ÖAW AUSTRIAN ACADEMY OF SCIENCES

IQOQI – INSTITUTE FOR QUANTUM OPTICS AND QUANTUM INFORMATION VIENNA

Theory-independent randomness generation with spacetime symmetries

Caroline L. Jones, Stefan L. Ludescher, Albert Aloy, **Markus P. Müller**

Institute for Quantum Optics and Quantum Information (IQOQI), Vienna

Perimeter Institute for Theoretical Physics (PI), Waterloo, Canada

FWF Der Wissenschaftsfonds.

PERIMETER INSTITUTE

Overview

1. Motivations: QG and device-independent QIT

2. Our protocol, and its quantum analysis

3. Rotation boxes beyond quantum theory

4. Conclusions

Overview

1. Motivations: QG and device-independent QIT

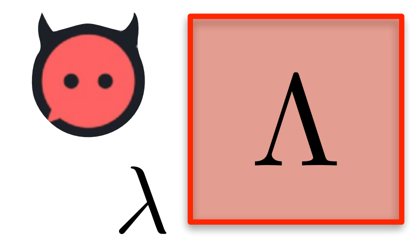
2. Our protocol, and its quantum analysis

3. Rotation boxes beyond quantum theory

4. Conclusions

Motivation 1: SDI randomness expansion

Goal: Generate **certifiably random** bits, unpredictable even by eavesdroppers with arbitrary classical side information.

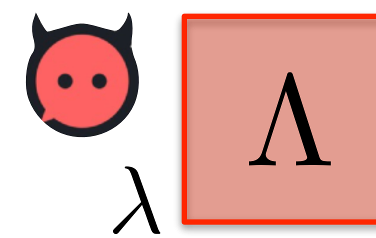


Motivation 1: SDI randomness expansion

Goal: Generate **certifiably random** bits, unpredictable even by eavesdroppers with arbitrary classical side information.

Device-independent: works for completely untrusted devices.

Needs a loophole-free Bell test to be realized. Extremely difficult.

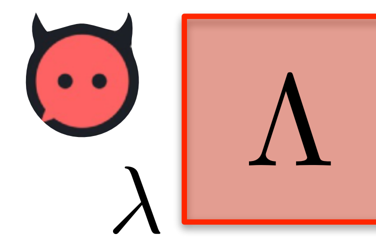


Motivation 1: SDI randomness expansion

Goal: Generate **certifiably random** bits, unpredictable even by eavesdroppers with arbitrary classical side information.

Device-independent: works for completely untrusted devices.
Needs a loophole-free Bell test to be realized. Extremely difficult.

Semi-device-independent (SDI): allow communication between devices.
Make some (modest?!) assumption on the transmitted phys. system.

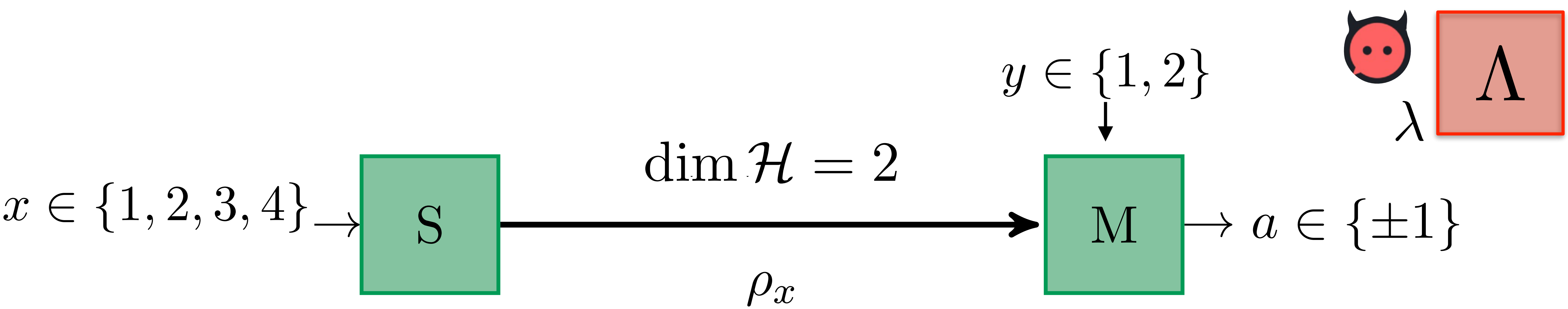


Motivation 1: SDI randomness expansion

Goal: Generate **certifiably random** bits, unpredictable even by eavesdroppers with arbitrary classical side information.

Device-independent: works for completely untrusted devices.
Needs a loophole-free Bell test to be realized. Extremely difficult.

Semi-device-independent (SDI): allow communication between devices.
Make some (modest?!) assumption on the transmitted phys. system.

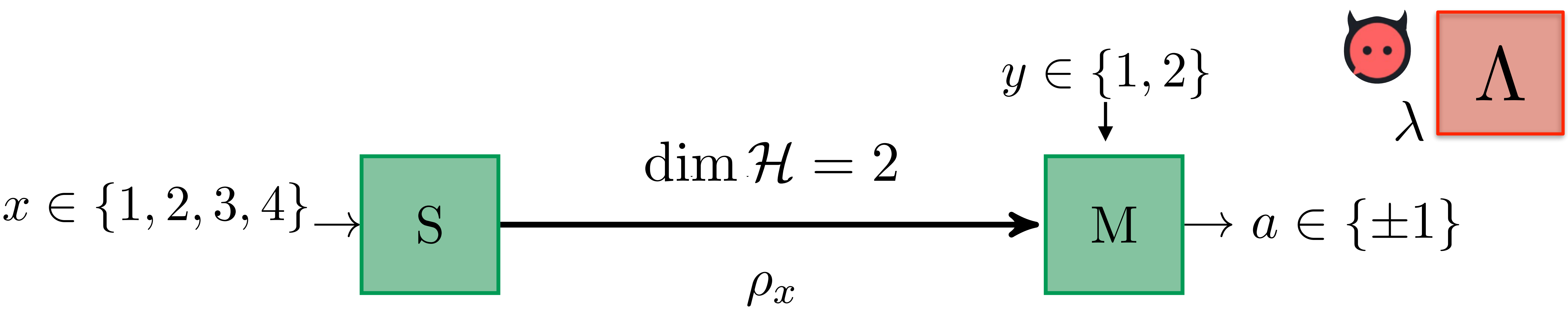


Motivation 1: SDI randomness expansion

Goal: Generate **certifiably random** bits, unpredictable even by eavesdroppers with arbitrary classical side information.

Device-independent: works for completely untrusted devices.
Needs a loophole-free Bell test to be realized. Extremely difficult.

Semi-device-independent (SDI): allow communication between devices.
Make some (modest?!) assumption on the transmitted phys. system.



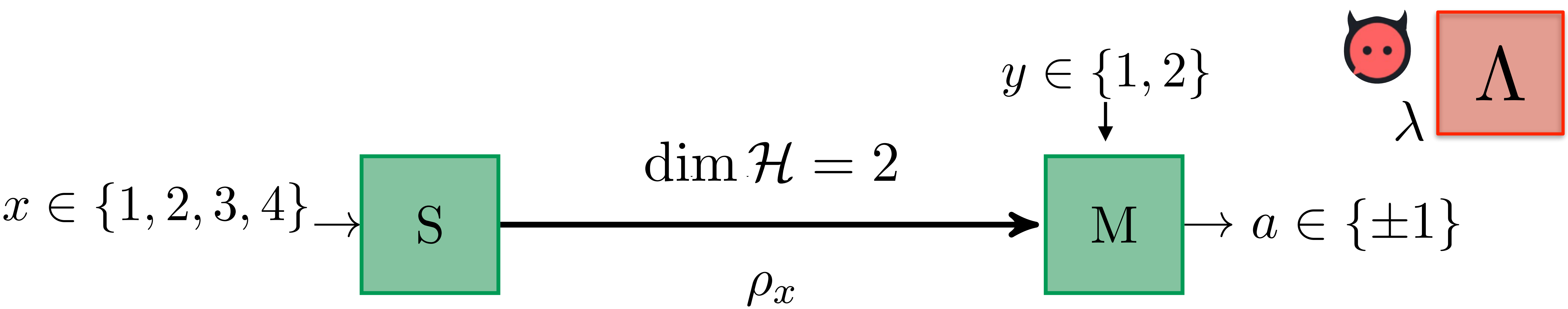
From observed correlations $p(a|x,y)$, infer $H(A|X,Y,\Lambda) \geq \ldots > 0$.

Motivation 1: SDI randomness expansion

Goal: Generate **certifiably random** bits, unpredictable even by eavesdroppers with arbitrary classical side information.

Device-independent: works for completely untrusted devices.
Needs a loophole-free Bell test to be realized. Extremely difficult.

Semi-device-independent (SDI): allow communication between devices.
Make some (modest?!) assumption on the transmitted phys. system.

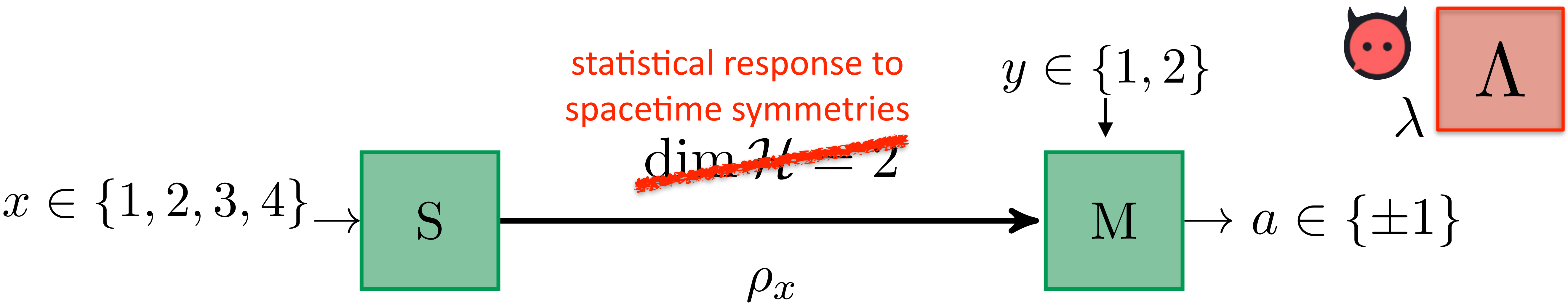


From observed correlations $p(a|x,y)$, infer $H(A|X,Y,\Lambda) \geq \ldots > 0$.

Problems: assumption not very well motivated; assumes QT is correct.

Motivation 1: SDI randomness expansion

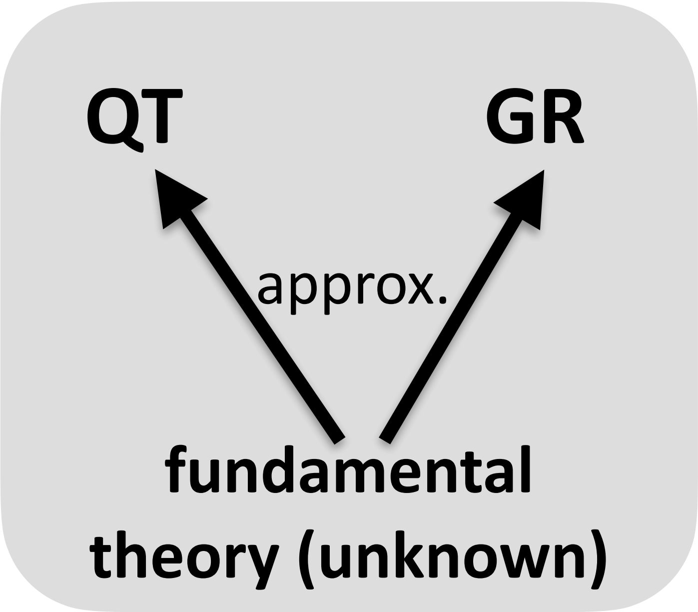
Our SDI assumption: essentially, a bound on how sensitive the system responds to spatial rotations (in QT: “spin quantum number”).
This turns out to make sense (and work) without assuming QT.



From observed correlations $p(a|x, y)$, infer $H(A|X, Y, \Lambda) \geq \ldots > 0$.

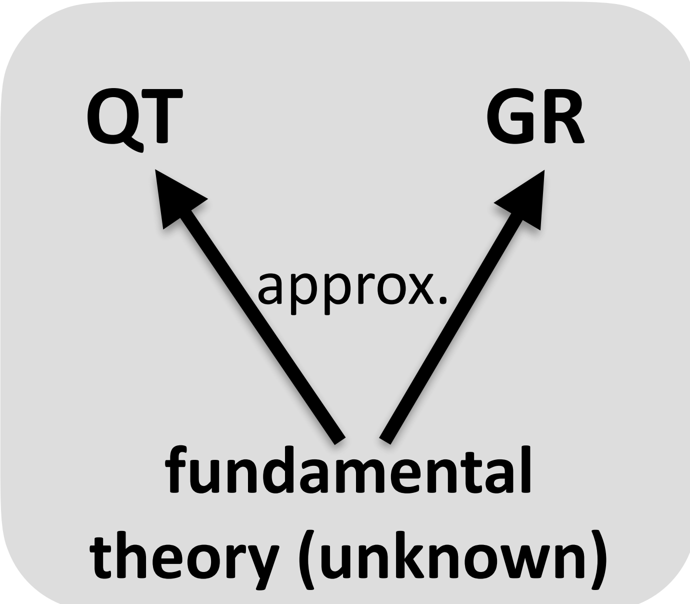
Motivation 2: quantum gravity

Motivation 2: quantum gravity



Instead of jumping directly to Quantum Gravity,
study the **logical architecture of physics**:
how do QT and spacetime constrain each other?

