Semi-device-independent information processing with spatiotemporal degrees of freedom

Andrew J. P. Garner,1 Marius Krumm,1,2 and Markus P. Müller1,3

1Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria
2Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria
3Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada

Dated: February 3, 2020

Nonlocality, as demonstrated by the violation of Bell inequalities, enables device-independent cryptographic tasks that do not require users to trust their apparatus. In this article, we consider devices whose inputs are spatiotemporal degrees of freedom, e.g. orientations or time durations. Without assuming the validity of quantum theory, we prove that the devices’ statistical response must respect their input’s symmetries, with profound foundational and technological implications. We exactly characterize the bipartite binary quantum correlations in terms of local symmetries, indicating a fundamental relation between spacetime and quantum theory. For Bell experiments characterized by two input angles, we show that the correlations are accounted for by a local hidden variable model if they contain enough noise, but conversely must be nonlocal if they are pure enough. This allows us to construct a “Bell witness” that certifies nonlocality with fewer measurements than possible without such spatiotemporal symmetries, suggesting a new class of semi-device-independent protocols for quantum technologies.

I. INTRODUCTION

Quantum theory radically challenges our classical intuitions. A famous example is provided by the violation of Bell inequalities [1–6], demonstrating that local hidden variable models are inadequate to account for all observable correlations in quantum theory. While this so-called nonlocality was initially of foundational concern, it transpires to have a very powerful practical use: it enables device-independent protocols in quantum information theory (e.g. [7–10]). In this paradigm, one can perform certain tasks (e.g. cryptography) without trusting one’s apparatus, or even necessarily assuming the full formalism of quantum mechanics. These protocols rely on the readily believable no-signalling constraint, which forbids the instantaneous transmission of information between sufficiently distant laboratories. Since this constraint originates in special relativity, it may be thought of as a property of spacetime itself.

A pillar of the device-independent formalism is its abstract black box description: experimental devices are fully characterized by probability tables of outputs given a supplied input (figure 1a). In this article, we supplement these inputs with physical structure, and adopt a semi-device-independent approach that makes no assumptions about the inner workings of the devices, or the physical theories governing them (i.e. quantum or otherwise), but assumes that their ensemble statistics can be characterized by a finite number of parameters. Specifically, we consider when inputs are spatiotemporal degrees of freedom, e.g. some orientation in space or duration of time. This includes, for example, the bias of a magnetic field, duration of a Rabi pulse, or angle of a polarizer (figure 1b). Spatiotemporal degrees of freedom bring with them a symmetry structure, which can be mathematically described using Lie group theory.

In this article, we introduce a general framework for spatiotemporal black boxes. We prove that the probability tables associated with spatiotemporal inputs must encode a linear representation of the corresponding

![FIG. 1: Bell scenario: abstract vs. spatiotemporal inputs. Spatially-separate Alice and Bob independently choose measurement settings x, y and receive some outputs a, b, yielding the joint conditional probability distribution P(a, b | x, y). (a) In the usual black box formalism, the inputs x and y are abstract labels. (b) Here, we consider the physical situation where the inputs are spatiotemporal degrees of freedom (e.g. angles x = α, y = β of polarizers).](image-url)
II. RESULTS

A. Representation theorem for spatiotemporal degrees of freedom

The device-independent formalism abstracts experiments into a table of output statistics conditional on some choice of input. This is imbued with *causal structure* \([13]\) by separating the inputs and outputs into local choices and responses made and observed by different local agents, acting in potentially different locations and times. The simplest structure is one agent at a single point in time. More commonly considered is the *Bell scenario* \([6]\), where two spatially separated agents each independently select an input (measurement choice) and record the resulting local output. Theorem 3 of this paper applies to *any* casual structure, but looking towards application the later examples will use the Bell scenario.

Here, we shall consider experiments where the local inputs correspond to *spatiotemporal* degrees of freedom: for example, the direction of inhomogeneity of a magnetic field in a Stern–Gerlach experiment, or the angle of a polarization filter (figure 1b). Crucially, we will describe such experiments without assuming the validity of quantum mechanics.

Let us first consider a single laboratory, say, Alice’s. For concreteness, assume for the moment that Alice’s input is given by the direction \(\vec{x}\) of a magnetic field. She chooses her input by applying a rotation \(R \in SO(3)\) to some initial magnetic field direction \(\vec{x}_0\), i.e. \(\vec{x} = R\vec{x}_0\). Her statistics of obtaining any outcome \(a\) will now depend on this direction, giving her a *black box* \(P(a | \vec{x})\).

In general, Alice will have a set of inputs \(X\) and a symmetry group \(G\) that acts on \(X\). Given some arbitrary \(x_0 \in X\), we assume that Alice can generate every possible input \(x \in X\) by applying a suitable transformation \(R \in G\), such that \(x = Rx_0\). Mathematically, \(X\) is then a *homogeneous space* \([14]\), which can be written \(X = G/H\), where \(H \subseteq G\) is the subgroup of transformations \(R'\) with \(R'x_0 = x_0\). In the example above, \(G = SO(3)\) describes the full set of rotations that Alice can apply to \(x_0\), while \(H = SO(2)\) describes the subset of rotations that leave \(x_0\) invariant (i.e. the axial symmetry of the magnetic field vector). Then, \(X = SO(3)/SO(2) = S^2\) is the 2-sphere of unit vectors (i.e. directions) in 3-dimensional space. Similarly, the polarizer (figure 1b) corresponds to \(G = SO(2)\), \(H = \{1\}\), and \(X = S^1\), which we identify with the unit circle.

Temporal symmetries also fit into this formalism. Suppose Alice’s input corresponds to letting her system evolve for some time, then \(G = (R, +)\) is the group of *time translations*. If we know that the system evolves periodically over intervals \(\tau \in \mathbb{R}^+\), which we model as a symmetry subgroup \(H = (\tau \cdot \mathbb{Z}, +)\), then the input domain \(X = G/H \simeq S^1\). Physically, this could correspond to applying a controlled-duration Rabi pulse to an atomic system of trusted periodicity before recording an outcome.

Now suppose Alice has a black box \(P\), where on spatiotemporal input \(x \in X\), the outcome \(a\) is observed with probability \(P(a | x)\). Then, Alice can “rotate” her apparatus by \(R \in G\), and induce a new black box \(P'\) with output probabilities \(P'(a|x) = P(a|R x)\). Physically, \(R\) could be an active rotation within Alice’s laboratory (e.g. spinning a polarizer), or the incident system (e.g. adding a phase plate), or could be a passive change of coordinates.

Thus, a given black box and a spatiotemporal degree of freedom defines a family of black boxes, and transformations \(R \in G\) map a given black box to another one in this family. Suppose we denote the action of \(R\) on the black boxes by \(T_R : P \mapsto P'\). If rotating the input first by \(R\) then by \(R'\) is equivalent to a single rotation \(R'' = R' \circ R\), it follows the black box formed by applying \(T_R\) and then \(T_{R'}\) is equivalent to applying the single transformation \(T_{R''} = T_{R'} \circ T_R\) on \(P\). We can say more about this action if we consider ensembles of black boxes. For any family of black boxes \(\{P_i\}_{i=1}^n\) and probabilities \(\{\lambda_i\}_{i=1}^n\), \(\sum \lambda_i = 1\), \(\lambda_i \geq 0\), the experiment of first drawing \(i\) with probability \(\lambda_i\) and then applying black box \(P_i\), defines a new, effective black box \(P\), with statistics \(P(a|x) = \sum \lambda_i P_i(a|x)\). All these black boxes are in principle operationally accessible to Alice. However, a priori, we cannot say much about the resulting set of boxes – it could be a complicated uncountably-infinite-dimensional set defying simple analysis. Thus, we make a minimal assumption that this set is not “too large”:

**Assumption (i).** Ensembles of black boxes can be characterized by a finite number of parameters.

The mathematical consequence is that the space of possible boxes for Alice is finite-dimensional. This is a weaker abstraction of a stronger assumption typically made in the *semi-device-independent* framework of quantum information: that the systems involved in the protocols are described by Hilbert spaces of bounded (usually small) dimension \([15, 16]\). For example, BB84 \([17]\) quantum cryptography assumes that the information carriers are two-dimensional, excluding additional degrees of freedom that could serve as a side channel for eavesdroppers \([18]\). Assumption (i) is much weaker; it does not presume that we have Hilbert spaces in the first place. It is for this assumption (and not the spatiotemporal structure of the input space) that the results presented in this article lie in the *semi-device-independent* regime.

We thus arrive at our first theorem. Recall that Alice chooses her input \(x_R \in X\) by selecting some \(R \in G\) and applying it to a default input \(x_0\), i.e. \(x = R x_0\). Then:

**Theorem 1.** There is a representation of the symmetry group \(G\) in terms of real orthogonal matrices \(R \mapsto T_R\), such that for each outcome \(a\), the outcome probabilities \(P(a | x_R)\) are a fixed (over \(R\)) linear combination of matrix entries of \(T_R\).

The proof is given in appendix \([A]\) and is based on the observation that \(T_R\) becomes a linear group representation on the space of ensembles. Motivated by this characteristic response, we refer to black boxes whose inputs are selected through the action of \(G\) as *G-boxes*. 

A few comments are in order. First, this theorem applies to any causal structure, including the case of two parties performing a Bell experiment. If Alice and Bob have inputs and transformations $X_A$, $G_A$ and $X_B$, $G_B$ respectively, then the full setup can be seen as an experiment with $\mathcal{X} = X_A \times X_B$ and $\mathcal{G} = G_A \times G_B$, to which Theorem 1 applies directly.

Secondly, there may be more than one transformation that generates the desired input $x$, i.e. both $x = R_0 x_0$ and $x = R' x_0$ for $R \neq R'$; this is precisely the case if $R^{-1} R' \in H$. For example, a magnetic field can be rotated from the $y$- to $z$-direction in many different ways. In this case, Theorem 1 applies to both $R$ and $R'$, which yields additional constraints.

Finally, quantum theory is contained as a special case. Typically, one argues that due to preservation of probability, transformations $R$ must be represented in quantum mechanics via unitary matrices $U_R$ acting on density matrices via $\rho \mapsto U_R \rho U_R^\dagger$. This projective action can be written as an orthogonal matrix on the real space of Hermitian operators, in concordance with Theorem 1.

As a specific example, consider a quantum harmonic oscillator with frequency $\omega$, initially in state $\rho_0$, left to evolve for a variable time $t$ before it is measured by a fixed POVM $\{M_a\}_{a \in A}$. The free dynamics are given by the Hamiltonian $H$, whose discrete set of eigenvalues $\{E_n = \hbar \omega (\frac{1}{2} + n)\}$ correspond to allowed “energy levels”. The evolution is periodic, so (recalling earlier) $G = (\mathbb{R}, +)$, $\mathcal{H} = (\frac{\mathbb{R}}{2\pi} \times \mathbb{Z}, +)$ and $X \simeq S^1$. The associated black box is thus $P(\alpha| t) = | \text{Tr} \left[ M_a \exp (-\frac{iHt}{\hbar}) \rho_0 \exp (\frac{iHt}{\hbar}) \right] |$. For any given $\rho_0$ and $M_a$, this evaluates to an affine-linear combination of terms of the form $\cos (\frac{n-m}{2}\hbar t)$ and $\sin (\frac{n-m}{2}\hbar t)$, involving all pairs of energy levels that have non-zero occupation probability in $\rho_0$ (and non-zero support in $M_a$). This is a linear combination of entries of the matrix representation

$$T_t = \bigoplus_{\alpha = E_n - E_m} \begin{pmatrix} \cos(\alpha t) & \sin(\alpha t) \\ -\sin(\alpha t) & \cos(\alpha t) \end{pmatrix},$$

in accordance with Theorem 1. For $T_t$ to be a finite matrix, there must only be a finite number of occupied energy differences $E_m - E_n$.

Here, Assumption 1 is equivalent to an upper (and lower) bound on the system’s energy. In the general framework that does not assume the validity of quantum mechanics (or presuppose trust in our devices, or our assignment of Hamiltonians), we can view Assumption 1 as a natural generalization of this to other symmetry groups and beyond quantum theory. By assuming a concrete upper bound on the representation label (such as $\alpha$ in eq. 1), we can establish powerful theory- and device-independent consequences for the resulting correlations, as we will now demonstrate by means of several examples.

### 2. Example: Two angles and Bell witnesses

Let us consider the simplest non-trivial spatio-temporal freedom, where Alice and Bob each have the choice of a single continuous angle: respectively $\alpha, \beta \in [0, 2\pi]$, and each obtain a binary output $a, b \in \{+1, -1\}$. Physically, this would arise, say, in experiments where a pair of photons is distributed to the two laboratories, each of which contains a rotatable polarizer followed by a photodetector (figure 1).

Due to Theorem 1, the probabilities $P(a, b | \alpha, \beta)$ are linear combinations of matrix entries of an orthogonal representation of $SO(2) \times SO(2)$. From the classification of these representations (see appendix B 1), it follows that all $SO(2) \times SO(2)$-boxes are of the form

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

resulting in a correlation function

$$C(\alpha, \beta) := P(+1, +1 | \alpha, \beta) + P(-1, -1 | \alpha, \beta)$$

$$- P(+1, -1 | \alpha, \beta) - P(-1, +1 | \alpha, \beta)$$

$$= \sum_{m=0}^{2J} \sum_{n=-2J}^{2J} C_{mn} \cos (\alpha m - \beta n) + S_{mn} \sin (\alpha m - \beta n),$$

where $J \in \{0, \frac{1}{2}, 1, \frac{3}{2}, \ldots \}$ is some finite maximum “spin”.

