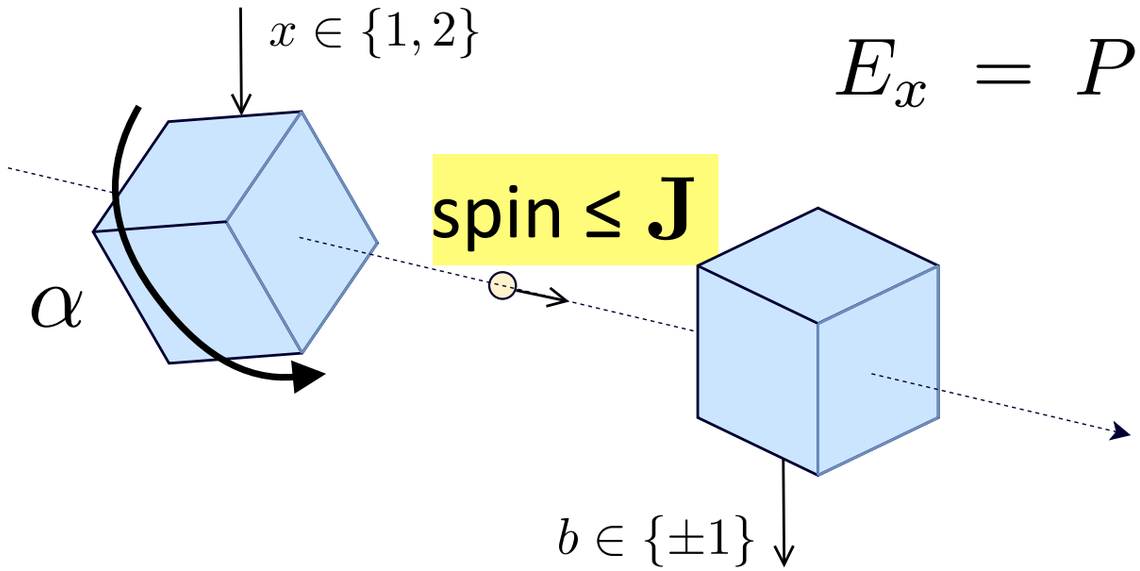
Which correlations are possible? **Theorem:** exactly those:

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

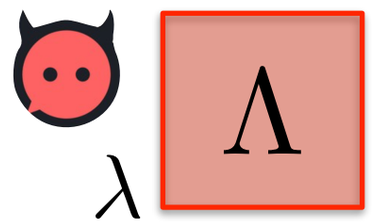


Blue curved set of correlations.