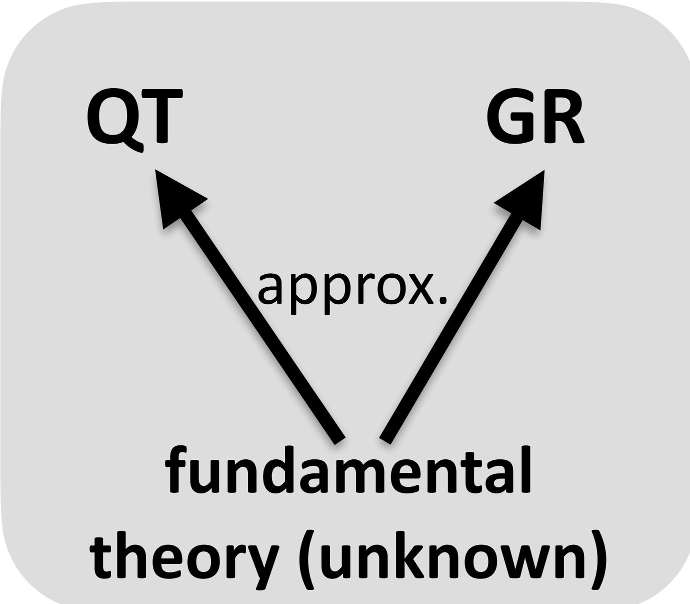
Motivation 2: quantum gravity



Instead of jumping directly to Quantum Gravity, study the **logical architecture of physics**: how do QT and spacetime constrain each other?

Analogy: suppose we would like to find a detailed theory of (bio.) **evolution**.

Motivation 2: quantum gravity

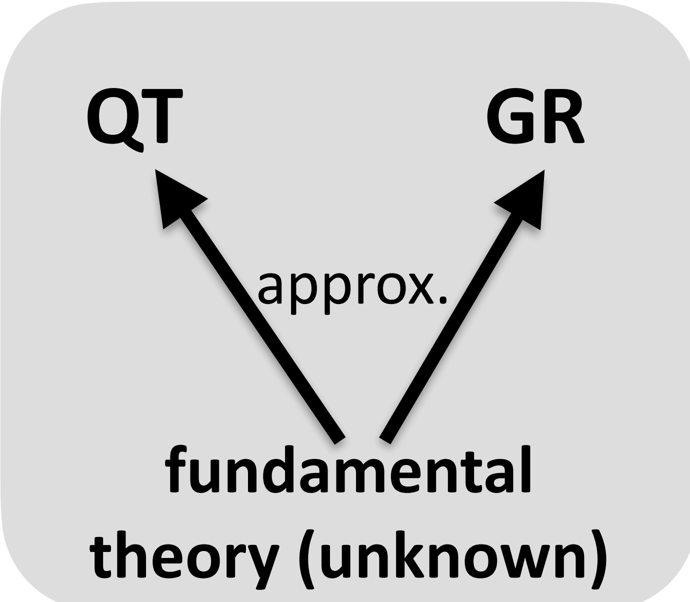


Instead of jumping directly to Quantum Gravity, study the **logical architecture of physics**: how do QT and spacetime constrain each other?

Analogy: suppose we would like to find a detailed theory of (bio.) **evolution**.

biology of life ⟷ geological environment

Motivation 2: quantum gravity



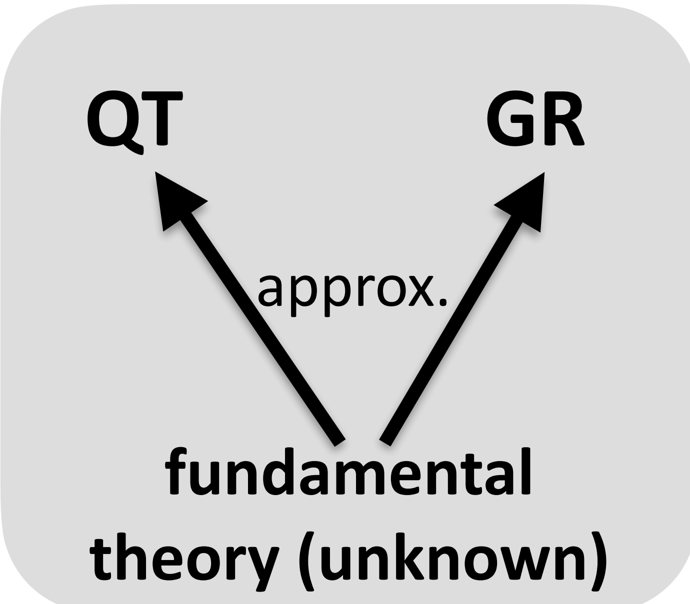
Instead of jumping directly to Quantum Gravity, study the **logical architecture of physics**: how do QT and spacetime constrain each other?

Analogy: suppose we would like to find a detailed theory of (bio.) **evolution**.

biology of life ⟷ geological environment

- Possibility 1: construct detailed theory how evolution supposedly unfolded.
- Possibility 2: first, study the relation of the two as presented right now.

Motivation 2: quantum gravity



Instead of jumping directly to Quantum Gravity, study the **logical architecture of physics**: how do QT and spacetime constrain each other?

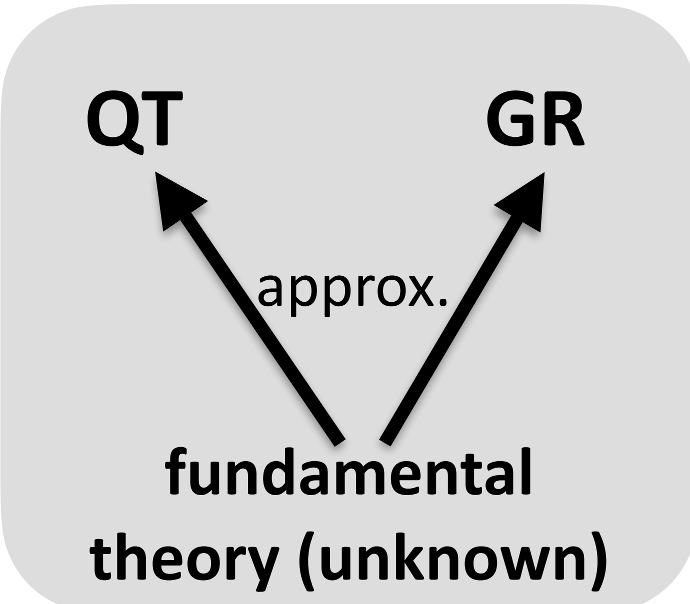
Analogy: suppose we would like to find a detailed theory of (bio.) **evolution**.

biology of life ⟷ geological environment

- Possibility 1: construct detailed theory how evolution supposedly unfolded.
- Possibilitv 2: first, study the relation of the two as presented right now.

Camel humps and thorns as a *consequence* of environment. What kind of life fits into a given environment *in principle?*

Motivation 2: quantum gravity

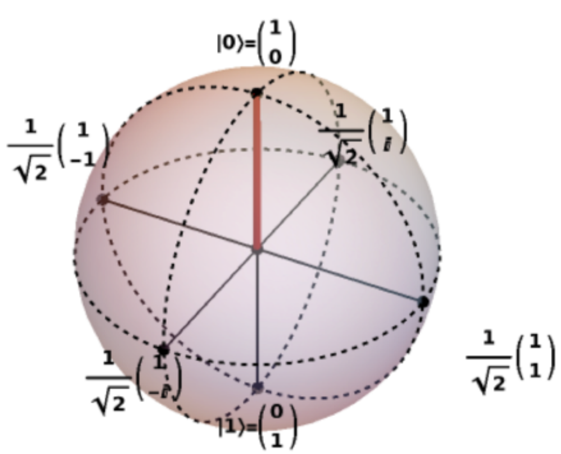


Instead of jumping directly to Quantum Gravity, study the **logical architecture of physics**: how do QT and spacetime constrain each other?

Analogy: suppose we would like to find a detailed theory of (bio.) **evolution**.

biology of life ⟷ geological environment

- Possibility 1: construct detailed theory how evolution supposedly unfolded.
- Possibility 2: first, study the relation of the two as presented right now.



Qubit Bloch ball and quantum correlations as *consequences of* spacetime structure? Which detector click probabilities fit *in principle* into space and time?

Overview

1. Motivations: QG and device-independent QIT

2. Our protocol, and its quantum analysis

3. Rotation boxes beyond quantum theory

4. Conclusions

Overview

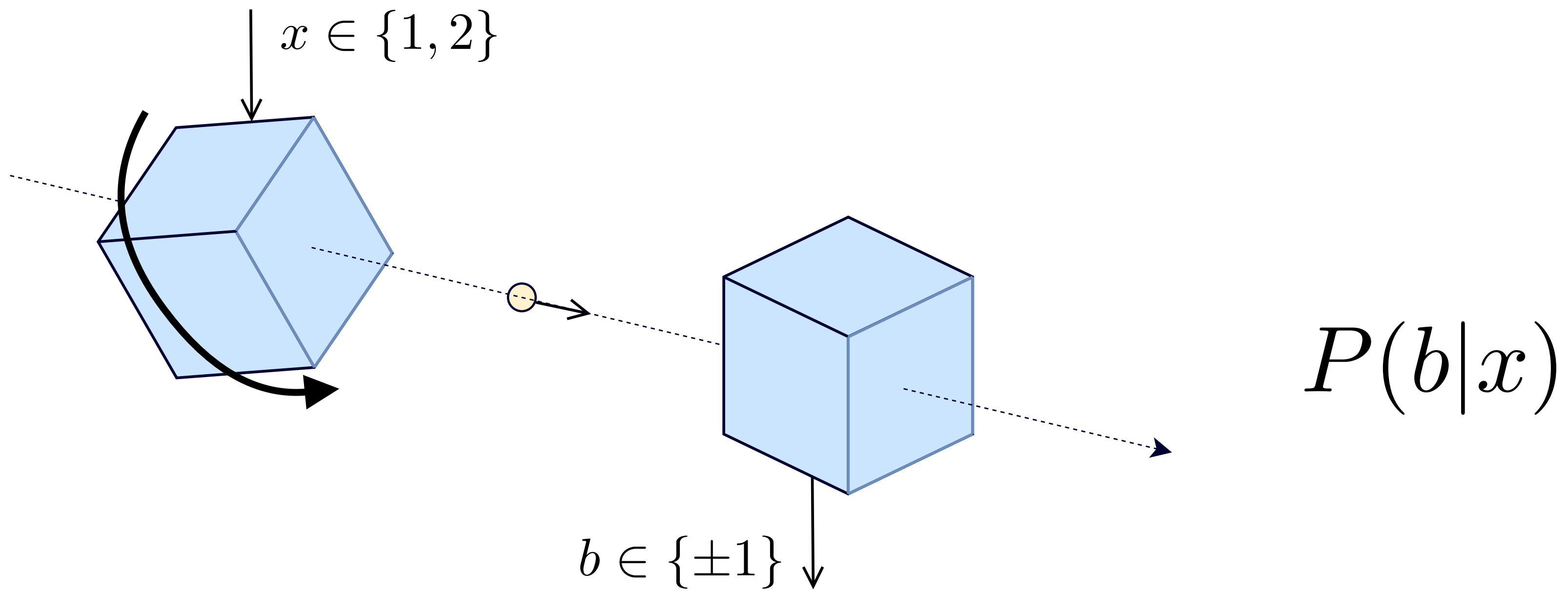
1. Motivations: QG and device-independent QIT