If Alice and Bob’s laboratories are spatially separated, the laws of relativity forbid Alice from sending signals to Bob instantaneously. This “no-signalling” principle constrains the valid set of joint probability distributions: namely Bob’s marginal statistics cannot depend on Alice’s choice of measurement, and vice versa. However, for any given correlation function of the form eq. (1), there is always at least one set of valid no-signalling probabilities (see appendix B 2) – for example, those where the marginal distributions are “maximally mixed” such that independent of $\alpha$, $a$ is $+1$ or $-1$ with equal probability (likewise for $b$ and $b$), consistent with an observation of Popescu and Rohrlich [20].

Consider a quantum example: two photons in a Werner state $|a\rangle_1 |b\rangle_2 \rho_W := p|\psi^-\rangle\langle\psi^-| + \frac{1}{2} (1-p) I_4$ where $|\psi^-\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$ and $p \in [0, 1]$. Alice and Bob’s polarizer/detector setups are described by the observables $M_a := (\cos 2\theta, \sin 2\theta)$ for orientations $\theta = \alpha, \beta$ respectively. Then, $C(\alpha, \beta) = \text{Tr} \left( \rho_W M_a \otimes M_b \right) = -p \cos 2 \cos (\alpha - \beta)$. This fits the form of eq. (2) for $J = 1$, with $C_{22} = -p$ and all other coefficients as zero.

A paradigmatic question in this setup is whether the statistics can be explained by a local hidden variable (LHV) model. Namely, is there a single random variable $\Lambda$ over some space $\Lambda$ such that $P(a, b | \alpha, \beta) = \int_\Lambda d\Lambda P_\Lambda(\lambda) P_A(a | \alpha, \lambda) P_B(b | \beta, \lambda)$, where $P_\Lambda(\lambda)$ is a classical probability distribution, and $P_A(a | \alpha, \lambda)$ and $P_B(b | \beta, \lambda)$ are respectively Alice and Bob’s local response functions (conditioned on their input choices $\alpha$ and $\beta$ and the particular realization of the hidden
variable $\lambda$? If no LHV model exists, then the scenario is said to be nonlocal. Famously, Bell’s theorem shows that quantum theory admits correlations that are nonlocal in this sense [1, 2]. This follows from the violation of Bell inequalities that are satisfied by all distributions with LHV models, the archetypical example being the Clauser–Horne–Shimony–Holt (CHSH) inequality [3]:

$$|C(\alpha_1, \beta_2) + C(\alpha_2, \beta_2) + C(\alpha_3, \beta_3) - C(\alpha_1, \beta_1)| \leq 2, \quad (5)$$

where $\alpha_1, \alpha_3$ are two choices of Alice’s angle, and $\beta_2, \beta_3$ of Bob’s. Classical systems always satisfy this bound, but quantum theory admits states and measurements that violate it. When working with a continuous parameter, Bell inequalities need not be limited to a subset of angles, but can also be formulated as a functional of the entire correlation function [23, 24].

Not all correlations of the form in eq. (1) are allowed by quantum theory. For example, “science fiction” polarizers with the correlation function $C(\alpha, \beta) = \frac{3}{4} \cos[3(\alpha - \beta)] - \cos[\alpha - \beta]$ would yield a CHSH value of 3.63, under choices of angles $\alpha_1 = 1.5, \alpha_3 = 0, \beta_2 = 3.9$ and $\beta_3 = 2.3$, violating quantum theory’s maximum achievable value of $2\sqrt{2} = 2.828$. With this general form, we can make broad statements about whether correlations are local or nonlocal. First, if the correlations are sufficiently “noisy”, we can systematically construct a LHV model by generalizing a procedure by Werner [21] (see appendix B). If the only constraint on the correlations is that it has some maximum $J$, then the existence of a LHV model implies the following protocol:

If no LHV model exists, then one can systematically construct a (Braunstein–Caves [25]) Bell inequality that will be violated (see appendix B). Specifically, “near perfect” means that for a given $J$, $C_{\text{rel}}(\Theta_+) \geq 1 - \varepsilon_J$ with

$$\varepsilon_J := -K_J + \sqrt{K_J^2 + \frac{\Delta^2}{4}} = \frac{\Delta^2}{8K_J} + \mathcal{O}(K_J^{-2}), \quad (7)$$

where $K_J := \sqrt{2\pi^2 J(2J+1)(4J+1)/3}$, and $C_{\text{rel}}(\Theta_-) \leq 1 - \Delta$ bounds the “other” value measured at $\Theta_-$. (See appendix B for proof).

We summarize these results (see also figure 2):

**Theorem 2.** Consider a two-angle Bell experiment with correlations $C$ in the form of eq. (4), with an upper bound $J$ on the representation labels.

A. If $C$ is sufficiently “noisy”, in the sense that

$$\max_{\alpha, \beta} |C(\alpha, \beta) - C_{00}| \leq \gamma_J (1 - |C_{00}|) \quad (8)$$

with $\gamma_J$ as in eq. (6), then the correlations can always be exactly accounted for by a LHV model.

B. If the relational part of $C$ is sufficiently “pure” for some angle $\Theta_+$ (above $1 - \varepsilon_J$, as defined in eq. (7)), but also sufficiently different (below $1 - \Delta$) for some other angle $\Theta_-$, then the correlations violate a Bell inequality.

![FIG. 2: Two-angle relational correlation functions.](image)

A “sufficiently noisy” correlation function can always be reproduced exactly by a LHV model (Theorem 2). This is represented by the green curve completed contained within the central green-shaded region (drawn for $C_{00} = 0$). Conversely, if the function is “pure enough”, then it must be nonlocal (Theorem 2). This is represented by the blue curve with values in both extremal blue-shaded regions. Not all curves can be realized within quantum theory, but simple sinusoidal curves certainly can (such as the dashed black curve), following from Theorem 3 in two dimensions.

This is a powerful result: with a choice between two experimental settings for Alice, and no choice made by Bob, we can witness nonlocality. This can be done by the following protocol:

- Alice and Bob share some random angle $\lambda$, uniformly distributed in the interval $[0, 2\pi]$.
- Alice chooses locally freely between the two possible angles $\alpha \in \{\Theta_+, \Theta_-\}$. 

Subject to extra restrictions that keep the form of $C$ simple, more permissive bounds are also derived. For instance, if there is only one non-zero coefficient in eq. (1), then $\gamma = \sqrt{2}/\pi \approx 0.4502$. Recall the correlation function for projection measurements on a Werner state, 

\[-p \cos [2(\alpha - \beta)],\]

and identify $\gamma$ with $p$. In this case, our bound is comparable with that in Hirsch et al. [26] of $p \sim 0.6829$.

Conversely, we can give a simple sufficient criterion for nonlocality if we separate the terms in eqs. (2) and (3) into relational and non-relational components. The relational components where $m = n$ account for behaviour that depends only on the difference between the two angles. Purely relational correlations, i.e. ones with $C(\alpha, \beta) = C(\alpha - \beta)$, can be motivated by symmetry (i.e. that in the absence of external references, only the relative angle should have operational meaning). Here, the $J = \frac{1}{2}$ case contains the bipartite rotational invariant correlations discussed in Nagata et al. [27]. Conversely, the correlations resulting from any experiment can be actively made relational as we will describe in more detail below.

If the relational part of a correlation function $C_{\text{rel}}$ has an angle difference $\Theta_+$, which results in near perfect (anti-)correlations, and another angle difference $\Theta_-$ that does not, then one can systematically construct
• Alice now inputs $\alpha + \lambda$ into her half of the box, while Bob inputs $\lambda$.
• By repeating the protocol, they determine the correlations $C_{\text{rel}}(\Theta_+)$ and $C_{\text{rel}}(\Theta_-)$, and verify that they violate the inequality above.

Randomization over $\lambda$ effectively projects $C$ onto its relational part $C_{\text{rel}}(\alpha,\beta) = \frac{1}{2d} \int d\lambda C(\alpha + \lambda,\beta + \lambda)$, which only depends on $\alpha - \beta$. The protocol above fixes $\beta$ to zero, while $\alpha \in \{\Theta_+,\Theta_-\}$. This is sufficient to determine the two correlation values.

The protocol assumes that Alice and Bob have some physically motivated promise on the maximum representation label $J$ (e.g. by assuming an upper bound on the total energy of the system, or the number of elementary particles transmitted), and that they know the angles $\Theta_+$ and $\Theta_-$ beforehand. The latter assumption is analogous to standard Bell experiments, where the relevant measurement settings are assumed to be known.

Witnessing Bell nonlocality is not the same as directly demonstrating nonlocality (i.e. collecting all the statistics for a Bell test, which is only possible if Bob has some free choice too) but rather, subject to Assumption \[3\] implies the existence of an experiment that would demonstrate nonlocality. In contrast to a full Bell experiment, a Bell witness has the advantage of being experimentally easier to implement: the protocol above allows one to witness nonlocality with only two measurement settings instead of four. Note that only making the correlation function relational (i.e. going from $C$ to $C_{\text{rel}}$ as above) without any additional assumption on $J$ is not sufficient to obtain this reduction, as we show in appendix \[B\].

Our protocol hence demonstrates that natural assumptions on the response of devices to spatiotemporal transformations can give additional constraints that allow for the construction of new Bell witnesses. This opens up the possibility of new methods of experimentally certifying nonlocal behaviour, similar to \[11\] \[12\] \[29\], but without the need to presume the validity of quantum theory or to trust all involved measurement devices.

Theorem 2 shows us that smaller values of $J$ (and hence “simpler” responses to changes in angles) result in more permissive bounds for finding LHV models, or witnessing non-locality. In our next example, we shall move from angles (SO(2)) to directions (SO(d)), but consider arguably the simplest non-trivial response.

C. Example: Characterizing quantum correlations

For our last example, we shall apply our framework to characterize the set of correlations that can be realized by two parties sharing a quantum state, each locally choosing one of two binary-outcome measurements – the thus called quantum “(2,2,2)"-behaviours. The set of quantum (2,2,2)-behaviours $\mathcal{Q}$ is a strict superset of the classical (2,2,2)-behaviours $\mathcal{C}$ (i.e. those admitting a LHV model). However, the set of all no-signalling behaviours $\mathcal{NS}$ is strictly larger: $\mathcal{C} \subseteq \mathcal{Q} \subseteq \mathcal{NS}$ \[20\] \[40\]. This has led to the search for simple physical or information-theoretic principles that would explain “why” nature admits no more correlations than in $\mathcal{Q}$. Several candidates have been suggested over the years, including information causality \[31\], macroscopic locality \[32\], or non-trivial communication complexity \[33\], but none of these have been able to single out $\mathcal{Q}$ uniquely \[34\].

Here, we will provide such a characterization by considering black boxes that transform in arguably the simplest manner. Over a spherical input domain $\mathcal{X} = S^{d-1}$ an SO(d)-box $P(a | x)$ is said to transform fundamentally if the representation matrix $T_R$ in Theorem 1 can be chosen as the block matrix $\mathbb{1} \oplus R$, where $\mathbb{1} := (1)$ and $R$ is the fundamental representation of SO(d) (e.g. for $d = 3$, $\{R\}$ are the familiar rotation matrices). Consequently, a black box that transforms fundamentally has an affine representation, $P(a | x) = c^a_0 + c^a_1 \cdot x$ where $x \in S^{d-1}$ is the input, and $c^a_0 \in \mathbb{R}^+$, $c^a_1 \in \mathbb{R}^d$ (proof in appendix \[C\]).

Motivated by symmetry, we consider a class of unbiased black boxes that do not prefer any particular output when averaged over all possible inputs. This implies that $c^a_0 = 1/|A|$ for every $a$. For example, this symmetry holds for measurements on quantum spin-$\frac{1}{2}$ particles: spin $+\frac{1}{2}$ in one direction is the same as spin $-\frac{1}{2}$ in the opposite, and hence neither outcome is preferred on average.

Imagine Alice and Bob residing in $d$-dimensional space ($d \geq 2$), sharing a non-signalling box $P(a,b | x,y)$, where both inputs $x, y \in S^{d-1}$ are spatial directions, and $a,b$ each can take two values. Suppose that their conditional boxes transform fundamentally and are unbiased. A conditional box $P^{x,y}_{A,B}(a | x) := P(a,b | x,y) / P_B(b | y)$ describes the local black box Alice would have if she was told Bob’s measurement choice $y$ and outcome $b$. If all conditional boxes for Alice and Bob transform fundamentally, then the bipartite box is said to transform fundamentally locally. Similarly, if all conditional boxes are unbiased, $P(a,b | x,y)$ is said to be locally unbiased.