A theory-independent SDI randomness generator

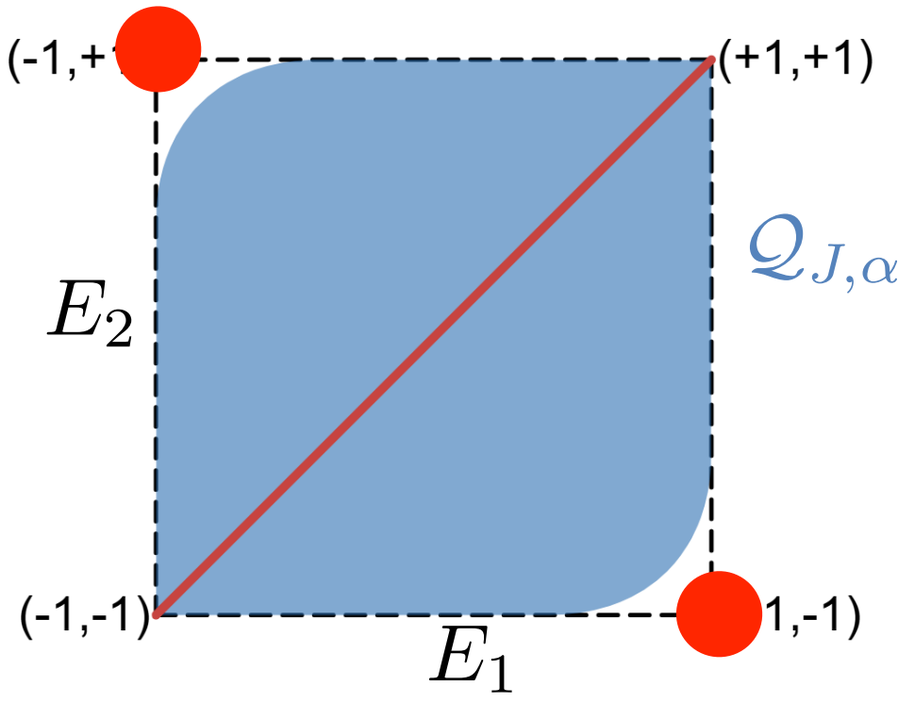


$$E_x \;=\; P(+1|x) \,-\, P(-1|x)$$



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

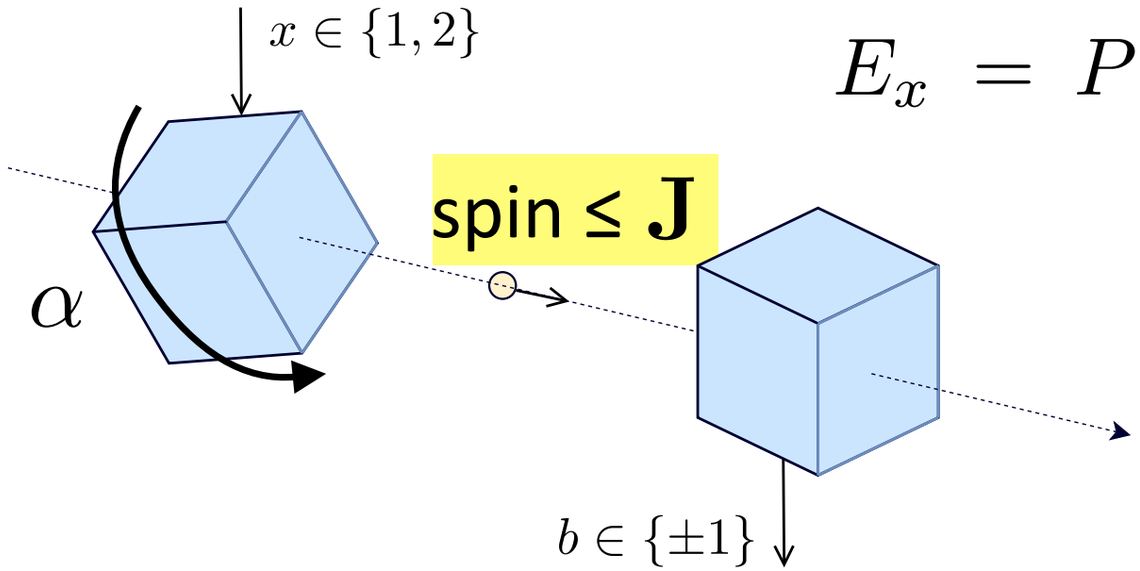
$$\frac{1}{2}\left(\sqrt{1+E_1}\sqrt{1+E_2}+\sqrt{1-E_1}\sqrt{1-E_2}\right) \geq \begin{cases} \cos(J\alpha) & \text{if } |J\alpha| < \frac{\pi}{2} \\ 0 & \text{if } |J\alpha| \geq \frac{\pi}{2} \end{cases}$$



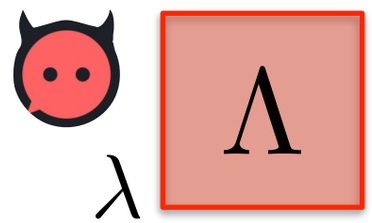
Blue curved set of correlations.