2. Our protocol, and its quantum analysis

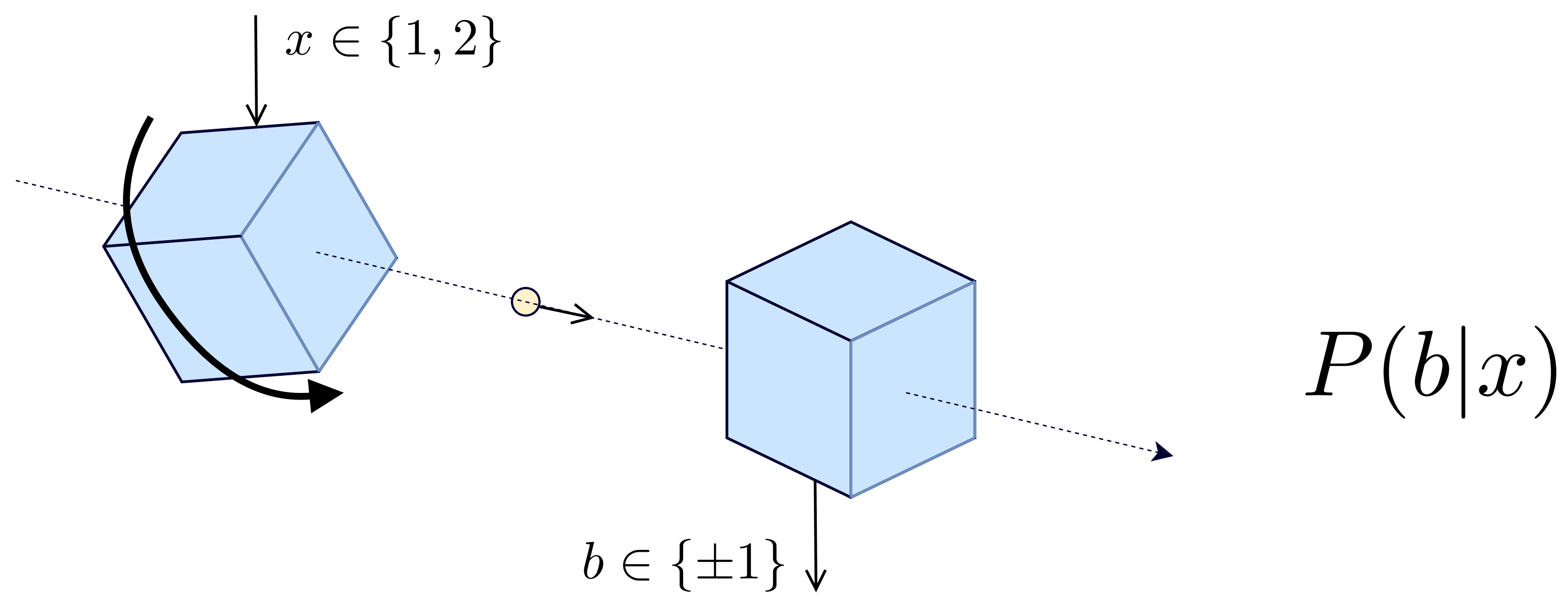
3. Rotation boxes beyond quantum theory

4. Conclusions

Our protocol and its quantum analysis



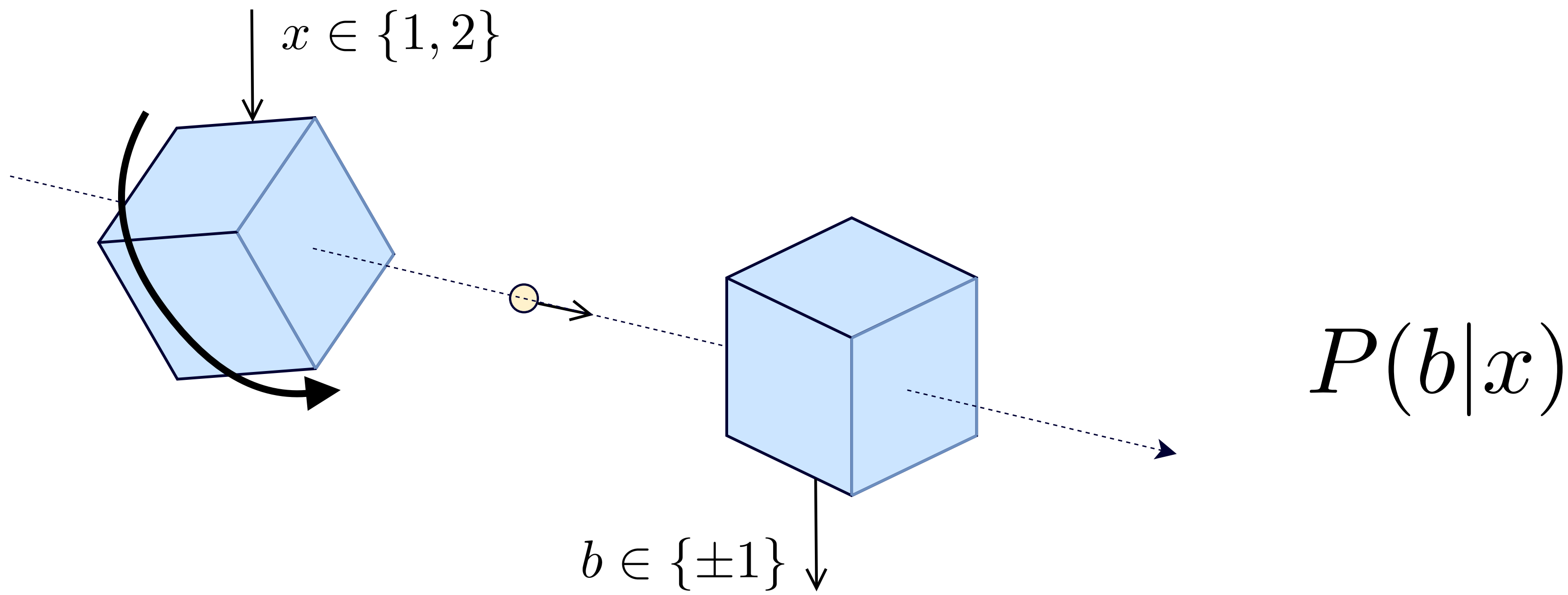
Our protocol and its quantum analysis



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

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

Our protocol and its quantum analysis



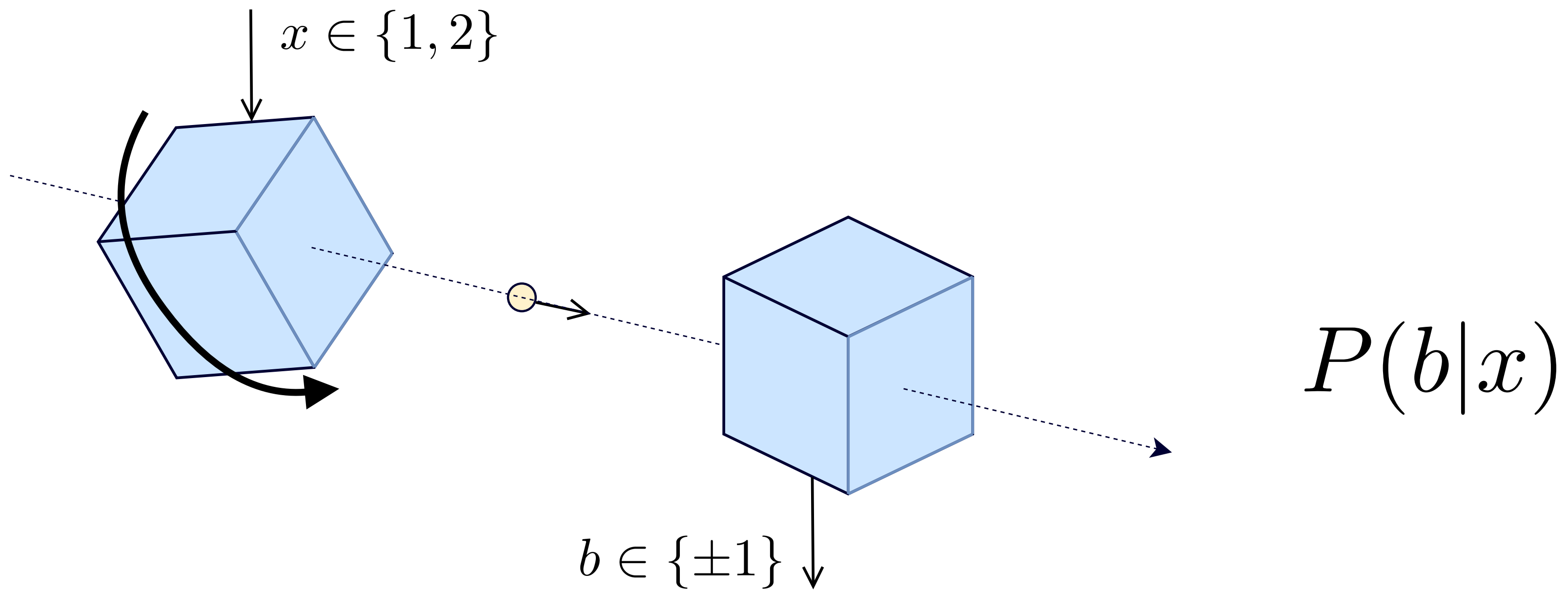
If input is x=1: do nothing to preparation device;

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

SDI assumption: spin of system ≤ $\mathbf{J}$

No further assumptions on devices / system.

Our protocol and its quantum analysis



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

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

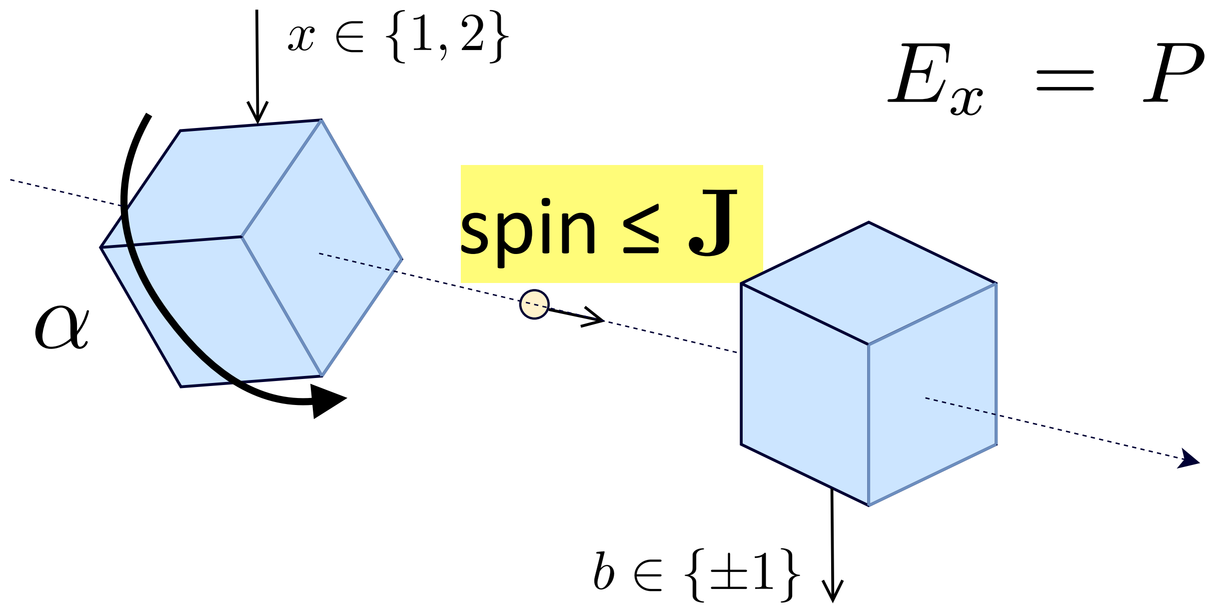
SDI assumption: spin of system ≤ $\mathbf{J}$

No further assumptions on devices / system.

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

$$U_\alpha = \bigoplus_{j=-J}^{J} n_j e^{ij\alpha}, \qquad P(b|\alpha) = \sum_\lambda p(\lambda)\mathrm{tr}(M_b(\lambda)U_\alpha \rho_1(\lambda)U_\alpha^\dagger)$$