Surprisingly, these local symmetries severely constrain the global correlations: they allow for only and exactly those correlations that can be realized by two parties who share a quantum state and choose between two possible two-outcome quantum measurements each—the quantum (2,2,2)-behaviours:

Theorem 3. The quantum (2,2,2)-behaviours are exactly those that can be realised by binary-outcome bipartite SO(d)×SO(d)-boxes that transform fundamentally locally and are locally unbiased, restricted to two choices of input direction per party per box, and statistically mixed via shared randomness.

The proof is given in appendix \[C\].

A few remarks are in place. First, the unbiasedness refers to the total set $S^{d-1}$ of possible inputs per party, not to the two inputs to which the box is restricted. Even if the unrestricted behaviour is unbiased in the sense described above, the resulting (2,2,2)-behaviour
can be biased. Secondly, this unbiasedness of the underlying \( SO(d) \times SO(d) \)-box is necessary to recover the quantum correlations – without it, one can realize arbitrary nonsignalling correlations, including PR-box behaviour, in a way that still transforms locally fundamentally (we give an example in appendix C). Finally, shared randomness is necessary to realize explicitly non-extremal quantum correlations by such boxes, following on the observation that the set of \((2,2,2)\)-behaviours realizable by POVMs on two qubits is not convex [35, 36]. Namely, if both parties share the \((2,2,2)\)-behaviours \(P_0\) and \(P_1\) and a random bit \(c \in \{0,1\}\) that equals 0 with probability \(\lambda\), they can statistically implement the mixed behaviour \(\lambda P_0 + (1 - \lambda) P_1\) by feeding their inputs into box \(P_c\).

For \(n = 2\) parties with \(m = 2\) measurements and \(k = 2\) outcomes each, our result provides a characterization of the quantum set. Although Theorem 3 cannot be extended to general \((m,n,k)\)-behaviours [37] without modification, this result shows that our framework of \(G\)-boxes offers a very natural perspective on physical correlations, and reinforces earlier observations that hint at a deep fundamental link between the structures of spacetime and quantum theory [38, 41].

### III. DISCUSSION AND OUTLOOK

We have introduced a general framework for semi-device-independent information processing, without assuming quantum mechanics, for black boxes whose inputs are degrees of freedom that break spatiotemporal symmetries. Such black boxes have characteristic probabilistic responses to symmetry transformations, and natural assumptions about this behaviour can certify technologically important properties like the presence or absence of Bell correlations.

Specifically, we have shown that the quantum \((2,2,2)\)-behaviours can be exactly classified as those of bipartite boxes that transform locally in the simplest possible way – by the fundamental representation of \(SO(d)\) rotations, respecting the unbiasedness of outcomes. For Bell experiments with \(SO(2) \times SO(2)\)-boxes, we have shown that correlations that are quantifiably “noisy enough” always admit a local hidden variable model, whereas relational correlations for which there are settings with differing “purity” must violate a Bell inequality. Since the underlying technical tools (e.g. Schur orthogonality [42]) hold in greater generality, many of our results could be applied to other groups.

Furthermore, these results have allowed us to construct a protocol to witness the violation of a Bell inequality within a causal structure that is otherwise too simple to admit the direct detection of nonlocality. We believe that our approach can be applied to experimental settings, such as the recent demonstration of Bell correlations in a Bose–Einstein condensate [12], and potentially eliminate the necessity to trust all detectors or to assume the exact validity of quantum mechanics. Many of these experiments do work with spatiotemporal inputs like Rabi pulses, which makes our approach particularly natural for analyzing them.

We have predominantly worked under the assumption that ensembles of black boxes are characterized by a finite number of parameters, and – more specifically – that an upper bound on the representation label (say, the “spin” \(J\)) of the boxes is known. On one hand, this assumption can likely be weakened, by employing group-theoretic results such as the Peter–Weyl theorem [42]. On the other hand, we have argued that this assumption is natural: it is weaker than assuming a Hilbert space with bounded dimension (standard in the semi-device-independent framework [16]) and constitutes a generalization of an “energy bound” beyond quantum theory (cf. [43]). Moreover, it incorporates an intuition conceptually closer to particle physics: to quantify the potential eavesdropping side channels, one might not count Hilbert space dimensions, but rather representation labels, since these are intuitively (and sometimes rigorously) related to the total number of particles.

Our framework opens up several potential avenues for future work. First, as the witness example demonstrates, our formalism hints at novel semi-device-independent protocols based on assumptions with firmer physical motivation than the usual dimension bounds. In contrast to recent proposals for using energy bounds [14, 16], our assumption on the devices’ symmetry behaviour does not presume the validity of quantum mechanics, but rather embodies a natural upper bound to the “fine structure” of the devices’ response. Meanwhile, one might apply the functional approach [23, 24] to our framework by taking Haar integrals over spatiotemporal input spaces to derive a device-independent family of generalized Bell–Zukowski inequalities for various limits of fine structure.

Secondly, our framework informs novel experimental searches for conceivable physics beyond quantum theory. Previous proposals (e.g. superstrong nonlocality [20] or higher-order interference [47, 48]) have simply described the probabilistic effects without predicting how they could actually occur within spacetime as we know it. This has made the search for such effects seem like the search for a needle in a haystack [49]. Our formalism promises a more direct spatiotemporal description of such effects – hopefully leading to predictions that are more tied to experiments and in greater compatibility with spacetime physics.

Combining the principles of quantum theory with special relativity has historically been an extremely fruitful strategy. Here, we propose to extend this strategy to device-independent quantum information and even beyond quantum physics. In principle, suitable extensions of our framework would allow us to address questions such as: which probability rules are compatible with Lorentz invariance? Any progress on these kind of questions has the potential to give us fascinating insights into the logical architecture of our physical world.
ACKNOWLEDGMENTS

We are grateful to Miguel Navascués, Matt Pusey, and Valerio Scarani for discussions. This project was made possible through the support of a grant from the John Templeton Foundation. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation. We acknowledge the support of the Austrian Science Fund (FWF) through the Doctoral Programme CoQuS. This research was supported in part by Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported by the Government of Canada through the Department of Innovation, Science and Economic Development Canada and by the Province of Ontario through the Ministry of Research, Innovation and Science.

[1] A. Einstein, B. Podolsky, and N. Rosen, “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?” [Physical Review 47, 777–780 (1935)]
[2] J. S. Bell, “On the Einstein Podolsky Rosen paradox,” Physics Physique Fizika 1, 195–200 (1964)
[3] J. Clauser, M. Horne, A. Shimony, and R. Holt, “Proposed Experiment to Test Local Hidden-Variable Theories,” Physical Review Letters 23, 880–884 (1969)
[4] A. Aspect, P. Grangier, and G. Roger, “Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell’s Inequalities,” Physical Review Letters 49, 91–94 (1982)
[5] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres,” Nature 526, 682–686 (2015)
[6] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, “Bell nonlocality,” Reviews of Modern Physics 86, 419–478 (2014)
[7] D. Mayers and A. Yao, “Quantum Cryptography with Imperfect Apparatus,” in Proceedings of the 39th Annual Symposium on Foundations of Computer Science (IEEE, Palo Alto, 1998).
[8] F. Hirsch, M. T. Quintino, T. Vértesi, M. Navascués, and N. Brunner, “Better local hidden variable models for two-bit Werner states and an upper bound on the Grothendieck constant \(K_2(3)\),” Quantum 1, 3 (2017)
[9] K. Nagata, W. Laskowski, M. Wieśniak, and M. Żukowski, “Rotational invariance as an additional constraint on realism,” Physical Review A 84, 010302 (2011)
[10] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Vol. 3 (1984) pp. 175–179.
[11] A. Acín, N. Gisin, and Ll. Masanes, “From Bell’s Theorem to Secure Quantum Key Distribution,” Physical Review Letters 97, 120405 (2006)
[12] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, 2000).
[13] A. Sen(De), U. Sen, and M. Żukowski, “Functional Bell inequalities can serve as a stronger entanglement witness than conventional Bell inequalities,” Physical Review A - Atomic, Molecular, and Optical Physics 66, 4 (2002)
[14] B. S. Cirel’son, “Quantum generalizations of Bell’s inequality,” Letters in Mathematical Physics 4, 93–100 (1980)
[15] F. Hirsch, M. T. Quintino, T. Vértesi, M. Navascués, and N. Brunner, “‘Better local hidden variable models for two-bit Werner states and an upper bound on the Grothendieck constant \(K_2(3)\)’,” Quantum 1, 3 (2017)
[16] K. Nagata, W. Laskowski, M. Wieśniak, and M. Żukowski, “Rotational invariance as an additional constraint on realism,” Physical Review A 84, 010302 (2011)
[17] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Vol. 3 (1984) pp. 175–179.
[18] A. Acín, N. Gisin, and Ll. Masanes, “From Bell’s Theorem to Secure Quantum Key Distribution,” Physical Review Letters 97, 120405 (2006)
[19] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, 2000).
[20] S. Popescu and D. Rohrlich, “Quantum nonlocality as an axiom,” Found. Phys. 24, 379–385 (1994)
[21] R. F. Werner, “Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model,” Physical Review A 40, 4277–4281 (1989)
[22] R. Augusiak, M. Demianowicz, and A. Acín, “Local hiddenvariable models for entangled quantum states,” Journal of Physics A: Mathematical and Theoretical 47, 244002 (2014)
[23] M. Żukowski, “Bell theorem involving all settings of measuring apparatus,” Physics Letters A 177, 290–296 (1993)
[24] A. Sen(De), U. Sen, and M. Żukowski, “Functional Bell inequalities can serve as a stronger entanglement witness than conventional Bell inequalities,” Physical Review A - Atomic, Molecular, and Optical Physics 66, 4 (2002)
[25] B. S. Cirel’son, “Quantum generalizations of Bell’s inequality,” Letters in Mathematical Physics 4, 93–100 (1980)
[26] F. Hirsch, M. T. Quintino, T. Vértesi, M. Navascués, and N. Brunner, “Better local hidden variable models for two-bit Werner states and an upper bound on the Grothendieck constant \(K_2(3)\),” Quantum 1, 3 (2017)
[27] K. Nagata, W. Laskowski, M. Wieśniak, and M. Żukowski, “Rotational invariance as an additional constraint on realism,” Physical Review Letters 93 (2004). 10.1103/PhysRevLett.93.230403.
[28] S. L. Braunstein and C. M. Caves, “Wringing out better Bell inequalities,” Annals of Physics 202, 22–56 (1990)
[29] Z. Wang, S. Singh, and M. Navascués, “Entanglement and Nonlocality in Infinite 1D Systems,” Physical Review Letters 118, 230401 (2017)
[30] L. A. Khalfin and B. S. Tsirel’son, “Quantum and Quasi-classical Analogs Of Bell Inequalities,” in Symposium on the foundations of modern physics, edited by P. Lahti and P. Mittelstaedt (World Scientific Publishing Co., 1985) pp. 441–460.
[31] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, “Information causality as a physical principle,” Nature 461, 1101–1104 (2009)
[32] T. H. Yang, M. Navascués, L. Sheridan, and V. Scarani, “Quantum Bell inequalities from macroscopic locality,” Physical Review A 83, 022105 (2011).

[33] G. Brassard, H. Buhrman, N. Linden, A. Mélèot, A. Tapp, and F. Unger, “Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial,” Physical Review Letters 96, 250401 (2006).

[34] M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín, “Almost quantum correlations,” Nature Communications 6, 6288 (2015).

[35] K. F. Pál and T. Vértesi, “Concavity of the set of quantum probabilities for any given dimension,” Physical Review A 80, 042114 (2009).

[36] J. M. Donohue and E. Wolfe, “Identifying nonconvexity in the sets of limited-dimension quantum correlations,” Physical Review A 92, 062120 (2015).

[37] A. Acín, R. Augusiak, D. Cavalcanti, C. Hadley, J. K. Korbicz, M. Lewenstein, Li. Masanes, and M. Piani, “Unified Framework for Correlations in Terms of Local Quantum Observables,” Physical Review Letters 104, 140404 (2010).

[38] W. K. Wootters, The acquisition of information from quantum measurements, Ph.D. thesis, University of Texas at Austin (1980).

[39] M. P. Müller and Li. Masanes, “Three-dimensionality of space and the quantum bit: an information-theoretic approach,” New Journal of Physics 15, 053040 (2013).

[40] P. A. Höhn and M. P. Müller, “An operational approach to spacetime symmetries: Lorentz transformations from quantum communication,” New Journal of Physics 18, 063026 (2016).

[41] 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,” Proceedings of the Royal Society A 473, 20170596 (2017).

[42] M. R. Sepanski, Complex Lie groups (Springer, New York, 2007).

[43] D. Branford, O. C. O. Dahlsten, and A. J. P. Garner, “On Defining the Hamiltonian Beyond Quantum Theory,” Foundations of Physics 48, 982–1006 (2018).

[44] T. van Himbeeck, E. Woodhead, N. J. Cerf, R. Garcia-Patrón, and S. Pironio, “Semi-device-independent framework based on natural physical assumptions,” Quantum 1, 33 (2017).

[45] T. Van Himbeeck and S. Pironio, “Correlations and randomness generation based on energy constraints,” arXiv:1905.09117 (2019).

[46] D. Rusca, T van Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, “Practical self-testing quantum random number generator based on an energy bound,” arXiv:1904.04819 (2019).