If $|\alpha| < \pi/(2J)$, then the "interesting deterministic correlations" are forbidden…

A theory-independent SDI randomness generator

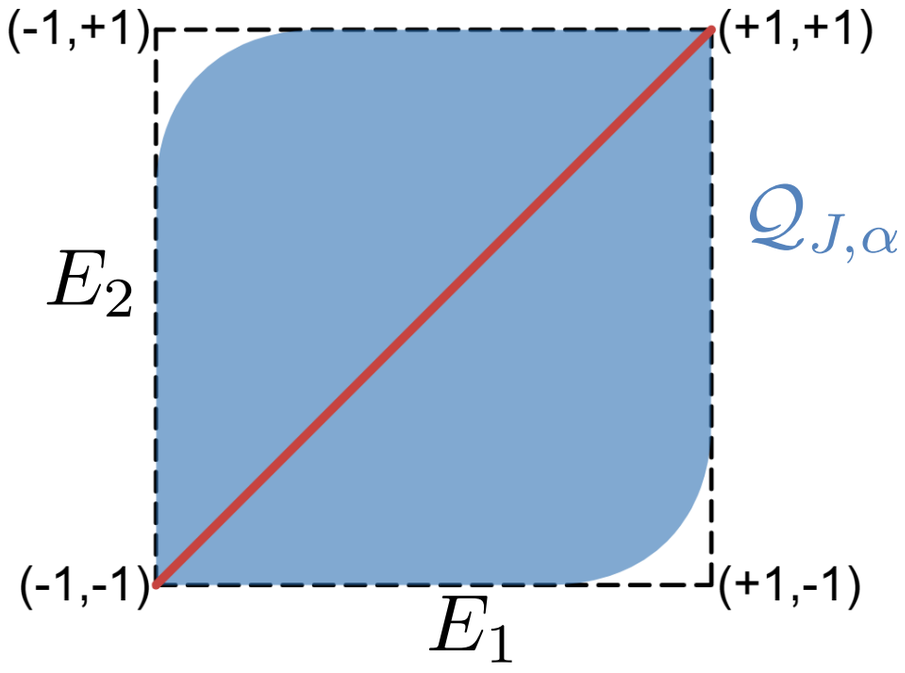


$$E_x \;=\; P(+1|x) \,-\, P(-1|x)$$



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

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

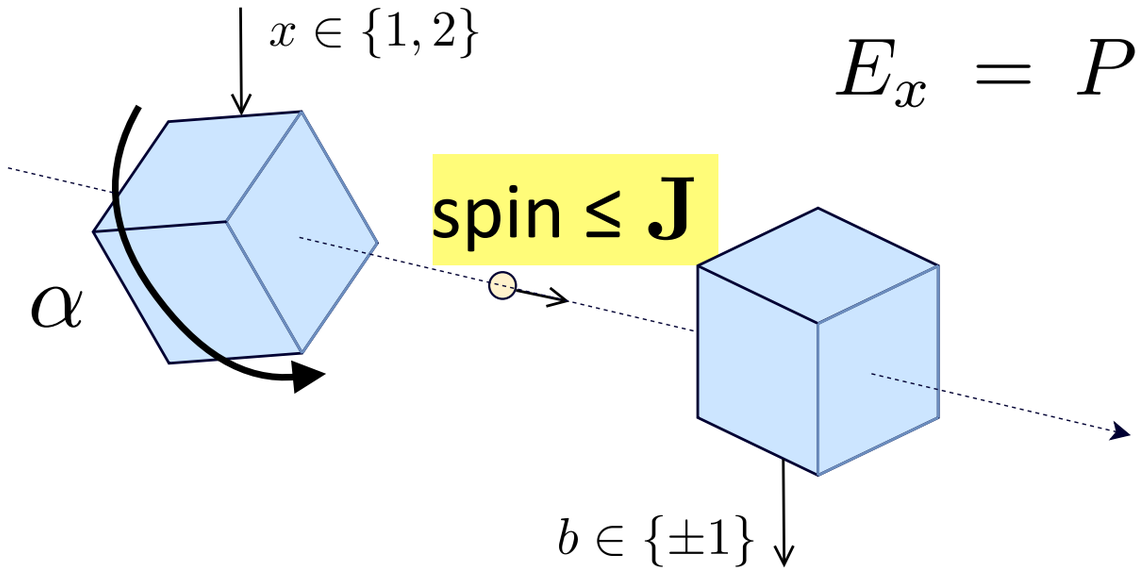


Blue curved set of correlations.