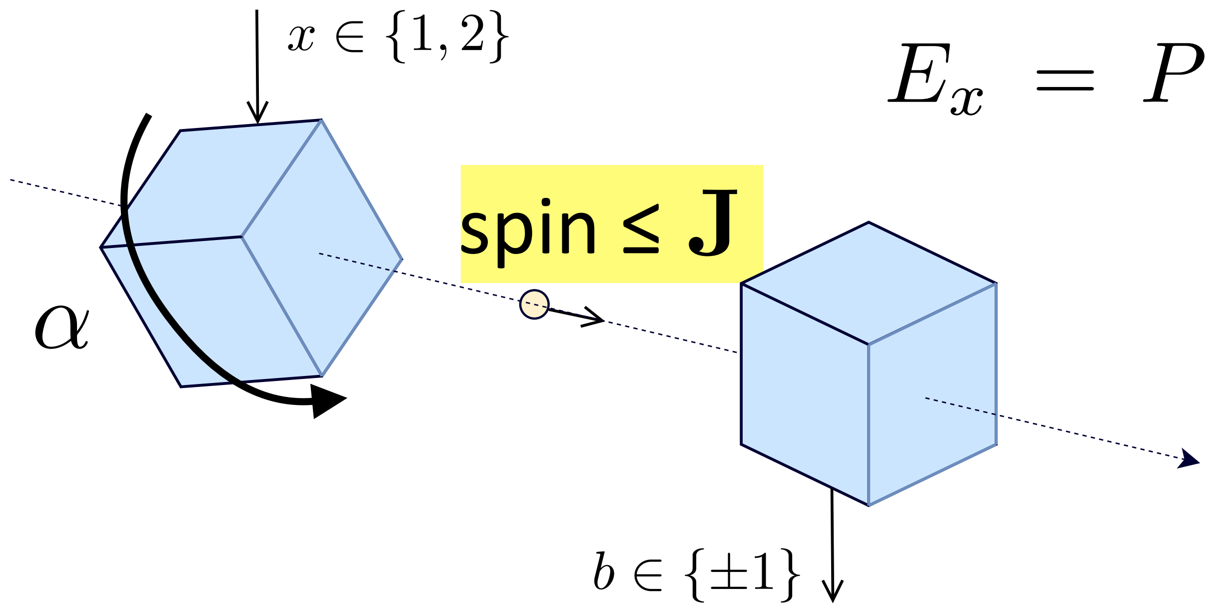
Our protocol and its quantum analysis



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

$$P(b|x)$$

Our protocol and its quantum analysis



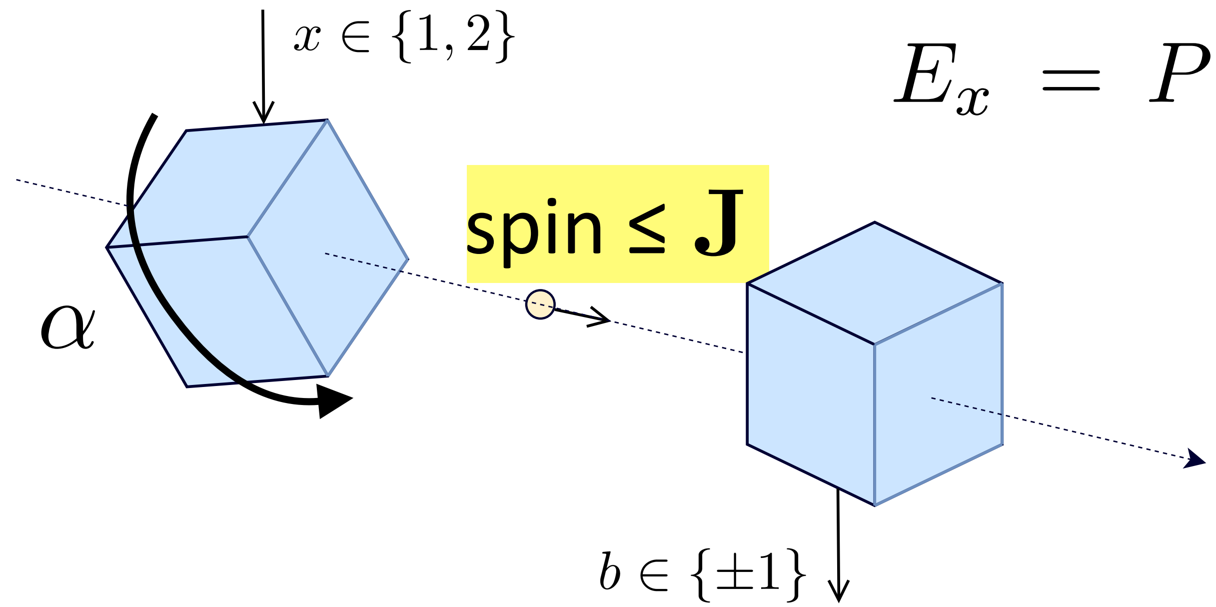
$$E_x = P(+1|x) - P(-1|x)$$

$$P(b|x)$$

Theorem. The following correlations are possible:

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

Our protocol and its quantum analysis

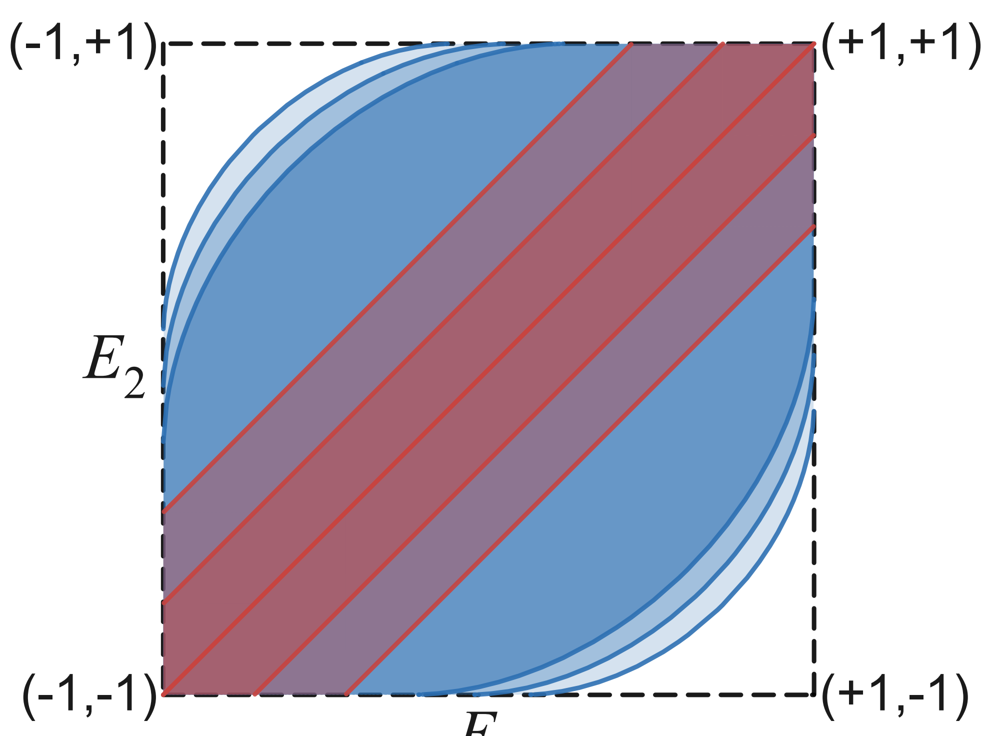


$$E_x = P(+1|x) - P(-1|x)$$

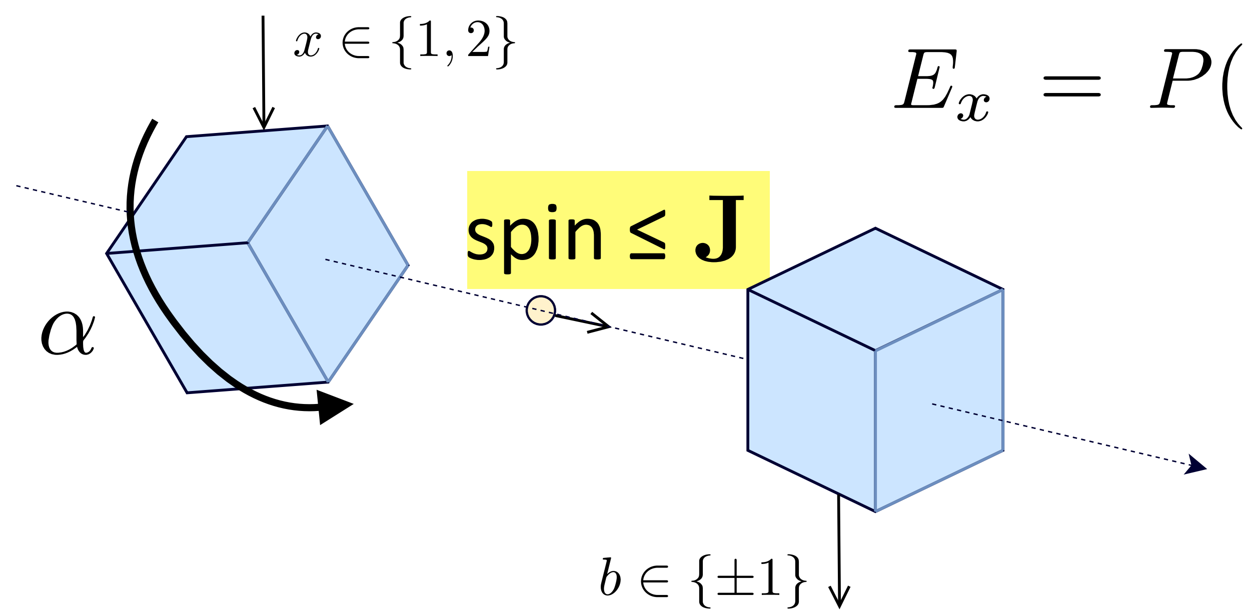
$$P(b|x)$$

Theorem. The following correlations are possible:

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



Our protocol and its quantum analysis

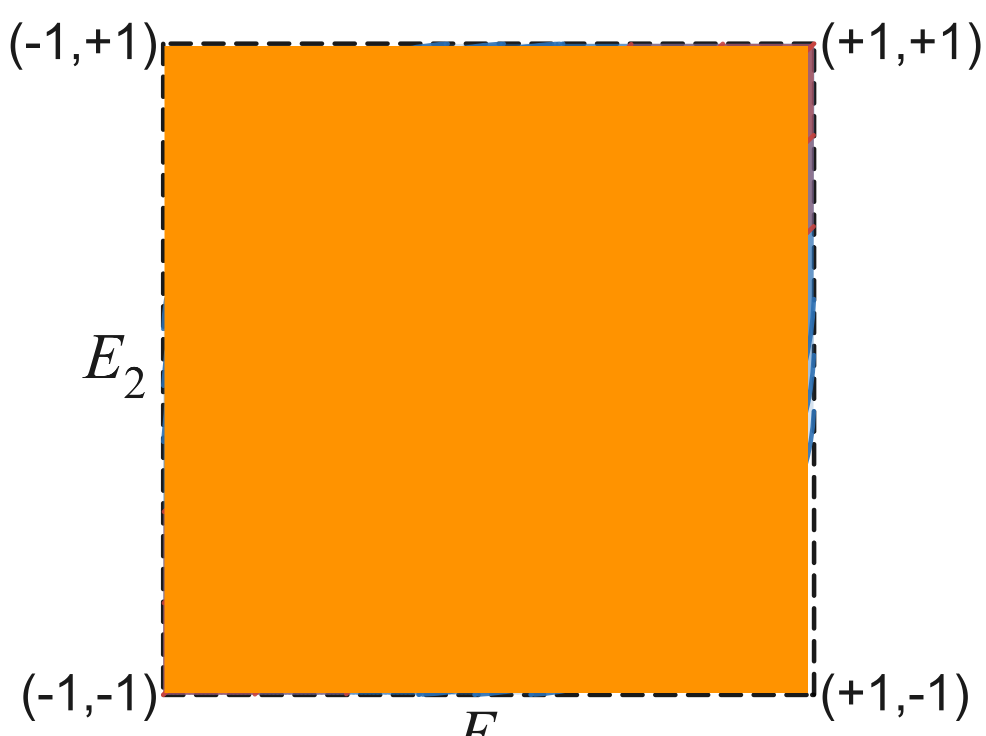


$$E_x = P(+1|x) - P(-1|x)$$

$$P(b|x)$$

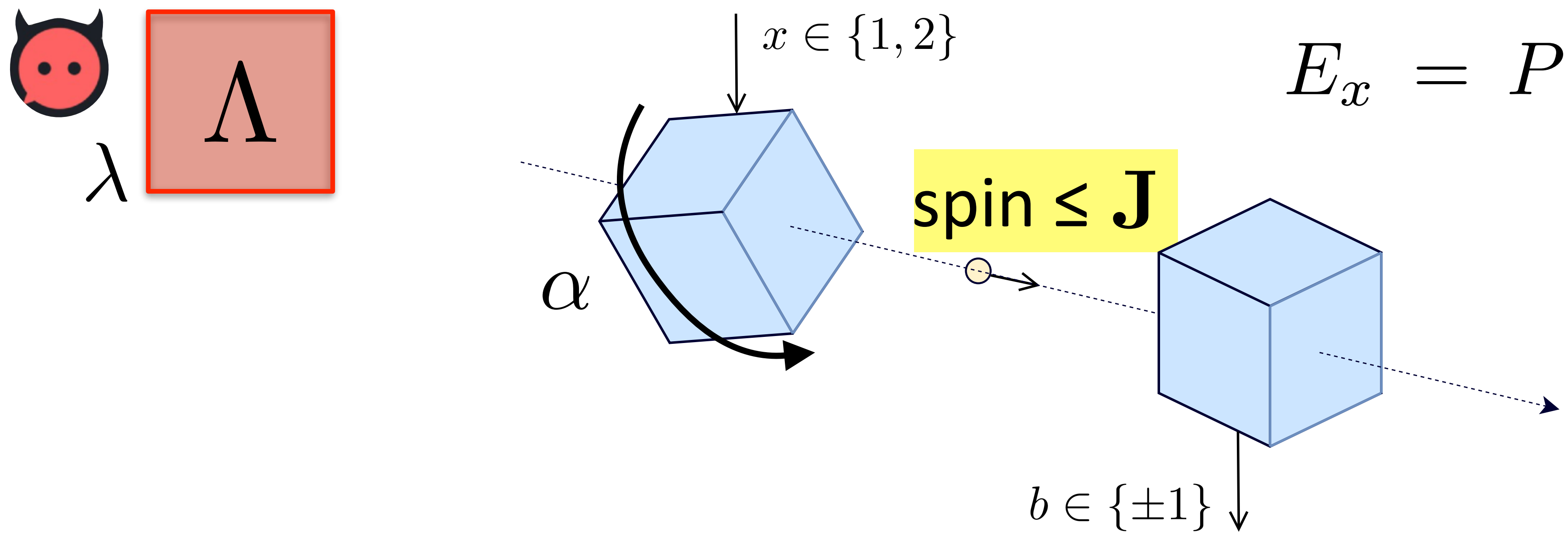
Theorem. The following correlations are possible:

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



Angle $|J\alpha| \geq \pi/2$:
Rotated and unrotated states may be **orthogonal**; outcome *b* may carry perfect classical info on *x*, i.e. $(E_1, E_2) = (\pm 1, \mp 1)$
All correlations possible, **no certifiable randomness.**