[47] R. D. Sorkin, “Quantum Mechanics as Quantum Measure Theory,” Modern Physics Letters A 09, 3119–3127 (1994).

[48] C. Ududec, H. Barnum, and J. Emerson, “Three Slit Experiments and the Structure of Quantum Theory,” Foundations of Physics 41, 396–405 (2010).

[49] U. Sinha, C. Couteau, T. Jennewein, R. Laflamme, and G. Weihs, “Ruling out multi-order interference in quantum mechanics,” Science (New York, N.Y.) 329, 418–21 (2010).

[50] “Finite-dimensional representation.” Encyclopedia of Mathematics. (2016).

[51] V. F. Molchanov, A. U. Klimyk, and N. Ya. Vilenkin, Representation Theory and Noncommutative Harmonic Analysis II, edited by A. A. Kirillov (Springer Verlag, 1995).

[52] M. Kleinmann, T. J. Osborne, V. B. Scholz, and A. H. Werner, “Typical Local Measurements in Generalized Probabilistic Theories: Emergence of Quantum Bipartite Correlations,” Physical Review Letters 110, 040403 (2013).

[53] H. Barnum, S. Beigi, S. Boixo, M. B. Elliott, and S. Wehner, “Local Quantum Measurement and No-Signaling Imply Quantum Correlations,” Phys. Rev. Lett. 104, 140401 (2010).

[54] Li. Masanes, “Extremal quantum correlations for N parties with two dichotomic observables per site,” arXiv:quant-ph/0512100 (2005).

[55] B. Toner and F. Verstraete, “Monogamy of Bell correlations and Tsirelson’s bound,” arXiv:quant-ph/0611001 (2006).
Appendix A: The representation of spatiotemporal degrees of freedom in black box statistics

Let us first furnish a mathematical description of a black box as an input–output process. We begin with the single party case (say, Alice). Suppose the domain of Alice’s inputs is the set $\mathcal{X}$, and of her outputs is the finite set $\mathcal{A}$. As motivated in the main text, we are interested in the case where $\mathcal{X}$ is a homogeneous space. That is, we have a group $\mathcal{G}$ that acts transitively on the set of inputs $\mathcal{X}$, such that $\mathcal{X} = \mathcal{G}/\mathcal{H}$, and $\mathcal{H} \subseteq \mathcal{G}$ is the corresponding stabilizer subgroup. The paradigmatic example is given by $\mathcal{X} = S^{d-1}$, $\mathcal{G} = SO(d)$ and $\mathcal{H} = SO(d-1) \subseteq \mathcal{G}$, such that the inputs $\vec{x} \in \mathcal{X}$ are unit vectors. Even though the inputs need not be vectors in general, we will use the vector notation in the following for convenience. We will assume that $\mathcal{G}$ is a locally compact group, such that all bounded finite-dimensional representations are unitary [50].

For such an input domain, we can assign an arbitrary “default input” $\vec{x}_0 \in \mathcal{X}$, such that every other input $\vec{x} \in \mathcal{X}$ can be written as $\vec{x} = R \vec{x}_0$ for some suitable transformation $R \in \mathcal{G}$. Physically, we can imagine that Alice chooses her input by “rotating” the default input $\vec{x}_0$ into her desired direction $\vec{x}$, and she can do so by applying a suitable rotation $R$. In general, $R$ is not unique, and Alice’s freedom of choice of transformation is given by $\mathcal{H}$.

A black box $P$ is then a map $P : \mathcal{X} \rightarrow \mathcal{R}^{[\mathcal{A}]}$ such that for $\vec{x} \in \mathcal{X}$, $P^a : \vec{x} \rightarrow P(\vec{x} | a) \subseteq \mathcal{X}$, where $P^a$ is the $a$th element of the vector map. Since for probabilities $0 \leq P(\vec{x} | a) \leq 1$, each $P^a$ is a non-negative real bounded function on $\mathcal{X}$. For probabilities, we also have the constraint that for all $\vec{x}$, $\sum_a P^a \vec{x} = 1$; so the range of the vector function $P$ is actually that of $(|\mathcal{A}| - 1)$-dimensional simplices (a compact convex subspace of $\mathcal{R}^{[\mathcal{A}]}$). As such, $P \in \mathcal{B}(\mathcal{X})^{[\mathcal{A}]}$ where $\mathcal{B}(\mathcal{X})$ is the set of bounded functions on $\mathcal{X}$.

Definition 1 (G-box). A black box (formalized above) whose input domain $\mathcal{X}$ is a homogeneous space acted transitively upon by the group $\mathcal{G}$ is known as a $\mathcal{G}$-box.

Proof of Theorem 1. Consider a $\mathcal{G}$-box whose ensemble behaviour can be characterized by a finite number of parameters (Assumption [14]). There is a representation of the symmetry group $\mathcal{G}$ in terms of real orthogonal matrices $R \mapsto T_R$, such that for each outcome $a$, the outcome probabilities $P(a | x_R)$ are a fixed (over $R$) linear combination of matrix entries of $T_R$.

Proof. Suppose Alice has a black box $P$, and access to a geometric freedom $\mathcal{G}$ acting on $\mathcal{X}$. For each $R \in \mathcal{G}$, Alice can induce a new black box $P^R$ by first applying $R$ to her input $\vec{x}$ and then supplying the input $R \vec{x}$ to $P$, which acts as $P^a : \vec{x} \mapsto P(a | R \vec{x})$, i.e. $P^R(a | \vec{x}) = P(a | R \vec{x})$.

For each $R$, we can define a map $T_R : P \mapsto P^R$, acting on each component of $P$ via $T_R P^a = P^R$. Obviously, $T_R R S = T_R S R$, so if we denote the “space of black boxes” accessible to Alice by $\Omega_\mathcal{G} := \{ T_R P | R \in \mathcal{G} \} \subseteq \mathcal{B}(\mathcal{X})^{[\mathcal{A}]}$, then $T_R$ defines a group action on $\Omega_\mathcal{G}$.

Consider the linear extension $\Omega_\mathcal{G}^\mathcal{R} := \text{span}(\Omega_\mathcal{G})$, a linear subspace of $\mathcal{B}(\mathcal{X})^{[\mathcal{A}]}$, with elements $Q = \sum_i \lambda_i P_i$, where $\lambda_i \in \mathbb{N}$ is arbitrary but finite, all $\lambda_i \in \mathbb{R}$, and $P_i \in \Omega_\mathcal{G}$. Note $Q : \mathcal{X} \rightarrow \mathcal{R}^{[\mathcal{A}]}$, but without further restriction on $\{\lambda_i\}$ this may map to outside of the simplex of normalized probabilities.

Now, consider the effect of $R \in \mathcal{G}$ on some object $Q$. Since $Q : \vec{x} \mapsto \sum_i \lambda_i P_i(a | \vec{x})$, applying $R$ first to take $R \vec{x} \mapsto \vec{x}$ gives us $Q \circ R : \vec{x} \mapsto \sum_i \lambda_i P_i(a | \vec{x})$, and hence $Q \circ R = \sum_i \lambda_i T_R P_i$. Since $T_R P = P \circ R$ for $P \in \Omega_\mathcal{G}$, we can define the map $T_R : \Omega_\mathcal{G}^\mathcal{R} \rightarrow \Omega_\mathcal{G}^\mathcal{R}$ via $T_R Q := Q \circ R$ as an extension of the map $T_R$. By construction, every $T_R$ is a linear map, and

$$T_R T_S(Q) = Q \circ R \circ S = Q \circ (R \circ S) = T_{RS}(Q),$$

hence $R \mapsto T_R$ is a real linear representation of $\mathcal{G}$. Since $T_R$ is an extension of $R$, we drop the tilde from our notation. As we have assumed that ensembles of black boxes can be characterized by a finite number of parameters, the linear space $\Omega_\mathcal{G}^\mathcal{R}$ is finite-dimensional. Then $T_R$, as linear maps acting on a finite-dimensional real vector space, may be expressed as real matrices.

Next, we need to show that the representation $R \mapsto T_R$ is bounded, i.e. that $\sup_{R \in \mathcal{G}} \|T_R\| < \infty$. This will exclude, for example, cases like $\mathcal{G} = (\mathbb{R}, +)$ and $T_i := \left( \frac{1}{i} \right)$. To this end, let $P_1, \ldots, P_D \in \Omega_\mathcal{G}$ be a linearly independent set of boxes that spans $\Omega_\mathcal{G}$ (that is, a basis of boxes, hence $D = \dim \Omega_\mathcal{G}$). Then, every $P \in \Omega_\mathcal{G}^\mathcal{R}$ has a unique representation $P = \sum_{i=1}^D \alpha_i P_i$, and $\|P\| := \sum_{i=1}^D \|\alpha_i\|$ defines a norm on $\Omega_\mathcal{G}^\mathcal{R}$. We can define another norm on this space via

$$\|P\| := \sup_{\vec{x} \in \mathcal{X}} \sum_{a \in \mathcal{A}} |P(a | \vec{x})|.$$  

This is finite since $P \in \mathcal{B}(\mathcal{X})^{[\mathcal{A}]}$, and it is easy to check that it satisfies the properties of a norm. Since all norms on a finite-dimensional vector space are equivalent, there is some $c > 0$ such that $\|P\| \leq c \|P\|$. Furthermore, all $P' \in \Omega_\mathcal{G}$ satisfy $\|P'\| = 1$. Thus, noting that $T_R P_i \in \Omega_\mathcal{G}$ for all $i = 1, \ldots, D$, we get

$$\|T_R P\| = \sum_{i=1}^D \alpha_i T_R P_i \leq \sum_{i=1}^D \|\alpha_i\| \cdot \|T_R P_i\| = \|P\| \leq c \cdot \|P\|.$$  

This establishes that the operator norm of all $T_R$ with respect to $\|\cdot\|$ (and hence with respect to all other norms) is uniformly bounded. Since we have assumed that $\mathcal{G}$ is locally compact, this implies that there is a basis of $\Omega_\mathcal{G}^\mathcal{R}$ in which the $T_R$ are orthogonal matrices.

Consider now the evaluation functional $\delta_{\vec{x}}^a : \Omega_\mathcal{G}^\mathcal{R} \rightarrow \mathbb{R}$; namely, the map from the space of black boxes to the particular probability of outcome $a$ given input $\vec{x}$. It follows that the statistics $P(a | \vec{x}) = P(a | R \vec{x}_0) = T_R P(a | \vec{x}_0) = \delta_{\vec{x}}^a(T_R P)$. Since the evaluation functional is a linear map, we then find that the probabilities are given by a linear combination of elements from $T_R$. For all $\vec{x} \in \mathcal{X}$, we use the same $P$ and the same $\delta_{\vec{x}}^a$ such...
that the only element that changes is the representation matrix $T_R$. 

Arguing via harmonic analysis on homogeneous spaces [21], we expect that Theorem [1] can be extended: it is not only entries of $T_R$ that appear in the probability table $P(a|x_R)$, but, more specifically, generalized spherical harmonics. A taste of this appears in Lemma \[\text{Lemma VII}\] but since the formulation of Theorem \[\text{[1]}\] is sufficient for the purpose of this article, we defer this extension to future work.

**Appendix B: SO(2) \times SO(2) Bell experiment setting**

1. **General form of correlations**

**Lemma I.** Consider a bipartite $SO(2) \times SO(2)$-box – i.e. Alice and Bob can each choose their inputs as angles $\alpha, \beta \in [0, 2\pi]$ – with local binary outcomes $a \in \{+1, -1\}$ and $b \in \{+1, -1\}$. Then, the most general joint probability distribution consistent with Theorem \[\text{[1]}\] is

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

where $J$ is some non-negative integer or half-integer. (Note that this does not yet assume the no-signalling principle.)

**Proof.** While the representation $T_R = T_{\alpha, \beta}$ from Theorem \[\text{[1]}\] acts on a real vector space $V$ of finite dimension $D$, we can also regard it as a representation on the complexification $W = V \oplus jV$. Since $SO(2) \times SO(2)$ is an Abelian group, all its irreducible representations are one-dimensional [12]. Thus, we can decompose $W$ as $W = \bigoplus_{j=1}^{D} W_j$, where each $W_j$ is a one-dimensional invariant subspace on which $T_{\alpha, \beta}$ acts as a complex phase. It follows that $T_{\alpha, \beta} = \bigoplus_{j=1}^{D} \exp(i(m_1 \alpha - n_1 \beta))$ with suitable integers $m_j, n_j \in \mathbb{Z}$ (to see this, write $T_{\alpha, \beta}$ as a composition of the $SO(2)$-representations $T_{\alpha, \theta}$ and $T_{\theta, \beta}$). Then, due to Theorem \[\text{[1]}\], $P(a, b | \alpha, \beta)$ must be a linear combination of real and imaginary parts of $T_{\alpha, \beta}$, which proves that it is of the form \[\text{[B1]}\].

2. **Generic no-signalling correlations**

It is well-known (e.g. [20]) that the no-signalling principle does not impose any constraints on the form of the correlation function if we have a bipartite box with two outcomes $a, b \in \{+1, -1\}$ each. Namely, if $\mathcal{X}, \mathcal{Y}$ denote two arbitrary sets of inputs, given an arbitrary function $C : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}$ with $-1 \leq C(x, y) \leq 1$ for all $x, y \in \mathcal{X}, \mathcal{Y}$, the simple prescription

$$P(a, b | x, y) := \frac{1}{4} + \frac{1}{4} ab C(x, y)$$

generates a valid no-signalling distribution that has $C(x, y)$ as its correlation function. It is a simple exercise to check that $C$ is non-negative, normalized and no-signalling, and that $C$ is the correlation function for $P$.