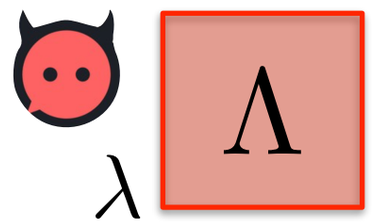
If $|\alpha| < \pi/(2J)$, then the "interesting deterministic correlations" are forbidden…

… and only correlations on the red line admit perfect outcome prediction by eavesdropper.

A theory-independent SDI randomness generator

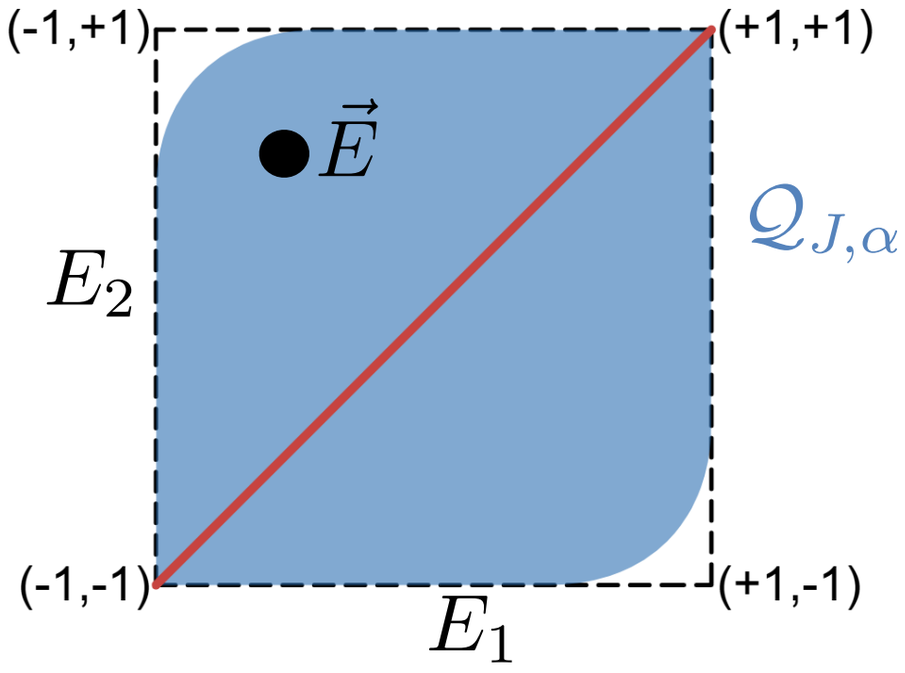


$$E_x \;=\; P(+1|x) \,-\, P(-1|x)$$



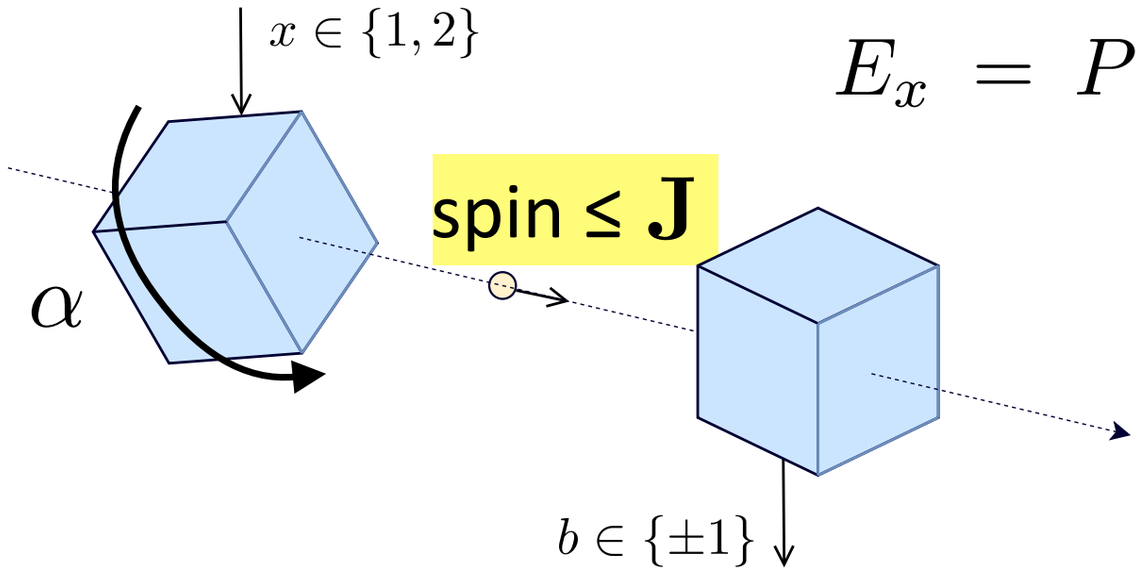
Which correlations are possible? **Theorem:** exactly those:

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