Our protocol and its quantum analysis

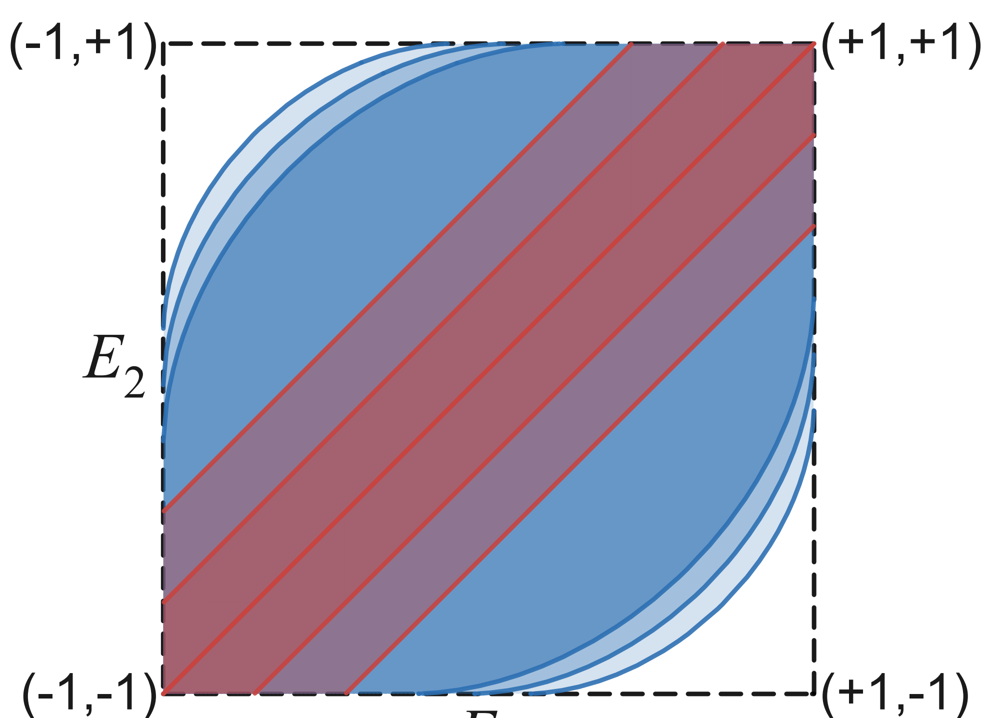


$$E_x = P(+1|x) - P(-1|x)$$

$$P(b|x)$$

Theorem. The following correlations are possible:

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

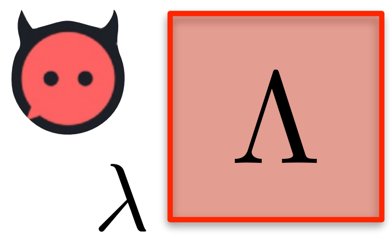


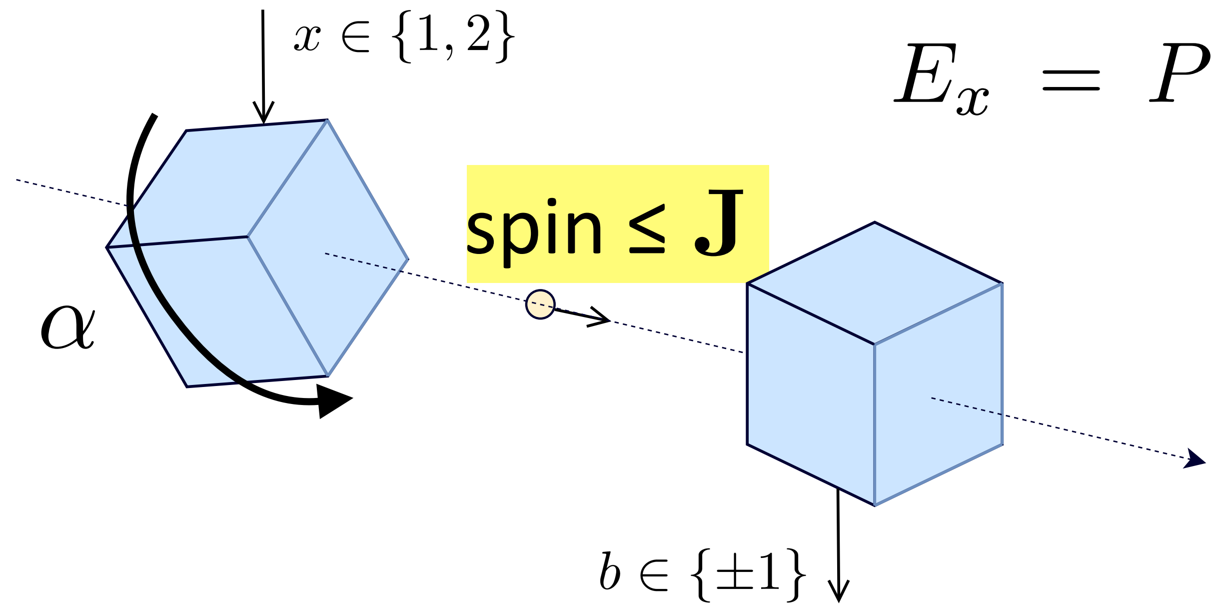
The curved set of correlations is possible.

b cannot carry full information on *x*, hence *b* must contain some randomness, even relative to classical side information λ, if *E* outside the red (“classical”) line:

non-zero amount of certified randomness.

A slide to scare the non-experts



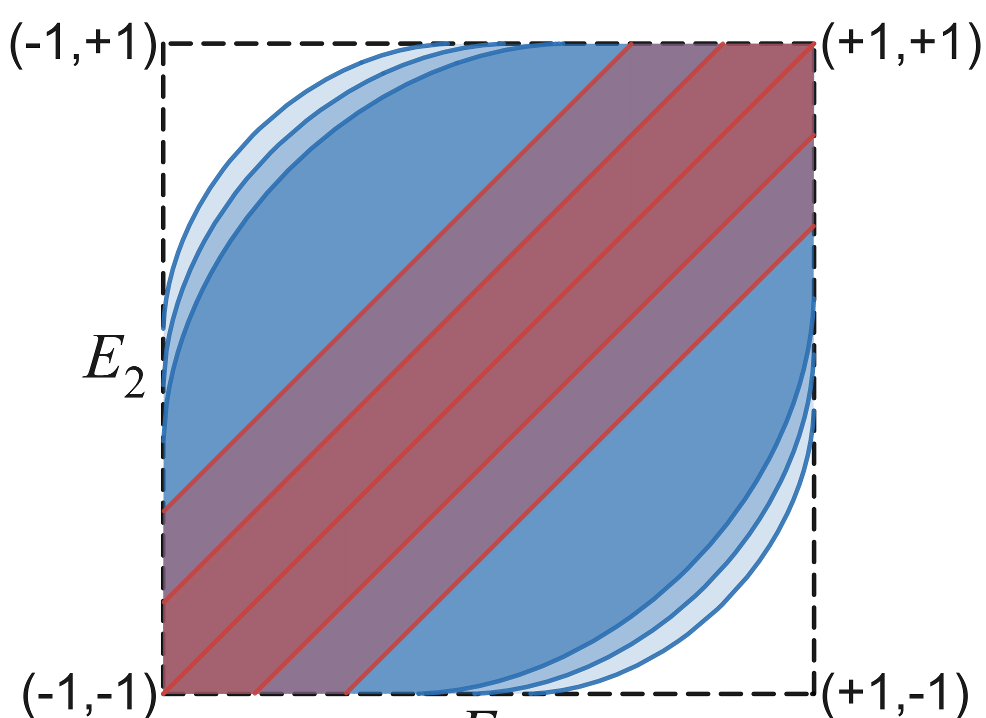


$$E_x = P(+1|x) - P(-1|x)$$

$$P(b|x)$$

Up to prob. ϵ, all “hidden” systems satisfy spin bound approximately.

$$\mathbf{E} = (E_1, E_2) = \sum_\lambda p(\lambda)(E_1^\lambda, E_2^\lambda) = \sum_\lambda p(\lambda)\mathbf{E}^\lambda.$$



# of certified random bits: $H(B|X,\Lambda) \geq H^\star,$

$$H^\star = \min_{\{p(\lambda),\mathbf{E}^\lambda\}} \sum_\lambda p(\lambda) H(\mathbf{E}^\lambda)$$

$$\text{subject to} \sum_{\lambda:\mathbf{E}^\lambda \in \mathcal{Q}^\omega_{J,\alpha}} p(\lambda) \geq 1 - \varepsilon$$

$$\text{and} \sum_\lambda p(\lambda)\mathbf{E}^\lambda = \mathbf{E}.$$

Overview

1. Motivations: QG and device-independent QIT

2. Our protocol, and its quantum analysis

3. Rotation boxes beyond quantum theory

4. Conclusions

Overview

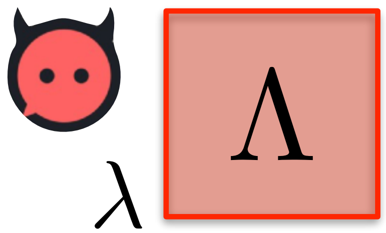
1. Motivations: QG and device-independent QIT

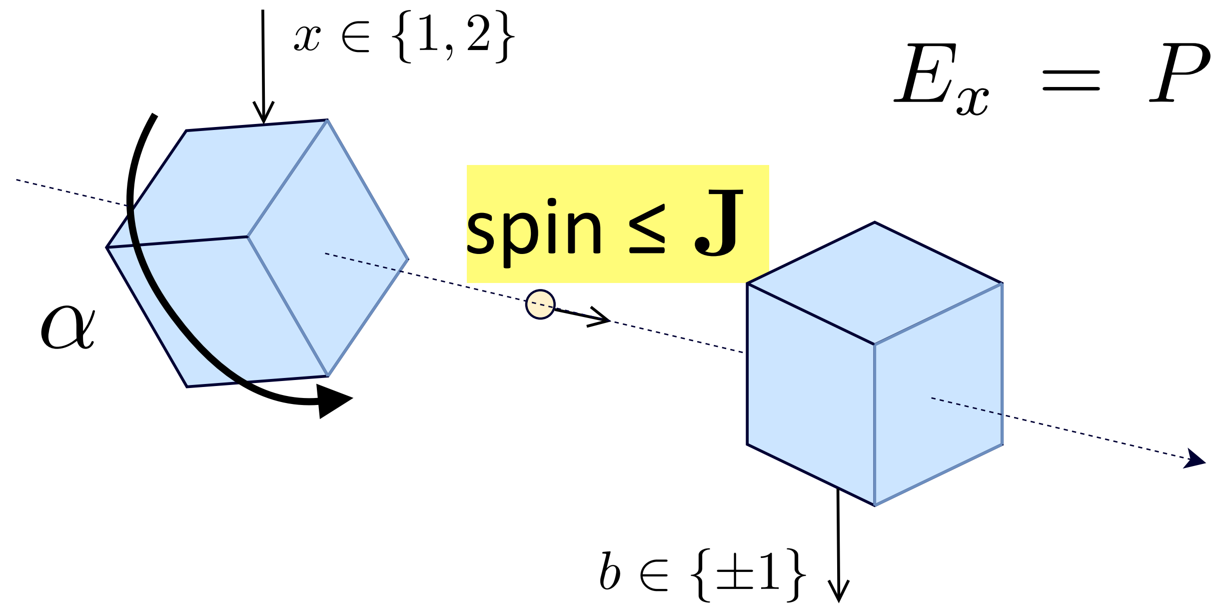
2. Our protocol, and its quantum analysis