3. **Local hidden variable models for $SO(2) \times SO(2)$ settings**

Generalizing ideas of Werner [21], we can show that for noisy enough correlation functions of $SO(2) \times SO(2)$ settings, we can always construct a LHV model that achieves these correlations.

**Lemma II.** Consider any two-angle function

$$f(\alpha, \beta) = \sum_{j=1}^{N} [c_j \cos(m_j \alpha - n_j \beta) + s_j \sin(m_j \alpha - n_j \beta)],$$

for $(m_j, n_j) \in \mathbb{Z} \times \mathbb{Z} \setminus (0,0)$ (i.e. disallowing constant terms). Without loss of generality \[\text{[B3]}\], we disallow $(m_j, n_j) = (m, n)$ when $i \neq j$, choose $m_j \geq 0$, and if $m_1 = 0$ then we choose $n_j > 0$. Suppose $-1 \leq f(\alpha, \beta) \leq 1$ for all $\alpha, \beta$. Then $C(\alpha, \beta) := \gamma f(\alpha, \beta)$ is a correlation function that has a LHV model whenever $0 \leq \gamma \leq \gamma_N$, where

$$\gamma_N := \frac{2}{N} \max_{0 \leq x \leq \pi} \left( \frac{x}{\pi} \right)^{N-1} \sin \frac{x}{\pi}. \quad \text{[B4]}$$

**Proof.** In this proof, we will express all angles as numbers in the interval $[-\pi, \pi]$. Under the inner product $(f, f) := \frac{1}{2\pi} \int_{-\pi}^{\pi} dx \int_{-\pi}^{\pi} \cos^2 \frac{m \alpha - n \beta}{2} \gamma f \,g(\alpha, \beta)$, the set of functions

$$\cos(m_1 \alpha - n_1 \beta), \quad \sin(m_1 \alpha - n_1 \beta) \quad \text{[B5]}$$

(with $m_j$ and $n_j$ defined as above) is an orthonormal system (this follows from Schur orthornormality for $SO(2) \times SO(2)$, and can be verified by direct integration). Hence the $L^2$-norm $\|f\|^2 := (f, f)$ satisfies

$$\|f\|^2 = \int_{-\pi}^{\pi} \int_{-\pi}^{\pi} \cos^2 \frac{m \alpha - n \beta}{2} \gamma f \,g(\alpha, \beta) \frac{m^2 + n^2}{2 \pi^2} = \sum_{j=1}^{N} (c_j^2 + s_j^2) \leq 2,$$

since $|f(\alpha, \beta)| \leq 1$ everywhere.

Our goal is to construct a LHV model of the form

$$P(a, b | \alpha, \beta) = \int_{\Lambda} d\mu(\lambda) \, P_A(a | \alpha, \lambda) \, P_B(b | \beta, \lambda). \quad \text{[B7]}$$

We will have a hidden variable $\lambda = (\tilde{\lambda}_1, \tilde{\lambda}_2, \ldots, \tilde{\lambda}_N)$, where each $\tilde{\lambda}_j = (\cos \phi_j, \sin \phi_j)^T$ is independently and uniformly distributed on the unit circle, hence $d\mu(\lambda) = (2\pi)^{-N} d\phi_1 \ldots d\phi_N$. This measure is invariant under $SO(2)$ rotations of the individual $\tilde{\lambda}_j$. 

\[1\] These restrictions ensure that the coefficients $c_j$ and $s_j$ are associated with unique trigonometric functions.
We will construct local probabilities that implement the dependence on $\alpha, \beta, \lambda$ in the following form:

$$P_A(\pm | \alpha, \lambda) = q_A \left( + \left| R_{m_1 \alpha} \tilde{X}_1, \ldots, R_{m_N \alpha} \tilde{X}_N \right| \right), \quad P_B(\pm | \beta, \lambda) = q_B \left( + \left| R_{n_1 \beta} \tilde{X}_1, \ldots, R_{n_N \beta} \tilde{X}_N \right| \right),$$

where $q_A$ and $q_B$ are response functions defined in the following way: $q_A(-|\tilde{X}_1, \ldots, \tilde{X}_N) = 1 - q_A(+|\tilde{X}_1, \ldots, \tilde{X}_N)$, $q_B(\pm|\tilde{X}_1, \ldots, \tilde{X}_N)$ = \( \begin{cases} 1 & \text{if } \phi_j' \in [-\xi, \xi] \text{ for all } j \\ 0 & \text{otherwise} \end{cases} \)

where $\xi \in (0, \pi)$ is some (small) constant and $\phi_j'$ is the angle such that $\tilde{X}_j = (\cos \phi_j', \sin \phi_j')^T$. Furthermore,

$$q_B(\pm|\tilde{X}_1, \ldots, \tilde{X}_N) = \frac{1}{2} \left( 1 + \frac{1}{\sqrt{2N}} \sum_{j=1}^{N} \tilde{b}_j \cdot \tilde{X}_j \right),$$

where $\tilde{b}_j := (c_j, -s_j)^T$. Note that $\sum_j \tilde{b}_j \cdot \tilde{X}_j = \tilde{b} \cdot \tilde{X}$, where $\tilde{b} := \oplus \tilde{b}_j$ and $\tilde{X} := \oplus \tilde{X}_j$. But since $|\tilde{b}|^2 = \sum_j |\tilde{b}_j|^2 = \sum_j (c_j^2 + s_j^2) \leq 2$ and $|\tilde{X}|^2 = \sum_j |\tilde{X}_j|^2 = N$, the sum hence is upper-bounded by $\sqrt{2N}$ due to the Cauchy-Schwarz inequality. This shows that $q_B$ yields valid probabilities.

We calculate the joint probability distribution obtained in the Bell test scenario:

$$P(+, \pm | \alpha, \beta) = \int_A \mu(\lambda) P_A(+ | \alpha, \lambda) P_B(\pm | \beta, \lambda)$$

$$= \int_A \mu(\lambda) q_A(+) P_{R_{m_1 \alpha} \tilde{X}_1, \ldots, P_{R_{m_N \alpha} \tilde{X}_N}) \cdot q_B(\pm| R_{n_1 \beta} \tilde{X}_1, \ldots, R_{n_N \beta} \tilde{X}_N).$$

We apply the substitution $\tilde{X}_j := R_{m_1 \alpha} \tilde{X}_j$ and $\tilde{X} := (\tilde{X}_1, \ldots, \tilde{X}_N)$, noting that this does not change the integral due to our choice of measure:

$$P(+, \pm | \alpha, \beta) = \int_A \mu(\lambda) q_A(+) \cdot q_B(\pm| R_{n_1 \beta} \tilde{X}_1, \ldots, R_{n_N \beta} \tilde{X}_N).$$

Due to the definition of $q_A$ and $q_B$, this equals

$$\int_{-\xi}^{\xi} d\phi_1' \int_{-\xi}^{\xi} d\phi_2' \frac{1}{2\pi} \frac{1}{2\pi} \left( 1 + \frac{1}{\sqrt{2N}} \sum_j f_j(\phi_j') \right),$$

where

$$f_j(\phi_j') = c_j \cos(\phi_j' + n_j \beta - m_j \alpha) - s_j \sin(\phi_j' + n_j \beta - m_j \alpha).$$

Noting that

$$\int_{-\xi}^{\xi} f_j(\phi_j') d\phi_j' = 2 \sin \xi [c_j \cos(m_j \alpha - n_j \beta)]$$

$$+ s_j \sin(m_j \alpha - n_j \beta),$$

we can evaluate the integral explicitly, obtaining

$$P(+, \pm | \alpha, \beta) = \frac{1}{2} \left( \frac{\xi}{\pi} \right)^N \pm \frac{1}{2\sqrt{2N}} \left( \frac{\xi}{\pi} \right)^{N-1} \frac{\sin \xi}{\pi} f(\alpha, \beta).$$

Next, let us look at the other probabilities:

$$P(-, \pm | \alpha, \beta) = \int_A \mu(\lambda) P_A(- | \alpha, \lambda) P_B(\pm | \beta, \lambda)$$

$$= \int_A \mu(\lambda)(1 - P_A(\pm | \alpha, \lambda)) P_B(\pm | \beta, \lambda)$$

$$= -P(-, \pm | \alpha, \beta) + \int_A \mu(\lambda) q_B(\pm| R_{n_1 \beta} \tilde{X}_1, \ldots, R_{n_N \beta} \tilde{X}_N),$$

and the final integral vanishes on all $\tilde{b}_j \cdot \tilde{X}_j$ terms of $q_B$, leaving only the constant term $1/2$. That is,

$$P(-, \pm | \alpha, \beta) = \frac{1}{2} - P(+, \pm | \alpha, \beta).$$

These give the correlation function

$$C(\alpha, \beta) = \sqrt{\frac{2}{N}} \left( \frac{\xi}{\pi} \right)^{N-1} \frac{\sin \xi}{\pi} f(\alpha, \beta).$$

Finally, we define $\gamma_N$ as the largest admissible prefactor among all possible choices of $\xi$.

Let us now introduce a constant term:

**Lemma III.** Consider any two-angle correlation function

$$C(\alpha, \beta) = c_0 + \sum_{j=1}^{N} [c_j \cos(m_j \alpha - n_j \beta) + s_j \sin(m_j \alpha - n_j \beta)],$$

where $(m_j, n_j) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0, 0)\}$, and (as above) without loss of generality we choose $m_j \geq 0$ and $n_j > 0$ if $m_j = 0$, and disallow $(m_n, n_n) = (m_j, n_j)$ if $i \neq j$. If

$$\max_{\alpha, \beta} |C(\alpha, \beta) - c_0| \leq \gamma_N(1 - |c_0|)$$

with constant $\gamma_N$ given by

$$\gamma_N = \begin{cases} \sqrt{2}/\pi & \text{if } N = 1, \\ 0.184375 \ldots & \text{if } N = 2, \\ 0.103893 \ldots & \text{if } N = 3, \\ \sqrt{2e^{-1} N^{-3/2}} & \text{if } N \geq 4, \end{cases}$$

then this correlation function has a local hidden variable model.

**Proof.** First, we obtain the form of $\gamma_N$ by solving the optimization problem of Lemma III exactly for $N = 1, 2, 3$, and by substituting $x = \pi(1 - 1/N)$ and using

$$\left( 1 - \frac{1}{N} \right)^{N-1} \pi \left( \frac{1 - \frac{1}{N}}{N} \right) \geq \frac{\pi}{Ne}$$

we can add the constant function $1/\sqrt{2}$ to the orthonormal system in (eq. [B3]); similar reasoning as in
the proof of Lemma [11] shows that $(\sqrt{2}c_0)^2 \leq 2$, i.e. that $-1 \leq c_0 \leq 1$, and $c_0 = 1$ is only possible if $C(\alpha, \beta) = c_0$ (i.e. with no angle-dependent terms). Now consider the case $0 \leq c_0 < 1$. We can write
\[
C(\alpha, \beta) = c_0 I + (1 - c_0) f(\alpha, \beta),
\]
where $I$ is the constant function that takes the value 1 on all angles, and $f(\alpha, \beta) = (C(\alpha, \beta) - c_0)/(1 - c_0)$ is of the form of the function in Lemma [11]. If inequality (B22) holds, then
\[
\max_{\alpha, \beta} |f(\alpha, \beta)| = \frac{1}{1 - c_0} \max_{\alpha, \beta} |C(\alpha, \beta) - c_0| \leq \gamma_N , \quad (B26)
\]
and so Lemma [11] proves that $f(\alpha, \beta)$ is a classical correlation function. Moreover, $I$ is trivially a classical correlation function, and thus so must be $C(\alpha, \beta)$, which is a convex combination of the two. Then case $-1 < c_0 < 0$ can be treated analogously, using that $-1$ is a classical correlation function too. \hfill $\square$

**Proof of Theorem 2A.** Consider an SO(2) × SO(2) box, with a correlation function in the form of eq. (4) with maximum (half-)integer $J \neq 0$. If
\[
\max_{\alpha, \beta} |C(\alpha, \beta) - C_{00}| \leq \gamma_J (1 - |C_{00}|), \quad (B27)
\]
where $C_{00}$ is the angle-independent contribution to the correlation function (as in eq. (4)), and $\gamma_J$ is a given
\[
\gamma_J = \sqrt{2} e^{-1} [4J (2J + 1)]^{-\frac{1}{2}}, \quad (B28)
\]
then there is a LHV model that accounts for these correlations. \hfill $\square$

**Proof.** This follows as a corollary of Lemma [11], We convert between the form of correlations in eq. (4) and eq. [B21] by counting the maximum number $N$ of unique terms that could appear for a given positive (half-)integer $J$. The double sum contributes $(2J + 1)(4J + 1)$ terms, from which we remove $2J$ cases corresponding to negative $n$ where $m = 0$, and the one completely constant case $m = n = 0$. This gives a maximum of $N = 4J (2J + 1)$. Since the lowest value ($J = \frac{1}{2}$) already yields $N = 4$ unique terms, we only need the final case of eq. (B23), and hence the constant $\gamma_J = \sqrt{2} e^{-1} [4J (2J + 1)]^{-\frac{1}{2}}$. \hfill $\square$

4. Witnessing nonlocality

Bell inequalities can be chained by direct addition. For instance, suppose one takes a CHSH inequality (eq. 5) with measurements $\{x_1, y_2, x_3, y_4\}$ and a second with measurements $\{x_1, y_6, x_5, y_6\}$. Adding these together yields $|C(x_1, y_2) + C(x_3, y_2) + C(x_3, y_4) + C(x_5, y_6) - C(x_1, y_6)| \leq 4$. This can inductively be done for a set of $N$ measurements ($\frac{N}{2}$ each for Alice and Bob), leading to a chained Bell inequality, known as the Brunstein–Caves inequality (BCI) [28]:
\[
\begin{align*}
C(x_1, y_2) &+ C(x_3, y_2) + C(x_3, y_4) + \cdots \\
&+ C(x_{N-1}, y_N) - C(x_1, y_N) \leq N - 2. \quad (B29)
\end{align*}
\]
If such an equation is violated, then no LHV can account for these statistics.