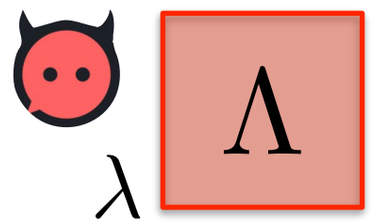


Observing some correlation $\vec{E} = (E_1, E_2)$ outside the red line thus allows us to certify randomness against the eavesdropper.

A theory-independent SDI randomness generator

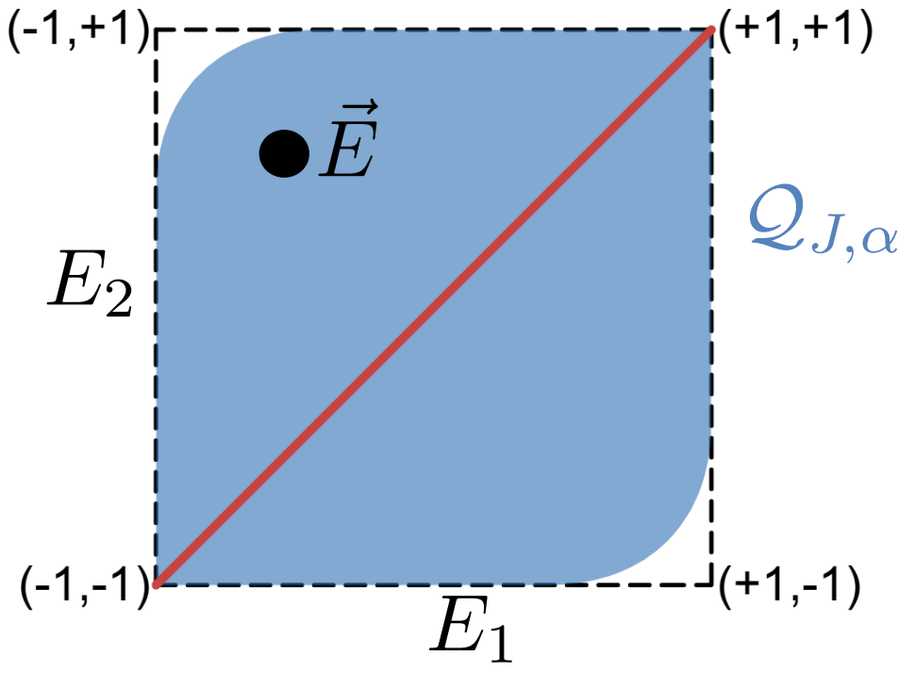


$$E_x \;=\; P(+1|x) \,-\, P(-1|x)$$



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

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



Observing some correlation $\vec{E} = (E_1, E_2)$ outside the red line thus allows us to certify randomness against the eavesdropper.