3. Rotation boxes beyond quantum theory

4. Conclusions

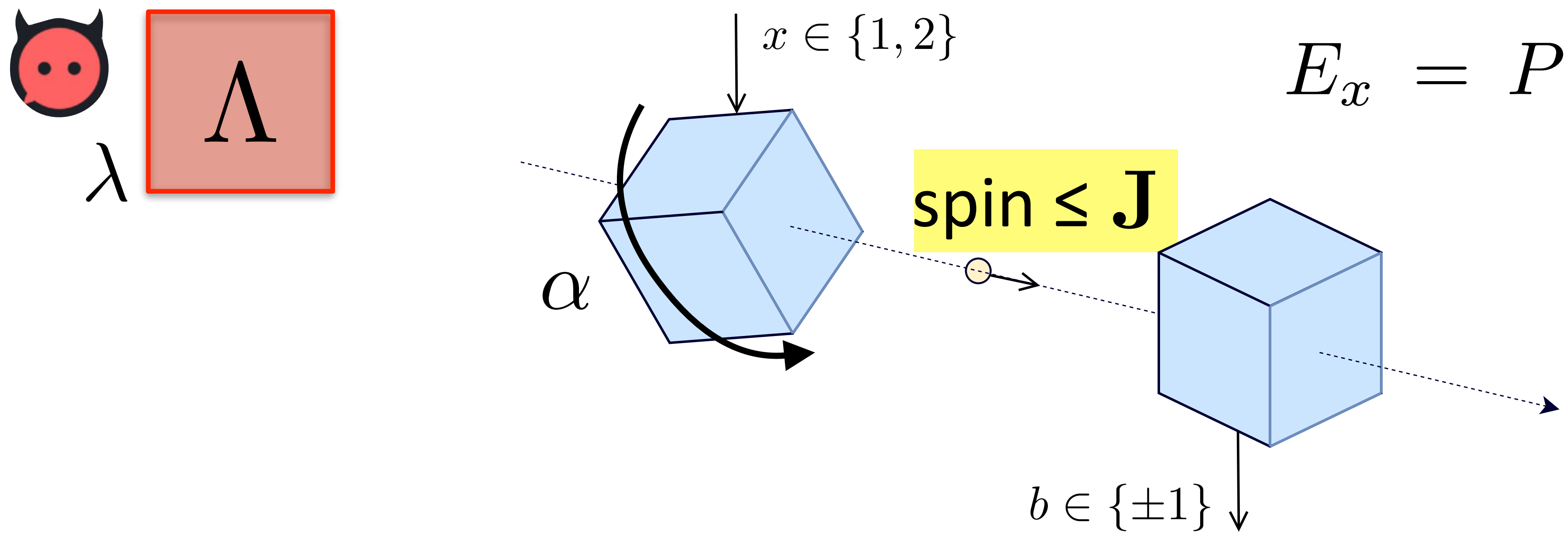
Rotation boxes beyond quantum theory





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

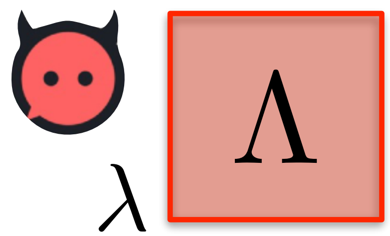
Rotation boxes beyond quantum theory

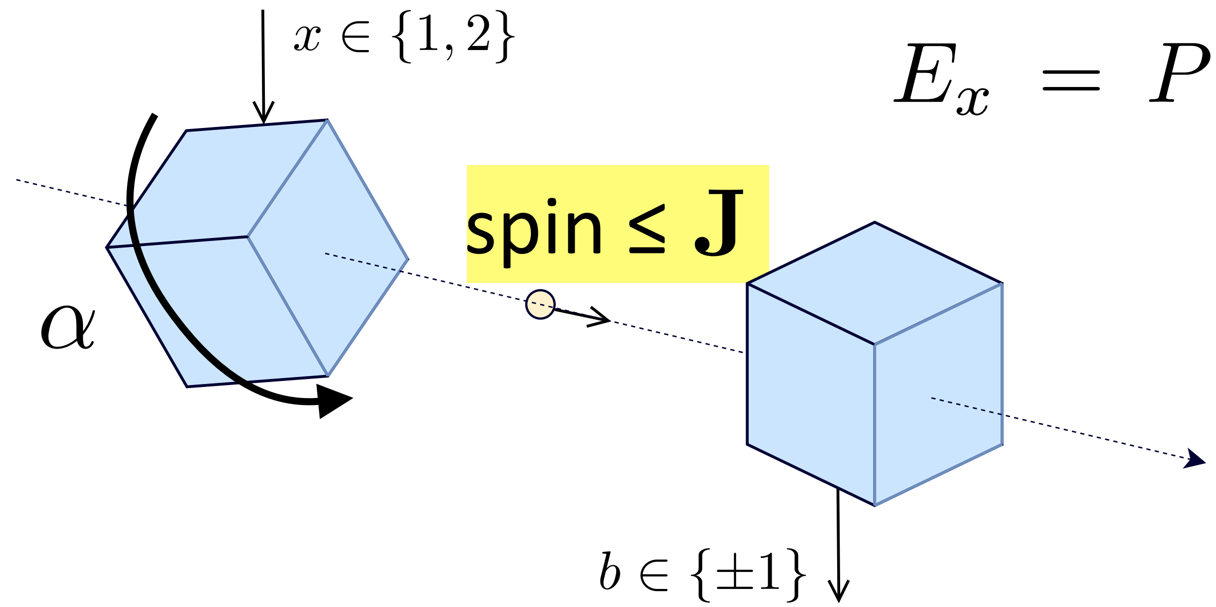


$$E_x = P(+1|x) - P(-1|x)$$

- Can we understand our SDI assumption without assuming QT?
- Can we use the protocol to certify random numbers without QT?

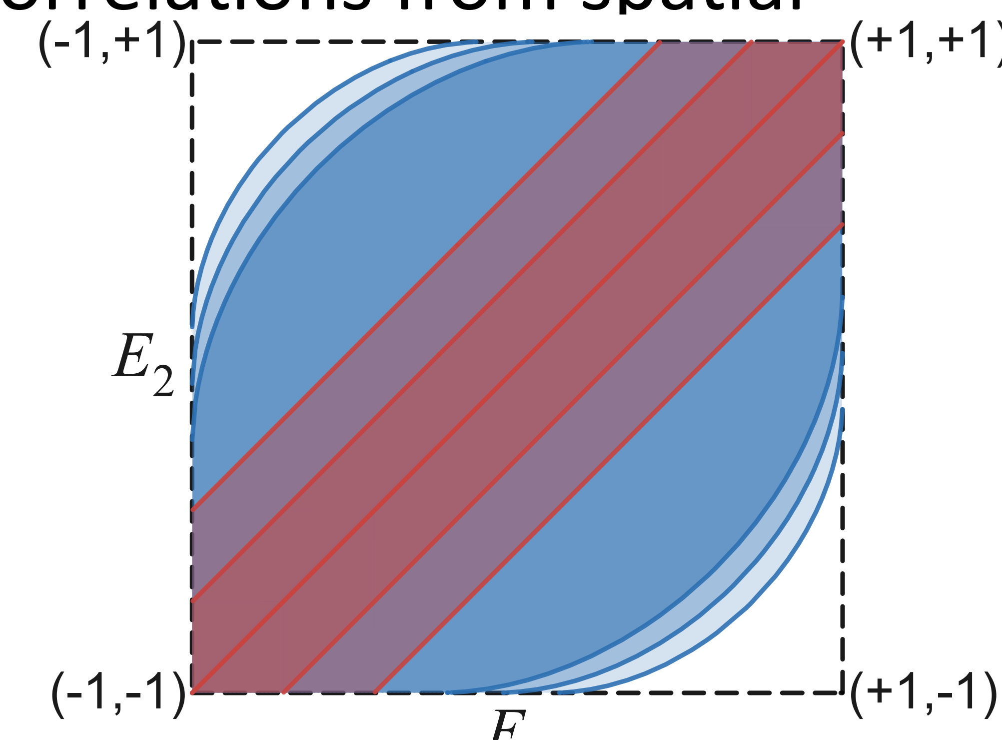
Rotation boxes beyond quantum theory



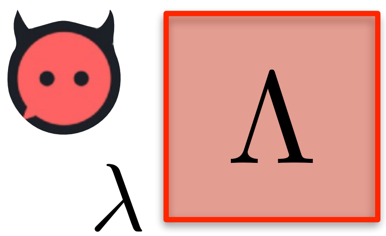


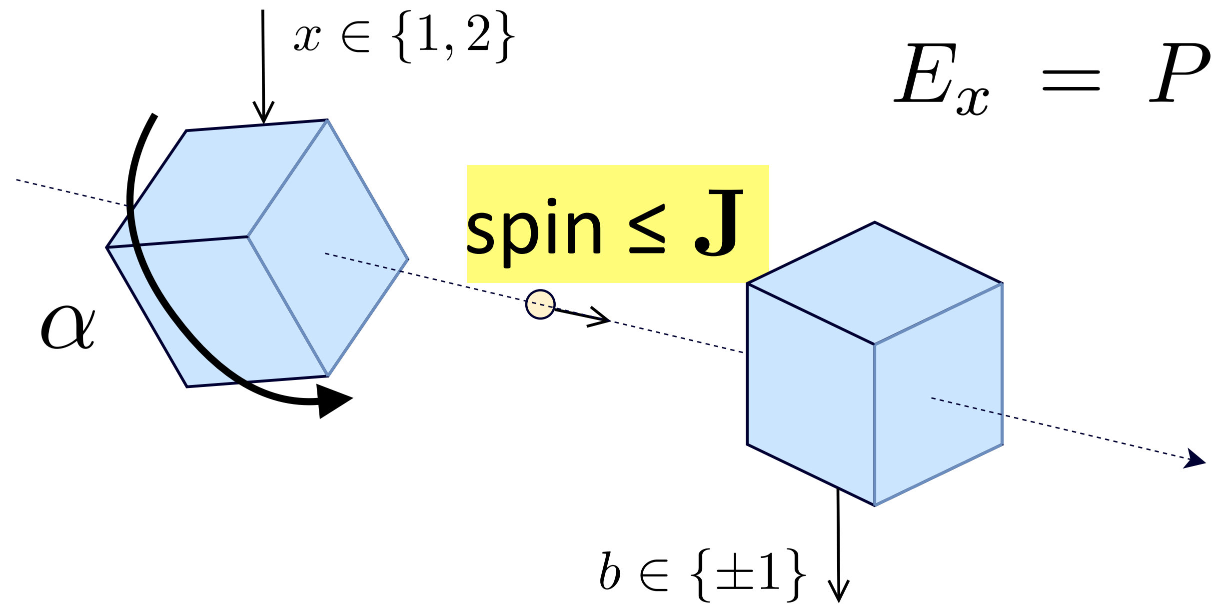
$$E_x = P(+1|x) - P(-1|x)$$

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



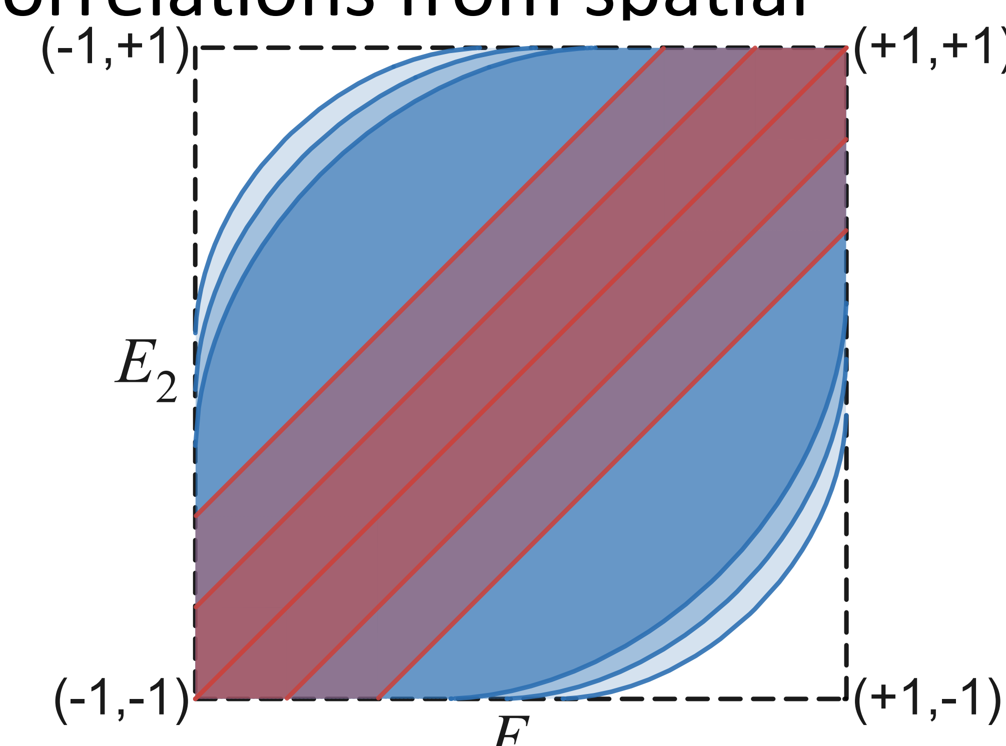
Rotation boxes beyond quantum theory





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

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



Yes we can!

Rotation boxes beyond quantum theory

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

Rotation boxes beyond quantum theory

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

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

$\{E_b\}$ some POVM, ρ some density matrix,

$$U_\alpha = \bigoplus_{j=-J}^{J} n_j e^{ij\alpha},$$ with arbitrary multiplicities n_j.

Rotation boxes beyond quantum theory

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

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

$\{E_b\}$ some POVM, ρ some density matrix,

$U_\alpha = \bigoplus_{j=-J}^{J} n_j e^{ij\alpha}$, with arbitrary multiplicities n_j.

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

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

Rotation boxes beyond quantum theory

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

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

$\{E_b\}$ some POVM, ρ some density matrix,

$U_\alpha = \bigoplus_{j=-J}^{J} n_j e^{ij\alpha}$, with arbitrary multiplicities n_j.

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

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

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

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

$0 \leq p(+1|\alpha) \leq 1$ for all α.