Recall, eq. (4) gives the generic SO(2) × SO(2) correlation function. If we restrict ourselves to relational correlations, this amounts to setting $S_{mm} = C_{mm} = 0$ when $m \neq n$, such that the correlation function has a single parameter form
\[
C(\beta - \alpha) = \sum_{m=0}^{2J} C_m \cos [m (\beta - \alpha)] + S_m \sin [m (\beta - \alpha)] \quad (B30)
\]
where $J$ is some positive (half-)integer, and $C_m := C_{mm}, S_m := S_{mm}$.

**Lemma IV.** Consider relational SO(2) × SO(2) correlations (of the form of eq. (B30)) for finite positive (half-)integer $J$. If there is some $\Theta_+ \in [0, 2\pi)$ such that $C(\Theta_+) = +1$, and $\Theta_+ \in [0, 2\pi)$ where $C(\Theta_-) = -1$, then there exists a BCI that demonstrates a Bell violation.

**Proof.** We show this by construction. For even $N$, define
\[
\delta_N := \frac{(\Theta_+ - \Theta_-) \mod 2\pi}{N - 1}. \quad (B31)
\]
We use the notation “$x \mod 2\pi$” to indicate $x - 2\pi n$ where $n \in \mathbb{Z}$ is chosen such that $x - 2\pi n \in [0, 2\pi)$, mapping the angle to the principal range.

![FIG. 3. Measurement angles for generic correlation function. The first choice of measurement angles are chosen such that $b_2 - a_1 = \Theta_+ + \delta$. Subsequent choices then proceed by $2\delta$, such that ultimately $b_N - a_1 = \Theta_-$.](image)

We construct a $N$-measurement BCI, as defined in eq. (B29). Since the correlation function is relational,
we write $C(\alpha, \beta)$ as the single parameter function $C(\beta - \alpha)$, and assign the measurement settings:

\[
\begin{align*}
    a_i &= (i - 1)\delta_N & \text{for odd } i, \\
    b_i &= \Theta_+ + (i - 1)\delta_N & \text{for even } i. \quad (B32)
\end{align*}
\]

(Illustrated in figure [3].) This amounts to setting the arguments of the correlation functions featured in the BCI to

\[
\begin{align*}
    b_2 - a_1 &= \ldots = b_{2m} - a_{2m-1} = \Theta_+ + \delta_N, \\
    b_2 - a_3 &= \ldots = b_{2m} - a_{2m+1} = \Theta_+ - \delta_N, \\
    b_N - a_1 &= \Theta_-, \quad \text{(B33)}
\end{align*}
\]

where equality is taken modulo $2\pi$.

With such assignments, the BCI is then written:

\[
\frac{N}{2} C(\Theta_+ + \delta_N) + \left( \frac{N}{2} - 1 \right) C(\Theta_+ - \delta_N) - C(\Theta_-) \leq N - 2. \quad (B34)
\]

Recall that $C(\Theta_+) = -1$. $C(\Theta_+) = +1$ must be a local maximum, and a finite $J$ allows us to assume the function $C$ is smooth at this point. Thus, in the limit of small $\delta_N$, $C(\Theta_+ \pm \delta_N) \approx 1 - k\delta_N^2 + O(\delta_N^3)$ where $k \geq 0$ is some constant. We then rewrite eq. (B34) as

\[
\begin{align*}
    (N - 1) \left( 1 - k\delta_N^2 + O(\delta_N^3) \right) + 1 &\leq N - 2, \\
    N + O((N - 1)^{-1}) &\leq N - 2, \quad (B35)
\end{align*}
\]

which for large enough $N$ will eventually be violated. \Box

The above construction can be shown to have some robustness to noise (tolerating a smaller maximum value than 1). To show this, we first prove an auxiliary lemma:

**Lemma V.** Consider relational $SO(2) \times SO(2)$ correlations (of the form of eq. (B30)) for finite positive (half-)integer $J$. Let there be some angle difference $\Theta_+$, where $C(\Theta_+) \geq 1 - \varepsilon$, and some other angle difference $\Theta_-$ where $C(\Theta_-) \leq 1 - \Delta$, with $\varepsilon \geq 0$ and $\Delta > 0$. If

\[
\varepsilon < -K_J + \sqrt{\frac{K_J^2 + \Delta^2}{4}} = \frac{\Delta^2}{8K_J} + O(\delta^{-2}), \quad (B41)
\]

where $K_J = \sqrt{2\pi^2 J(2J + 1)(4J + 1)/3}$, then there will be a BCI that is violated.

**Proof.** First, since the correlation function $C$ is continuous, it attains its global maximum at some $\Theta'$. Since $C(\Theta') \geq C(\Theta_+) \geq 1 - \varepsilon$, the premises of this lemma are also satisfied if $\Theta_+$ is replaced by $\Theta'$, i.e., we can assume without loss of generality that $C$ attains its global maximum at $\Theta_+$.

With these $\Theta_+$ and $\Theta_-$, we use the prescription in Lemma [IV] with the angle choices in eq. (B32) to generate the following BCI, which must hold for all even integers $N \geq 2$ if there exists a LHV model:

\[
\frac{N}{2} C(\Theta_+ + \delta_N) + \left( \frac{N}{2} - 1 \right) C(\Theta_+ - \delta_N) - C(\Theta_-) \leq N - 2. \quad (B42)
\]

Let us write $\delta \Theta := \Theta_+ - \Theta_- \mod 2\pi$, such that $\delta \Theta = \frac{\pi}{N - 1}$. Let $K \in \mathbb{R}$ be any constant such that $C''(x) \geq -K$ for all $x$; it follows from Lemma [V] that such $K$ exists, and we will fix $K$ later in accordance with that lemma. Since $\Theta_+$ is a local maximum, we know that $0 \geq C''(\Theta_+) \geq -K$, i.e. $K \geq 0$. The global bound on the second derivative of $C$ gives us

\[
C(\Theta_+ \pm x) \geq C(\Theta_+) - K \frac{x^2}{2} \text{ for all } x. \quad (B43)
\]

Thus, eq. (B42) implies

\[
(N - 1) \left( 1 - \varepsilon - K \frac{\delta \Theta^2}{2} \right) - (1 - \Delta) \leq N - 2. \quad (B44)
\]

Under what conditions does there exist an even integer $N \geq 2$ such that this inequality is violated, i.e. the existence of a LHV model is ruled out? The negation of this inequality can be rearranged into a quadratic equation in $(N - 1)$:

\[
\varepsilon(N - 1)^2 - \Delta(N - 1) + K \frac{\delta \Theta^2}{2} < 0. \quad (B45)
\]
If this equation has a solution for some even integer \( N \), then the non-existence of a LHV model follows. If \( \varepsilon = 0 \), then there will always be a solution for large enough \( N \), recovering Lemma \text{[V]}. Thus, we here only give further consideration to the case where \( \varepsilon > 0 \).

Since this quadratic function in \( (N-1) \) is positive for large values of \( \pm(N-1) \), it is necessary for the existence of a negative value that this function has zeroes over the real numbers. The zeroes are

\[
N_{\pm} = \frac{\Delta \pm \sqrt{\Delta^2 - 2\varepsilon K(\Theta)^2}}{2\varepsilon},
\]

and so the following inequality is necessary for the existence of a solution of eq. \text{[B45]}:

\[
\Delta^2 > 2\varepsilon K(\Theta)^2. \tag{B47}
\]

If it is satisfied, then the values of \( (N-1)_{\pm} \) are well-defined, and we can continue to argue as follows. The quadratic function in eq. \text{[B45]} is negative for all real numbers \( N \), where \( 0 < N_{-} < N_{+} \). Now, this interval definitely contains an even integer \( N \) if \( N_{+} - N_{-} > 2 \). Since \( N_{+} - N_{-} = \sqrt{\Delta^2 - 2\varepsilon K(\Theta)^2}/\varepsilon \), this difference is larger than two if and only if

\[
4\varepsilon^2 + 2\varepsilon K(\Theta)^2 - \Delta^2 < 0. \tag{B48}
\]

The two solutions of the corresponding quadratic equation are

\[
\varepsilon_{\pm} = \frac{-K(\Theta)^2 \pm \sqrt{K^2(\Theta)^4 + 4\Delta^2}}{4}. \tag{B49}
\]

They are both real, and \( \varepsilon_{-} < 0 < \varepsilon_{+} \). Thus, \( \varepsilon < \varepsilon_{+} \) implies a suitable solution of eq. \text{[B45]}, i.e. rules out the existence of a LHV model.

In fact, if \( \varepsilon < \varepsilon_{+} \), then we automatically get

\[
4\varepsilon < -K(\Theta)^2 + K(\Theta)^2 \sqrt{1 + \frac{4\Delta^2}{K^2(\Theta)^4}} \leq \frac{2\Delta^2}{K(\Theta)^2},
\]

i.e. eq. \text{[B47]} is automatically satisfied. Now, considering \( \varepsilon_{+} \) as a function in \( \Theta \), this function is decreasing for \( \delta \Theta > 0 \). Since \( \delta \Theta \leq 2\pi \), \( \varepsilon < \varepsilon_{+}(\delta \Theta) \equiv \varepsilon_{+} \). Thus, the inequality

\[
\varepsilon < \frac{-K(2\pi)^2 + \sqrt{K^2(2\pi)^4 + 4\Delta^2}}{4} \tag{B51}
\]

implies a violation of a BCI. The statement of the lemma now follows from taking the value of \( K \) from Lemma \text{[V]} and by substituting \( K_{J} : = \pi^2 K \).

This has consequence for generic (possibly non-relational) \( \text{SO}(2) \times \text{SO}(2) \) settings.

**Proof of Theorem 2B.** Consider \( \text{SO}(2) \times \text{SO}(2) \) correlations \( C \) for finite maximum (half-)integer \( J \). Let \( C_{\text{rel}} \) the relational core of \( C \) (that is, the function of the form eq. \text{[B30]} formed by only including terms of eq. \text{[4]} where \( m = n \)). Let there be some angle difference \( \Theta_{+} \), where \( C_{\text{rel}}(\Theta_{+}) \geq 1 - \varepsilon \), and some other angle difference \( \Theta_{-} \) where \( C_{\text{rel}}(\Theta_{-}) \leq 1 - \Delta \), with \( \varepsilon \geq 0 \) and \( \Delta > 0 \).

If \( \varepsilon < -K_{J} + \sqrt{K_{J}^2 + \frac{\Delta^2}{4}} = \frac{\Delta^2}{8K_{J}} + O(K_{J}^{-2}) \), \tag{B52}

where \( K_{J} = \sqrt{2\pi^2J(2J+1)(4J+1)/3} \), then there will be a BCI for the (possibly non-relational) correlation function \( C \) that is violated.

**Proof.** Subtracting the “non-relational” parts of \( C(\alpha, \beta) \) is equivalent to performing the following integration:

\[
C_{\text{rel}}(\alpha, \beta) = \frac{1}{2\pi} \int_{0}^{2\pi} d\phi \ C(\alpha + \phi, \beta + \phi). \tag{B53}
\]

This may be directly verified by noting that terms of the form \( \cos(m\alpha - n\beta + (m-n)\phi) \) and \( \sin(m\alpha - n\beta + (m-n)\phi) \) individually integrate to 0 over \( \phi \) except when \( m = n \). This allows us to interpret taking the relational core of a correlation function as mixing \( C \) over many settings offset by a shared uniform random angle.

It then follows from the convexity of Bell inequalities that if the BCI implied by Lemma \text{[VI]} for the relational core is violated “on average” for this mixture of settings, there must be at least one single set of input settings that also results in that BCI being violated.

\[ \square \]

5. **Necessity of a bound on \( J \)**

We will now show that our protocol for witnessing nonlocality does not work if we simply drop the assumption that \( J \) is finite.