This fact, *and* the amount of random bits, is **independent of the probabilistic theory.**

Overview

1. Motivation (and some history)

2. “Rotation boxes” within and beyond QT

3. A metrological game and the (sub)optimality of QT

4. A theory-independent SDI randomness generator

5. Conclusions

Overview

1. Motivation (and some history)

2. “Rotation boxes” within and beyond QT

3. A metrological game and the (sub)optimality of QT

4. A theory-independent SDI randomness generator

5. Conclusions

Bonus: Characterization of the quantum (2,2,2) **Bell correlations**

Bonus: Characterization of the quantum (2,2,2) **Bell correlations**

Consider a Bell scenario where all **local** conditional boxes

$$P^{A}_{b,\beta}(a|\alpha) := \frac{P(a,b|\alpha,\beta)}{P^{B}(b|\beta)} \qquad \text{(and similarly for Bob)}$$

are **unbiased** and **spin-1/2**. Unbiased means $P(a|\alpha) = P(-a|\alpha+\pi)$.

Bonus: Characterization of the quantum (2,2,2) **Bell correlations**

Consider a Bell scenario where all **local** conditional boxes

$$P^A_{b,\beta}(a|\alpha) := \frac{P(a,b|\alpha,\beta)}{P^B(b|\beta)} \qquad \text{(and similarly for Bob)}$$

are **unbiased** and **spin-1/2**. Unbiased means $P(a|\alpha) = P(-a|\alpha+\pi)$.

Theorem 9. *Under the assumptions above, the behavior P is a quantum behavior. That is, there exists a quantum state ρ_{AB} on the two-qubit Hilbert space AB and a positive map τ on B with $\tau(\mathbf{1}_B) = \mathbf{1}_B$ such that*

$$P(a,b|\alpha,\beta) = Tr\left(\rho_{AB} e^{-i\alpha Z}|a\rangle\langle a|e^{i\alpha Z} \otimes \tau(e^{-i\beta Z}|b\rangle\langle b|e^{i\beta Z})\right),$$

where $Z = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ *is half of the Pauli-Z matrix, and* $|\pm 1\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

Bonus: Characterization of the quantum (2,2,2) **Bell correlations**

Consider a Bell scenario where all **local** conditional boxes

$$P^A_{b,\beta}(a|\alpha) := \frac{P(a,b|\alpha,\beta)}{P^B(b|\beta)} \qquad \text{(and similarly for Bob)}$$

are **unbiased** and **spin-1/2**. Unbiased means $P(a|\alpha) = P(-a|\alpha+\pi)$.

Theorem 9. *Under the assumptions above, the behavior P is a quantum behavior. That is, there exists a quantum state ρ_{AB} on the two-qubit Hilbert space AB and a positive map τ on B with $\tau(\mathbf{1}_B) = \mathbf{1}_B$ such that*

$$P(a,b|\alpha,\beta) = Tr\left(\rho_{AB} e^{-i\alpha Z}|a\rangle\langle a|e^{i\alpha Z} \otimes \tau(e^{-i\beta Z}|b\rangle\langle b|e^{i\beta Z})\right),$$

where $Z = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ *is half of the Pauli-Z matrix, and* $|\pm 1\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

Restricting to two input angles each, and allowing convex mixtures, this **completely characterizes the quantum (2,2,2) Bell correlations!**