Rotation boxes beyond quantum theory

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

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

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

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

Rotation boxes beyond quantum theory

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

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

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

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

Rotation boxes beyond quantum theory

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

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

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

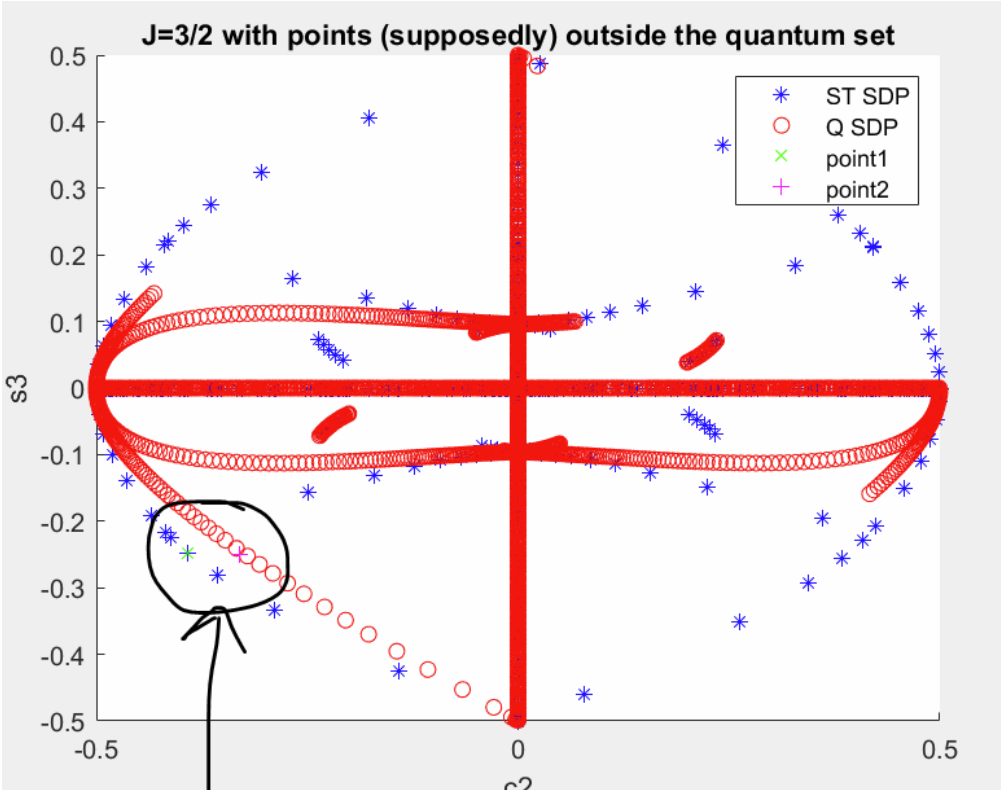
$$\mathcal{R}_J := \left\{\alpha \mapsto p(+1|\alpha) = c_0 + \sum_{j=1}^{2J} c_j \cos(j\alpha) + s_j \sin(j\alpha)\right\},$$

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

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

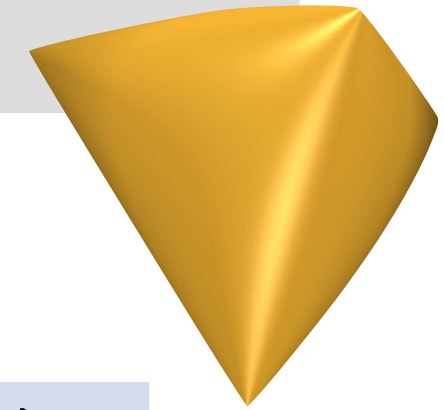
Upcoming paper (mid-2023): $\mathcal{Q}_{3/2} \subsetneq \mathcal{R}_{3/2}$.

We do not know whether $\mathcal{Q}_1 = \mathcal{R}_1$,
but numerics suggests equality!



Rotation boxes beyond quantum theory

Quantum boxes: real representation of SO(2) on the density matrices.
Rotation boxes: real rep. of SO(2) on "orbitope" state spaces.



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

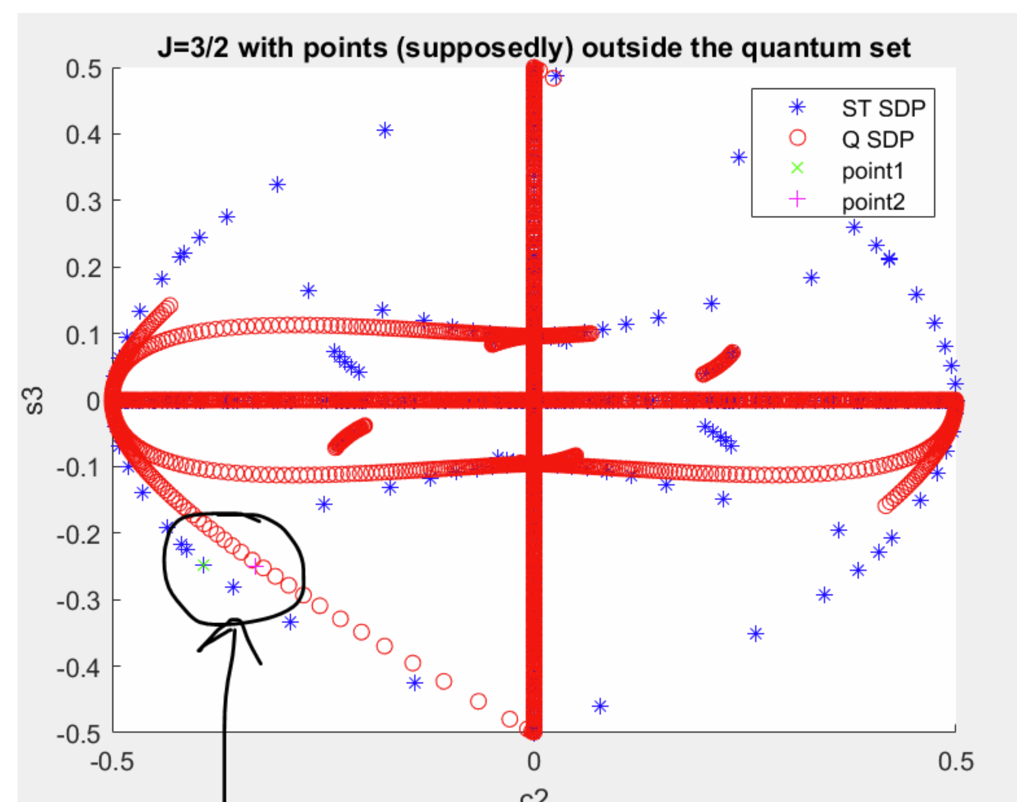
$$\mathcal{R}_J := \left\{ \alpha \mapsto p(+1|\alpha) = c_0 + \sum_{j=1}^{2J} c_j \cos(j\alpha) + s_j \sin(j\alpha) \right\},$$

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

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

Upcoming paper (mid-2023): $\mathcal{Q}_{3/2} \subsetneq \mathcal{R}_{3/2}$.

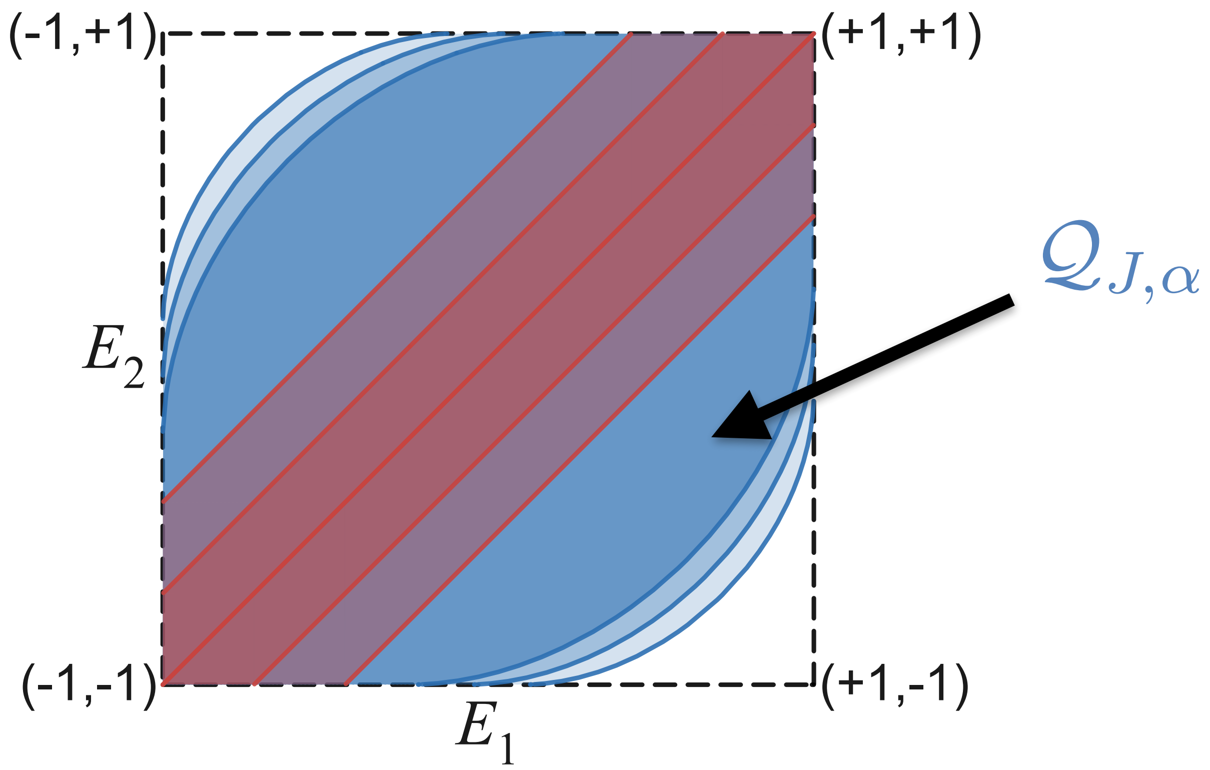
We do not know whether $\mathcal{Q}_1 = \mathcal{R}_1$,
but numerics suggests equality!



Boxes for only **two** input angles

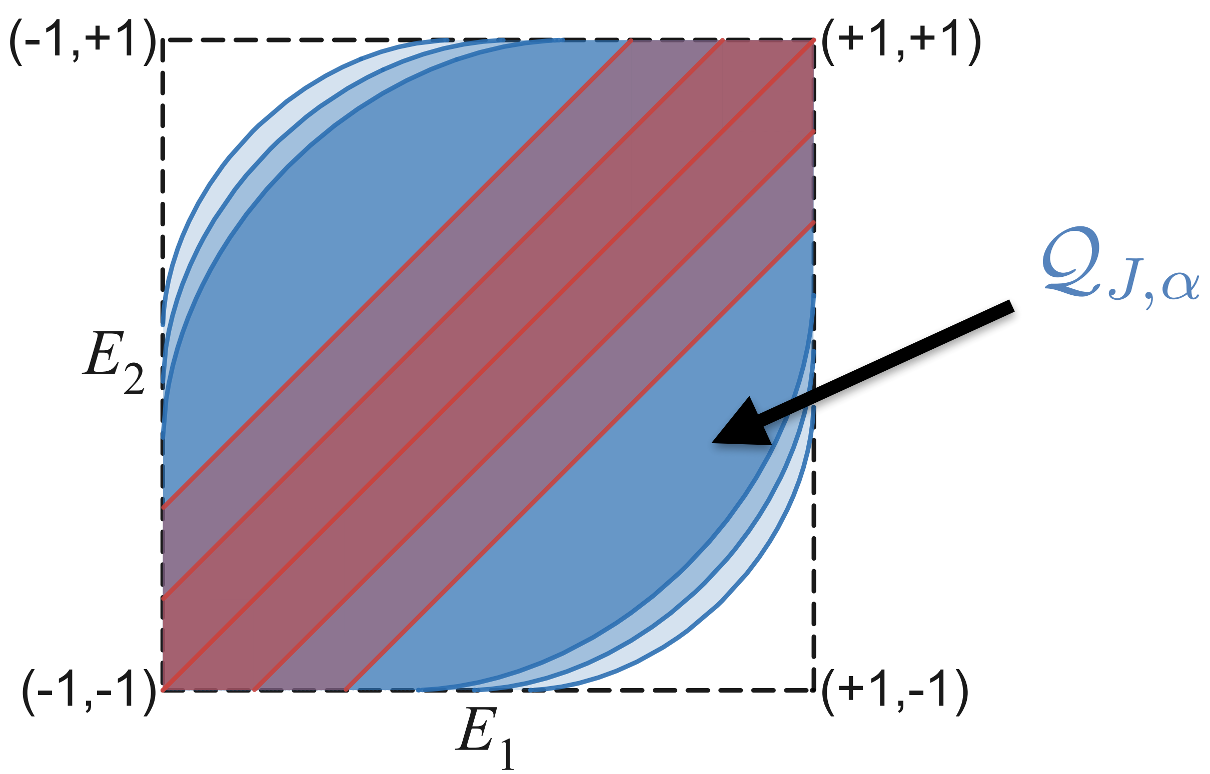
Boxes for only **two** input angles

$$\mathcal{Q}_{J,\alpha} = \{(E_1, E_2) \quad | \quad E_1 = P(+1|0) - P(-1|0), E_2 = P(+1|\alpha) - P(-1|\alpha),$$
$$P \text{ is some spin-J quantum box}\},$$