A correlation function \( C(\alpha, \beta) \) has a LHV model if and only if there exists a variable \( \lambda \in \Lambda \), distributed via some \( P_{\Lambda}(\lambda) \), and a family of local response functions \( C_{\Lambda}(\alpha, \lambda) := \sum_{\lambda \in \Lambda_{\alpha}} a_{\Lambda}(\alpha, \lambda) \) and \( B_{\Lambda}(\beta, \lambda) := \sum_{\lambda \in \Lambda_{\beta}} b_{\Lambda}(\beta, \lambda) \) such that

\[
C(\alpha, \beta) = \int_{\Lambda} d\lambda P_{\Lambda}(\lambda) C_{\Lambda}(\alpha, \lambda) B_{\Lambda}(\beta, \lambda). \tag{B54}
\]

Suppose that there are two angles \( \theta_{+}', \theta_{-}' \) such that our protocol gives correlation values \( C_{\text{rel}}(\theta_{\pm}') \) very close to \( \pm 1 \). If this is the only experimental syndrome, without further assumptions on the form of the correlation function (in particular, without any assumption on \( J \) as explained in the main text), then this experimental behavior can always be reproduced to arbitrary accuracy by local hidden variables. Namely, \( \theta_{\pm}' \) can be arbitrarily well approximated by angles \( \theta_{\pm} \) that satisfy the premises of the following lemma:

**Lemma VII.** Suppose that \( \theta_{+}, \theta_{-} \in [0, 2\pi) \) are such that \( \theta_{+} - \theta_{-} = \frac{n\pi}{m} \), where \( n \in \mathbb{N} \) and \( m \leq n \) is an odd integer. Then there exists a local relational correlation function \( C(\alpha, \beta) \equiv C(\alpha - \beta) \) such that

\[
C(\theta_{+}) = +1 \text{ and } C(\theta_{-}) = -1. \tag{B55}
\]
Proof. We set \( \Lambda = [0, 2\pi) \) and \( P_\Lambda(\lambda) = \frac{1}{2\pi} \) - the uniform measure on this interval. Without loss of generality, assume that \( \Theta_- > \Theta_+ \) and \( \Theta_+ = 0 \) (we can choose our local coordinates \( \alpha, \beta \) to make this the case). Define 
\[
C_\Lambda(x, \lambda) = C_B(x, \lambda) := f(x + \lambda), \text{ where } f : \mathbb{R} \to \{-1, +1\} \text{ is the } 2\pi \text{-periodic extension of } f \text{ defined as: }
\]
\[
f(x) := \left\{
+1 \text{ if } x \in \left[0, \frac{1}{n}\right) \cup \left[\frac{2}{n}, \frac{3}{n}\right) \cup \ldots \cup \left[\frac{2n-2}{n}, \frac{2n-1}{n}\right) \text{ and } -1 \text{ for all other } x \in [0, 2\pi).
\right.
\]
(B56)

That is, \( f \) is a square-wave function of period \( \frac{2\pi}{n} \). This \( f \) is piecewise continuous and satisfies \( f(x + \frac{2\pi}{n}) = -f(x) \) for all \( x \). Thus, \( f(x + \frac{2\pi}{n}) = -f(x + \frac{\pi}{n}) = f(x + \frac{\pi}{n}) = -f(x) \) for all \( x \), and in particular, by induction, \( f(x + \frac{m\pi}{n}) = -f(x) \) for all \( x \) since \( m \) is odd by assumption. Now, defining \( C(\alpha, \beta) \) as in \( (B54) \), this correlation function is relational, since
\[
C(\alpha + x, \beta + x) = \frac{1}{2\pi} \int_0^{2\pi} f(\alpha + x + \lambda)f(\beta + x + \lambda) \, d\lambda
= \frac{1}{2\pi} \int_0^{2\pi} f(\alpha + \lambda)f(\beta + \lambda) \, d\lambda
= C(\alpha, \beta)
\]
(B57)

by substitution and due to the \((2\pi)\)-periodicity of \( f \). Furthermore,
\[
C(0, 0) = \frac{1}{2\pi} \int_0^{2\pi} f(\lambda)^2 \, d\lambda = 1,
\]
\[
C(0, \pi) = C\left(\frac{m}{n}, 0\right) = \frac{1}{2\pi} \int_0^{2\pi} f\left(\frac{m}{n} \pi + \lambda\right) f(\lambda) \, d\lambda
= -\frac{1}{2\pi} \int_0^{2\pi} (f(\lambda))^2 \, d\lambda = -1.
\]
(B58)

Therefore, simply following our protocol but relaxing our assumption on \( J \) (while not imposing any other assumptions) cannot be sufficient to certify nonlocality.

Appendix C: Characterizing quantum correlations

Let us consider black boxes that have a particularly simple transformation behaviour under rotations:

**Definition 2** (Transforming fundamentally). Consider an \( \text{SO}(d) \)-box \( P(a | x) \), where \( d \geq 2 \). Let \( x_0 \in X \). We say that this box transforms fundamentally under rotations if for all \( x \in X \) and all \( R_x \in G \) with \( R_xx_0 = x \) one finds
\[
P(a | x) \equiv P(a | R_xx_0) = c_{\theta}^a + \sum_{i,j=1}^d (R_x)_{i,j} c_{\theta}^j, \quad (C1)
\]
where \((R_x)_{i,j}\) is the fundamental matrix representation of \( R_x \in G \), and \( c_{\theta}^a, c_{\theta}^j \) are constants independent of \( x \) and \( R_x \).

Equivalently, a black box transforms fundamentally if the corresponding representation \( R \mapsto T_R \) from Theorem 1 can be chosen as a direct sum of copies of the trivial and the fundamental representations of \( G = \text{SO}(d) \). Since \( G \) is transitive on \( X \), the existence of the above representation is independent of the particular \( x_0 \): any alternative \( x'_0 \in X \) satisfies \( x'_0 = Sx_0 \) for some \( S \in G \), satisfying the above with \( R' = RS^{-1} \).

**Lemma VIII.** Suppose that \( X = S^{d-1} \) (the unit sphere), and \( P(a | \vec{x}) \) transforms fundamentally under rotations in \( G = \text{SO}(d) \). Then, \( P(a | \vec{x}) = c_{\theta}^a + \tilde{c}_{\theta}^a \cdot \vec{x} \), \( (C2) \) where constants \( c_{\theta}^a \in \mathbb{R} \) and \( \tilde{c}_{\theta}^a \in \mathbb{R}^d \) satisfy
\[
\sum_{a \in A} c_{\theta}^a = 0, \quad \sum_{a \in A} \tilde{c}_{\theta}^a = \vec{0} \quad (C3)
\]
such that for all \( a, |c_{\theta}^a| \geq 0 \) and \( |\tilde{c}_{\theta}^a| \leq \min(c_{\theta}^0, 1 - c_{\theta}^0) \).

Conversely, if a black box has this form, then it transforms fundamentally under rotations.

In other words, an \( \text{SO}(d) \)-box transforms fundamentally if and only if \( P(a | \vec{x}) \) is affine-linear in \( \vec{x} \) (and non-negativity and normalization of probabilities holds).

Proof. Set \( \vec{x}_0 := \vec{e}_1 = (1, 0, \ldots, 0)^T \). Fix some choice of rotations \( \vec{x} \mapsto R_x \) with \( R_{\vec{x}_0} = \vec{x} \). Consider the stabilizer subgroup \( G_{\vec{e}_1} := \{ R \in \text{SO}(d) \mid R\vec{e}_1 = \vec{e}_1 \} \):
\[
G_{\vec{e}_1} = \left\{ \begin{pmatrix} 1 & 0^T \\ 0 & T \end{pmatrix} \mid T \in \text{SO}(d-1) \right\}. \quad (C4)
\]
The fact that this group is isomorphic to \( \text{SO}(d-1) \) is precisely due to the fact that our set of inputs is the homogeneous space \( X = \text{SO}(d)/\text{SO}(d-1) \), i.e. the \((d-1)\)-sphere. For \( d \geq 3 \), we have \( \int_{\text{SO}(d-1)} T \, dT = 0 \), and thus
\[
\int_{G_{\vec{e}_1}} S \, dS = Q := \begin{pmatrix} 1 & 0^T \\ 0 & 0 \end{pmatrix}. \quad (C5)
\]
Since \( R_x S_{\vec{e}_1} = \vec{x} \) for every \( S \in G_{\vec{e}_1} \), every rotation matrix \( R_x \) can be substituted for \( R_x \) into definition 2. Thus \( P(a | \vec{x}) = c_{\theta}^a + \sum_{i,j=1}^d (R_x)_{i,j} c_{\theta}^j \). By taking the average over all \( S \in G_{\vec{e}_1} \), according to the Haar measure, we get
\[
P(a | \vec{x}) = c_{\theta}^a + \sum_{i,j=1}^d \left( R_x \int_{G_{\vec{e}_1}} S \, dS \right) c_{\theta}^j. \quad (C6)
\]
But \( R_x Q = (\vec{x}, \vec{0}, \ldots, \vec{0}) \), i.e. a matrix with first column equal to \( \vec{x} \) and all further columns equal to zero. This proves that \( P(a | \vec{x}) \) is affine-linear in \( \vec{x} \) as claimed, in the case \( d \geq 3 \).

Now consider the case \( d = 2 \). Here, \( \vec{x} = (x_1, x_2)^T \), and there is a unique choice of \( R_x \), namely \( R_x = \begin{pmatrix} 1 & -x_2 \\ x_2 & x_1 \end{pmatrix} \). Then, \( P(a | \vec{x}) \) being affine-linear in \( \vec{x} \) is equivalent to being affine-linear in \( \vec{x} \).

From normalization, \( \sum_{a} P(a | \vec{x}) = 1 \) \( \forall \vec{x} \in X \), which by transitivity of \( G \) on \( X \) can be re-written
The next two lemmas show that these properties are preserved by convex combinations of boxes.

**Lemma IX.** Let \( \{ P_i(a, b | x, y) \}_{i=1,...,N} \) be a set of non-signalling bipartite black boxes that transform fundamentally locally. Any convex combination 
\( P(a, b | x, y) := \sum_i \lambda_i P_i(a, b | x, y) \)
where all \( \lambda_i \geq 0 \) and \( \sum_i \lambda_i = 1 \) also transforms fundamentally locally.

**Proof.** First, we calculate the marginal distribution:
\[ P_A(a | x) := \sum_b P(a, b | x, y) = \sum_b \lambda_i \sum_b \lambda_i P_i(a, b | x, y) = \sum_i \lambda_i \sum_b \lambda_i P_i(a, b | x, y) = \sum_i \lambda_i P_{A,i}(a | x), \]
Similarly,
\[ P_{B,i}(b | y) = \sum_a \lambda_i P_{A,i}(a | x) \]
First, we note that 
\( P_{B,i}(b | y) = 0 \) only if 
\( P_{B,i}(b | y) = 0 \) for all \( i \).
In this case, the combined conditional box is undefined, and there is nothing to prove. Thus, we may proceed with the case that 
\( P_{B,i}(b | y) > 0 \).
With 
\[ P(a, b | x, y) = \sum_i \lambda_i P_i(a, b | x, y) \]
we obtain
\[ P_{A,i}^{b,y}(a | x) = \sum_i \lambda_i P_{B,i}(b | y) P_{A,i}(a | x) \] (10)
Here, \( \sum_i' \) denotes a sum over all those \( i \) for which
\( P_{B,i}(b | y) > 0 \). These are exactly the \( i \) for which
\( P_{A,i}(a | x) \) is well-defined. Meanwhile,
\( \sum_i' \lambda_i P_{A,i}^{b,y}(a | x) = 1 \),
and hence we may define 
\( \mu_i := \lambda_i P_{A,i}^{b,y}(a | x) \) for those \( i \) with 
\( P_{B,i}(b | y) > 0 \), and
\( \mu_i = 0 \) for all other \( i \), such that
\( \mu_i \geq 0 \) and moreover
\( \sum_i \mu_i = \sum_i' \mu_i = 1 \). Thus, the new conditional box is itself a convex combination of the constituent conditional boxes. A similar convex combination can be found for 
\( P_{A,i}^{a,y}(b | y) \).
Since the constituent conditional boxes transform fundamentally, from Lemma VIII we write
\[ P_{A,i}^{b,y}(a | x) = c_{i}(b,y) \cdot \lambda_i \cdot P_{A,i}^{b,y}(a | x) \]
where
\[ c_{i}(b,y) := \sum_a \lambda_i c_{i}(a,b,y) \cdot a \]
\[ c_{i}(b,y) := \sum_a \lambda_i c_{i}(a,b,y) \cdot a \]
by the converse part of Lemma VIII.
\( P_{A,i}^{b,y}(a | x) \) is thus a valid black box that transforms fundamentally. The same argument holds for Bob’s conditional boxes.

**Lemma X.** Let \( \{ P_i(a, b | x, y) \}_{i=1,...,N} \) be a set of non-signalling bipartite black boxes that are locally unbiased with respect to \( \mathcal{G} \). Any convex combination 
\( P(a, b | x, y) := \sum_i \lambda_i P_i(a, b | x, y) \)
where all \( \lambda_i \geq 0 \) and \( \sum_i \lambda_i = 1 \) is also locally unbiased with respect to \( \mathcal{G} \).