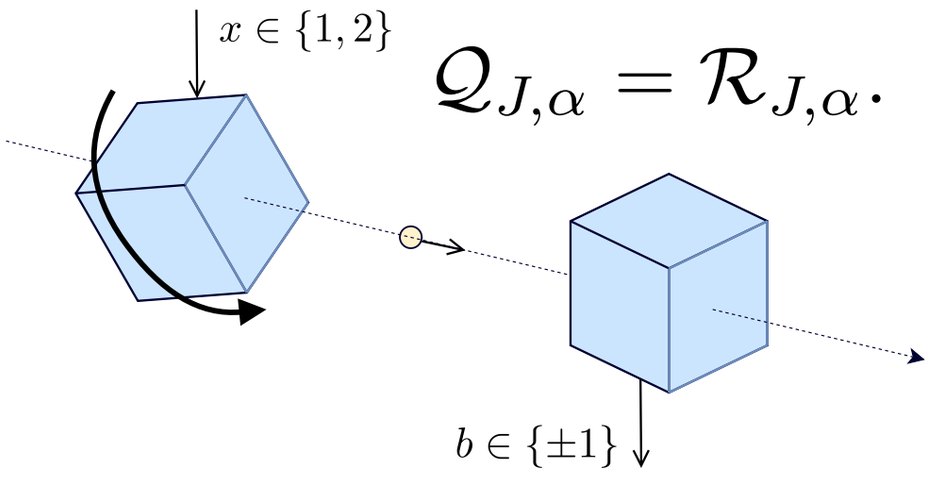
Conclusions

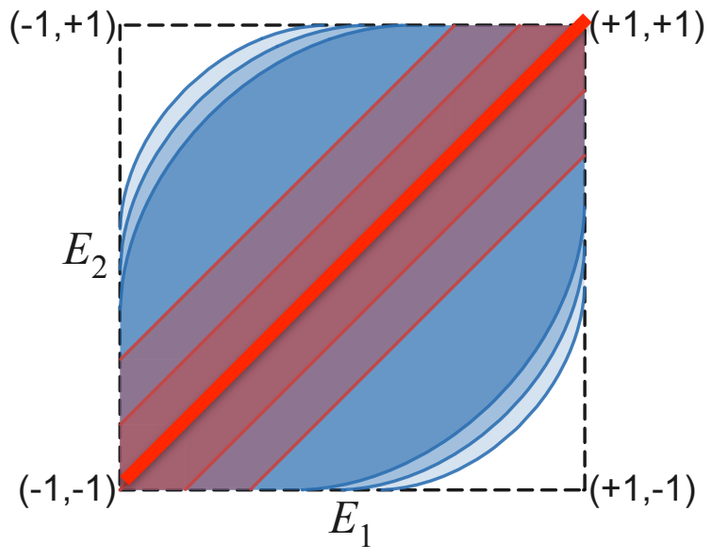
- Motivated the foundational study of how spacetime constrains probabilities (quantum or more general).

- Studied **rotation boxes** for spin-J.
  Fundamental results: $\mathcal{Q}_0 = \mathcal{R}_0, \quad \mathcal{Q}_{1/2} = \mathcal{R}_{1/2}, \quad \mathcal{Q}_1 = \mathcal{R}_1.$
  Exact characterization of these sets. But $\mathcal{Q}_{3/2} \subsetneq \mathcal{R}_{3/2}.$

- Interpretation: (sub)optimality of QT in **metrological games**.

- "Application": **theory-independent SDI randomness**.
  Correlations exactly determined by covariance for 2 settings.





References

- A. Aloy, T. D. Galley, C. L. Jones, S. L. Ludescher, and M. P. Müller, *Spin-bounded correlations: rotation boxes within and beyond quantum theory*, Commun. Math. Phys. **405**, 292 (2024).
- C. L. Jones, S. L. Ludescher, A. Aloy, and M. P. Müller, *Theory-independent randomness generation from spatial symmetries*, Quantum **10**, 1966 (2026).
- A. J. P. Garner, M. P. Müller, and O. C. O. Dahlsten, *The complex and quaternionic quantum bit from relativity of simultaneity on an interferometer,* Proc. R. Soc. A **473**, 20170596 (2017).



Slides, papers and more: **mpmueller.net**

Thank you!