Boxes for only **two** input angles

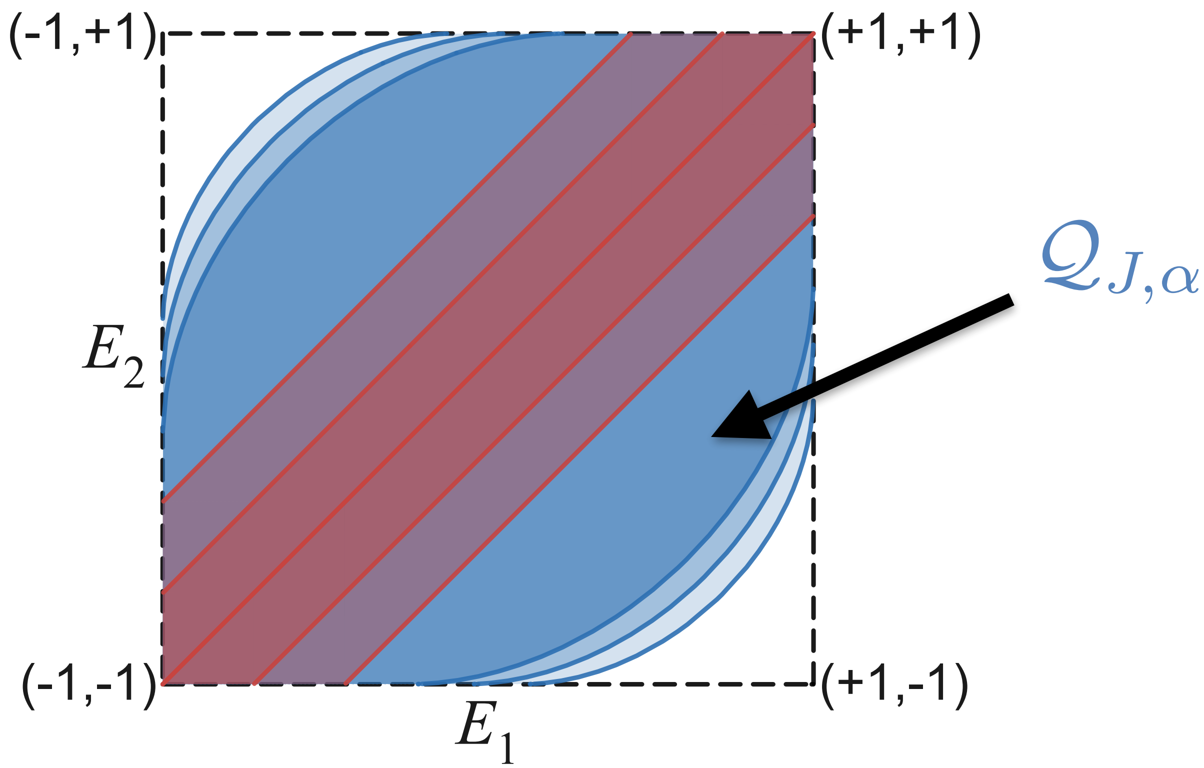
$$\mathcal{Q}_{J,\alpha} = \{(E_1, E_2) \quad | \quad E_1 = P(+1|0) - P(-1|0), E_2 = P(+1|\alpha) - P(-1|\alpha),$$
$$P \text{ is some spin-J quantum box}\},$$



$$\mathcal{R}_{J,\alpha} = \{(E_1, E_2) \quad | \quad E_1 = P(+1|0) - P(-1|0), E_2 = P(+1|\alpha) - P(-1|\alpha),$$
$$P \text{ is some spin-J rotation box}\}$$

Boxes for only **two** input angles

$$\mathcal{Q}_{J,\alpha} = \{(E_1, E_2) \quad | \quad E_1 = P(+1|0) - P(-1|0), E_2 = P(+1|\alpha) - P(-1|\alpha),$$
$$P \text{ is some spin-J quantum box}\},$$

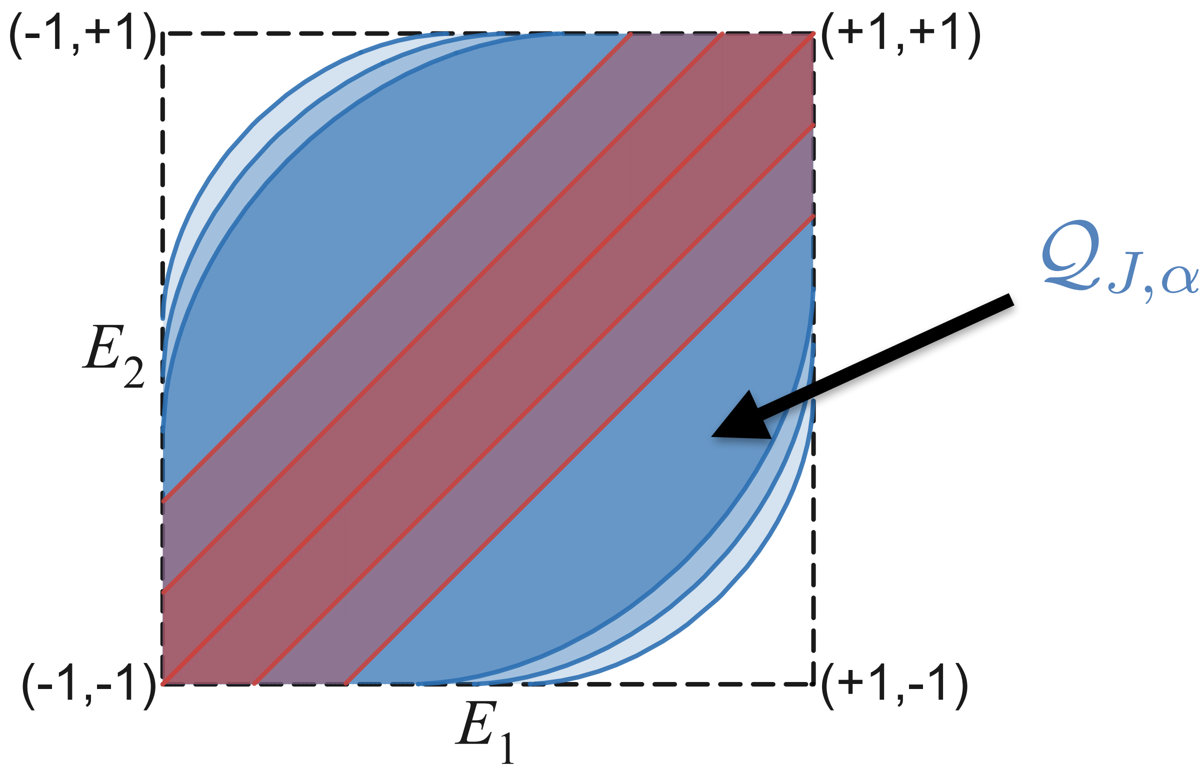


$$\mathcal{R}_{J,\alpha} = \{(E_1, E_2) \quad | \quad E_1 = P(+1|0) - P(-1|0), E_2 = P(+1|\alpha) - P(-1|\alpha),$$
$$P \text{ is some spin-J rotation box}\}$$

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

Boxes for only **two** input angles

$$\mathcal{Q}_{J,\alpha} = \{(E_1, E_2) \quad | \quad E_1 = P(+1|0) - P(-1|0), E_2 = P(+1|\alpha) - P(-1|\alpha), \\ P \text{ is some spin-J quantum box}\},$$



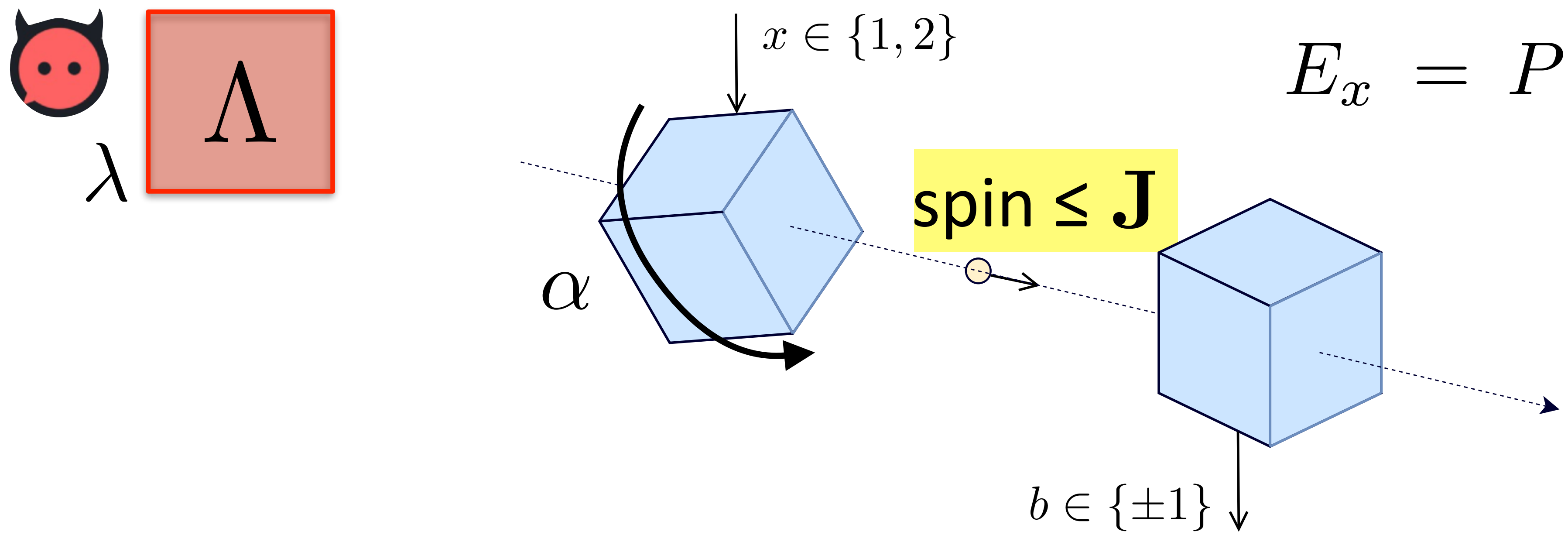
$$\mathcal{R}_{J,\alpha} = \{(E_1, E_2) \quad | \quad E_1 = P(+1|0) - P(-1|0), E_2 = P(+1|\alpha) - P(-1|\alpha), \\ P \text{ is some spin-J rotation box}\}$$

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

We do not need to assume QT to derive the blue set of correlations!

Consequences of $\mathcal{Q}_{J,\alpha} = \mathcal{R}_{J,\alpha}$

Consequences of $\mathcal{Q}_{J,\alpha} = \mathcal{R}_{J,\alpha}$



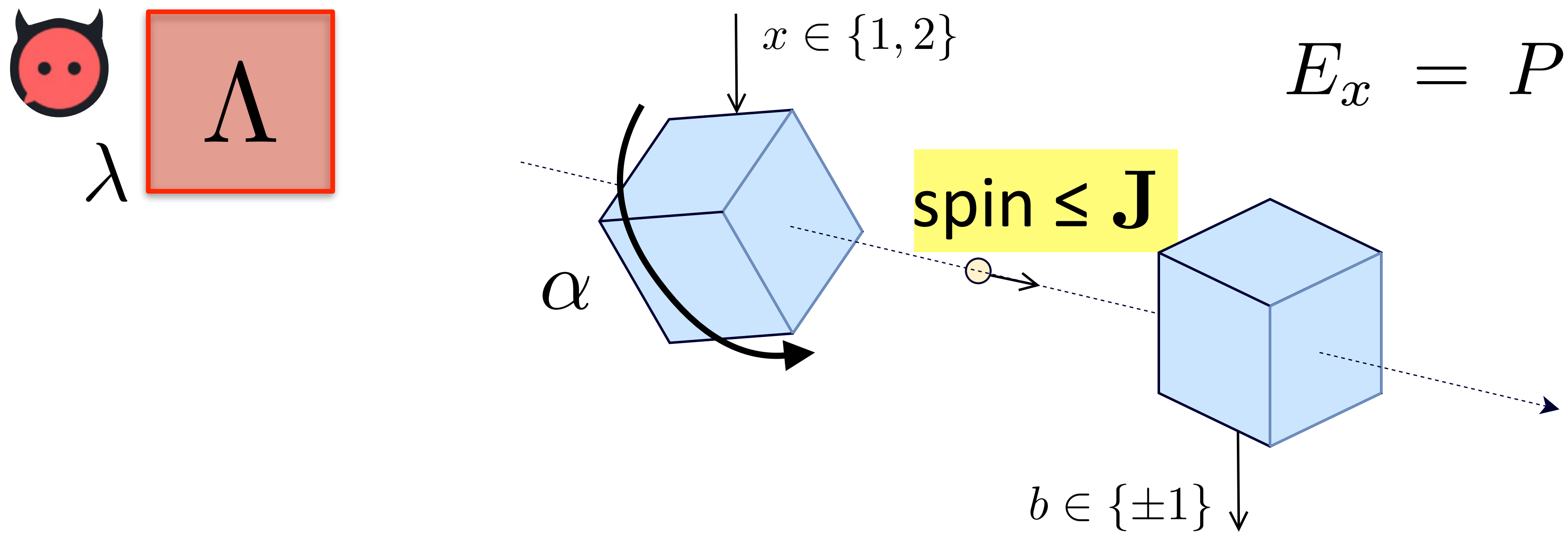
$$E_x = P(+1|x) - P(-1|x)$$

$$P(b|x)$$

Theorem. The following correlations are possible:

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

Consequences of $\mathcal{Q}_{J,\alpha} = \mathcal{R}_{J,\alpha}$



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

$$P(b|x)$$

Theorem. The following correlations are possible:

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

All results for our protocol remain valid beyond QT:

- The set of correlations,
- the number of certifiable random bits,
- security against eavesdropper with classical side information…

… and this may include information about **beyond-quantum systems** that are sent between the devices (whose average is quantum).

Overview

1. Motivations: QG and device-independent QIT

2. Our protocol, and its quantum analysis

3. Rotation boxes beyond quantum theory

4. Conclusions

Overview

1. Motivations: QG and device-independent QIT

2. Our protocol, and its quantum analysis

3. Rotation boxes beyond quantum theory

4. Conclusions

Conclusions

- Modest approach complementing direct QG approaches: use SDI quantum information to study the **relation between spacetime and QT**.
- Simplest setup: rotations around fixed axis, but can study more general setups. **"Spacetime boxes"**.

$$\mathrm{SO}(2) \subset \mathrm{SO}(3) \subset \mathrm{SO}(3,1)$$

- Result: protocols can be formulated and analyzed without assuming QT. Sets of correlations agreed in our case!
  $\longrightarrow$ Many actual experiments work on spatiotemporal DOFs. Our approach may admit a **theory-agnostic analysis** and security proofs.
- Spacetime structure determines part of quantum correlations.

arXiv:2210.14811