**Proof.** In the proof of Lemma IX we have seen that there exists a probability distribution \( \{ \mu_i \}_{i=1} \) such that
\( P_{A,i}^{b,y}(a | x) = \sum_i \mu_i P_{A,i}^{b,y}(a | x) \).
Thus we find
\[ \int P_{A,i}^{b,y}(a | R) dR = \sum_i \mu_i \int P_{A,i}^{b,y}(a | R) dR = \] (11)
Likewise holds for Bob’s conditional boxes, and hence, 
\( P(a, b | x, y) \) is also locally unbiased.
Lemma XI. Consider a bipartite black box with inputs $X = Y = S^{d-1}$ and binary outcomes $A = B = \{+1, -1\}$. If this box transforms fundamentally locally and is locally unbiased, then it describes quantum correlations.

Proof. From Lemma VIII, binary-outcome conditional boxes that transform fundamentally and are unbiased can be written:

\[
P_A^{\vec{y}}(a|\vec{x}) := \left( \frac{1}{a \vec{c}(0, \vec{y})} \right) \cdot \left( \frac{1}{a \vec{e}} \right),
\]

\[
P_B^{\vec{y}}(b|\vec{x}) := \left( \frac{1}{b \vec{c}(a, \vec{x})} \right) \cdot \left( \frac{1}{b \vec{e}} \right),
\]

(C12)

such that the joint probability distribution is given by:

\[
P(a, b | \vec{x}, \vec{y}) = P_B(b|\vec{y}) \left( \frac{1}{\vec{c}(\vec{y}, \vec{z})} \right) \cdot \left( \frac{1}{a \vec{e}} \right),
\]

(C14)

\[
P(a, b | \vec{x}, \vec{y}) = P_A(a|\vec{x}) \left( \frac{1}{\vec{c}(a, \vec{x})} \right) \cdot \left( \frac{1}{b \vec{e}} \right).
\]

(C15)

This defines a map $\omega_{AB}$ acting on $\vec{e}_{a,\vec{x}} := (1, a \vec{e})^T$ and $\vec{e}_{b,\vec{y}} := (1, b \vec{e})^T$, such that $\omega_{AB}(\vec{e}_{a,\vec{x}}, \vec{e}_{b,\vec{y}}) = P(a, b | \vec{x}, \vec{y})$. Moreover, $\text{span}(\vec{e}_{a,\vec{x}}) = \text{span}(\vec{e}_{b,\vec{y}}) = \mathbb{R}^{d+1}$, and so this function has a unique bilinear extension $\omega_{AB} : \mathbb{R}^{d+1} \times \mathbb{R}^{d+1} \rightarrow \mathbb{R}$.

The set of non-negative linear combinations of $\vec{e}_{a,\vec{x}}$ define a positive Euclidean cone $A^+ \subset \mathbb{R}^{d+1}$, whose extremal rays are the non-negative multiples of $(1, \vec{e})^T$ for $\vec{x} \in S^{d-1}$. We may then define an Archimedean order unit (AOU) $\vec{u} := (2, 0, \ldots, 0)^T \in \mathbb{R}^{d+1}$ and define an AOU-space $(\mathbb{R}^{d+1}, A^+, \vec{u})$. An identical AOU-space $(\mathbb{R}^{d+1}, B^+, \vec{u})$ can be defined using the non-negative linear combinations of $\vec{e}_{b,\vec{y}}$.

Now, we shall employ a result from Kleinnmann et al. [52] (generalizing a result by Barnum et al. [53]) that pertains to bilinear maps on positive Euclidean cones. If a bilinear map $\omega_{AB}$ on such cones is both unital and positive, then there exists a bipartite quantum system $\rho_{AB}$ and a map from each point $\vec{u} \in A^+$, $\vec{v} \in B^+$ onto local quantum POVM elements $M_{ab}$, $M_{b}$ such that

\[
\omega_{AB}(\vec{u}, \vec{v}) = \text{tr}(\rho_{AB} M_{ab} \otimes M_{b}).
\]

We show that $\omega_{AB}$ satisfies these conditions. First, for any given $a$, $\vec{x}$ (likewise $b$, $\vec{y}$), it can be seen that

\[
\vec{e}_{+a,\vec{x}} + \vec{e}_{-a,\vec{x}} = \vec{u} = \vec{e}_{b,\vec{y}} + \vec{e}_{-b,\vec{y}},
\]

(C16)

and hence $\omega_{AB}(\vec{u}, \vec{u}) = \sum_{a,b} P(a, b | \vec{x}, \vec{y}) = 1$, which means that $\omega_{AB}$ is unital. Next, since every $\vec{y} \in A^+$ can be written as a non-negative linear combination of finitely many $\vec{e}_{a,\vec{x}}$ (likewise for $\vec{q} \in B^+$), then $\omega_{AB}(\vec{p}, \vec{q}) = 0$ for all $\vec{p}, \vec{q} \in A^+$, $B^+$, showing that $\omega_{AB}$ is positive. Hence, $\omega_{AB}$ can be realised by a quantum system, and $P(a, b | \vec{x}, \vec{y})$ is a quantum behaviour.}

The premise of local unbiasedness cannot be removed: if we only demand that a box transforms fundamentally locally, then it can generate correlations that are disallowed by quantum theory. To see this, let $P_B$ be any non-signalling $(2, 2, 2)$-behaviour (for example, a PR-box), and define

\[
P(a, b | \vec{x}, \vec{y}) := \lambda_A \lambda_B P_B(a, b|0, 0) + \lambda_A \lambda_B P_B(a, b|0, 1) + \lambda_A \lambda_B P_0(a, b|1, 0) + \lambda_A \lambda_B P_0(a, b|1, 1),
\]

(C17)

where $a, b \in \{-1, +1\}$, $\vec{x}, \vec{y} \in S^{d-1}$, $\lambda_A := \frac{1}{2}(1 + x_1)$, $\lambda_B := \frac{1}{2}(1 + y_1)$, and $\lambda_B := 1 - \lambda_B$. If $d = 3$, for example, this describes a situation in which two possible local inputs $x, y \in \{0, 1\}$ are encoded into the first Bloch vector component of a qubit, the qubits are locally measured, and the measurement results $x, y \in \{0, 1\}$ are input into the original box $P_B$. This defines a valid non-signalling box, and the linear dependence of the outcome probabilities on $\vec{x}$ (resp. $\vec{y}$) demonstrate, via Lemma VIII, that $P$ transforms fundamentally locally. However, it reproduces $P_B$ via $P_B(a, b|t) = P(a, b | \vec{x}, \vec{y})$, where $\vec{x}_0 = \vec{y}_0 = (1, 0, \ldots, 0)$ and $\vec{x}_1 = \vec{y}_1 = (-1, 0, \ldots, 0)$.

Now we show a converse statement, so that we get an exact classification of the quantum $(2, 2, 2)$-behaviours: i.e. the family of probabilities obtained in quantum theory during a two party Bell test, where each agent has two choices of input and obtains one of two outcomes.

Lemma XII. Let $d \geq 2$. Then all extremal quantum $(2,2,2)$-behaviours can be realised by locally unbiased SO($d$)-boxes that transform fundamentally locally with $X_A = X_B = S^{d-1}$; the two settings (inputs) correspond to two choices of directions.

Proof. It has been shown [25] [44] [51] [53] that the extremal quantum $(2, 2, 2)$-behaviours can be realised by rank-1 projective measurements on two-qubit pure states. Any extremal quantum $(2, 2, 2)$-behaviour $P(a, b | r, t)$ can then be written in the form $P(a, b | r, t) = \text{Tr}[\rho_{AB}(E_{r,t}^\rho \otimes F_{r,t}^\rho)]$ where $\rho$ is a pure state of two qubits and $E_{r,t}^\rho$ and $F_{r,t}^\rho$ are qubit rank-1 projectors, $a, b \in \{-1, +1\}$ and $r, t \in \{1, 2\}$. We shall show that there exists a non-signalling SO($d$) × SO($d$)-box $P(a, b | \vec{x}, \vec{y})$ that transforms fundamentally locally, is locally unbiased, and has choices $\vec{x}_r, \vec{y}_t$ such that $P(a, b | \vec{x}_r, \vec{y}_t) = P(a, b | r, t)$.

Write $E := E_{11}^+$ and $\hat{E} := E_{12}^+$. As $\hat{T}$ is $E_{11}^+$, its expansion in the Pauli operator basis is of the form $E = \frac{1}{2} (I_2 + \sigma_x \sigma_x + \sigma_y \sigma_y + \sigma_z \sigma_z)$, and the associated Bloch vector $\vec{x}_1 := (E_{12,1}, E_{12,2}, E_{12,3})$ has Euclidean norm 1. Let $\vec{z}_2$ be the Bloch vector similarly associated with $\hat{E}$. By changing the local bases unitarily, we can ensure that $\vec{x}_1 = (1, 0, 0)^T$ and $\vec{x}_2 = (\cos \theta, \sin \theta, 0)^T$, where $0 \leq \theta < 2\pi$. Similarly, we can define the Bloch vectors $\vec{y}_t$ for $t = 1, 2$ via the rank-1 projections $F_{r,t}^\rho$.

Define a linear map $\Pi : \mathbb{R}^4 \rightarrow \mathbb{R}^3$ in the following way. If $d = 2$, set $\Pi(v_1, v_2) := (v_1, v_2, 0)^T$; if $d \geq 3$, set $\Pi(v_1, \ldots, v_d) := (v_1, v_2, v_3)^T$, which is an orthogonal projection (and the identity if $d = 3$). Furthermore, for $\vec{v} \in \mathbb{R}^3$, define $E_{\vec{v}} := \frac{1}{2}(1 + \vec{v} \cdot \vec{s})$, which is
positive-semidefinite whenever $|\vec{v}| \leq 1$. Consider the non-signalling $\text{SO}(d) \times \text{SO}(d)$-box
\begin{equation}
P(a, b | \vec{x}, \vec{y}) := \text{Tr} \left[ \rho_{AB} E_{a|\vec{x}} \otimes E_{b|\vec{y}} \right].
\end{equation}
Since $|a I \vec{x}| \leq |\vec{x}| = 1$ for $\vec{x} \in S^{d-1}$ (and similarly for $b I \vec{y}$), this defines a valid (quantum) behaviour. The conditional boxes are
\begin{equation}
P^{\vec{k} \vec{j}}_A (a | \vec{x}) = \frac{1}{2} \frac{\text{Tr} \left[ \rho_{AB} (\mathbb{1} + a \vec{x} \cdot (\vec{j}^T \vec{x})) \otimes E_{b|\vec{y}} \right]}{\text{Tr}(\rho_B E_{b|\vec{y}})}.
\end{equation}
This expression yields well-defined probabilities by construction, and it is affine-linear in $\vec{x}$. Analogous statements hold for the other conditional boxes. Thus, according to Lemma VII, $P(a, b | \vec{x}, \vec{y})$ transforms fundamentally locally. Furthermore, averaging the above conditional box uniformly over $\vec{x}$ replaces $\vec{x}$ by zero and annihilates all dependence on $a$; hence this box is locally unbiased.

Let $\vec{x}_r \in \mathbb{R}^d$ be the vector whose first two components are the first two components of $\vec{x}'_r$, and all other $(d-2)$ components are zero; define $\vec{y}_t$ analogously. Then $P(a, b | r, t) = P(a, b | \vec{x}_r, \vec{y}_t)$.

**Proof of Theorem 3** Let $d \geq 2$. The quantum $(2, 2, 2)$-behaviours are exactly those that can be realised by binary-outcome bipartite $\text{SO}(d) \times \text{SO}(d)$-boxes that transform fundamentally locally and are locally unbiased, restricted to two choices of input direction per party per box, and statistically mixed via shared randomness.

Proof. Lemma XI tells us that “$(2, S^{d-1}, 2)$-behaviours” that transform fundamentally locally, and are locally unbiased, can be realised by local measurements on a bipartite quantum system. If we restrict our choice of inputs from the full $S^{d-1}$ freedom to just two choices of orientation per party, then these will be $(2, 2, 2)$-behaviours, and since they can be realised by a quantum system, they are quantum $(2, 2, 2)$-behaviours.

The other direction follows from Lemma XII all extremal quantum $(2, 2, 2)$-behaviours can be realised by restricting binary-outcome bipartite $\text{SO}(d) \times \text{SO}(d)$-boxes, transforming fundamentally locally and being locally unbiased, to two possible input directions per party. Additional shared randomness allows the two parties to generate all statistical mixtures of these behaviours, yielding all further quantum $(2, 2, 2)$-behaviours.

Theorem 3 cannot hold for all $d \geq 2$ without allowing shared randomness. For example, suppose that $d = 3$, then the proof of Lemma XI shows that all correlations realizable with binary-outcome bipartite $\text{SO}(3) \times \text{SO}(3)$-boxes that transform fundamentally locally and are locally unbiased can be realized via unital positive bilinear forms on the positive semidefinite qubit cone. Consequently, the result by Barnum et al. [53] implies that all these correlations can also be realized via POVMs on arbitrary two-qubit quantum state space. However, Donohue and Wolfe [36] (extending results by Pál and Vértesi [35]) have shown that the set of $(2, 2, 2)$-behaviours realizable on two qubits via POVMs is not convex, and thus not equal to the convex set of quantum $(2, 2, 2)$-behaviours.