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

Andrew J. P. Garner¹, ,¹ Marius Krumm,^{1,2} and Markus P. Müller^{1,3} ¹*Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria*²*Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria*³*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, Canada N2L 2Y5*

(Received 26 July 2019; accepted 14 December 2019; published 3 February 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 space-time 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 an alternative class of semi-device-independent protocols for quantum technologies.

DOI: [10.1103/PhysRevResearch.2.013112](https://doi.org/10.1103/PhysRevResearch.2.013112)

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 transpired to have a very powerful practical use: It enables device-independent protocols in quantum information theory (see, 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-signaling 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 space-time 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 [Fig. 1(a)]. 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 [Fig. 1(b)]. 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 symmetry groups (Sec. II A). We demonstrate the power of this approach with two examples in Bell test scenarios. First, if each laboratory controls a single angle (Sec. II B), we find, independently of the theory, that the response to rotations can in some cases certify the existence of a local hidden-variable model, or the violation of a Bell inequality. Consequently, we present a protocol for witnessing nonlocality, similar in spirit to [11,12] but without prerequiring the validity of quantum theory. Second, we consider when both inputs are chosen via rotations in d -dimensional space. We show that natural assumptions on the local response to those rotations recover the set of bipartite binary quantum correlations exactly (Sec. II C), indicating a fundamental relation between the structures of space-time and of quantum mechanics. Finally, we discuss the implications of these results (Sec. III), particularly for the construction of experimental tests of quantum mechanics and of semi-device-independent protocols for quantum technologies.

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

FIG. 1. Bell scenario: abstract vs spatiotemporal inputs. Spatially separate Alice and Bob independently choose measurement settings x and y and receive some outputs a and 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 $x = \alpha$ and $y = \beta$ of polarizers).

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 1 of this paper applies to any casual structure, but looking towards application the later examples will use the Bell scenario.

Here we consider experiments where the local inputs correspond to spatiotemporal degrees of freedom: for example, the direction of inhomogeneity of the magnetic field in a Stern-Gerlach experiment or the angle of a polarization filter [Fig. 1(b)]. Crucially, we 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 $R \in \text{SO}(3)$ 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 $\mathcal{X}$ and a symmetry group $\mathcal{G}$ that acts on $\mathcal{X}$. Given some arbitrary $x_0 \in \mathcal{X}$, we assume that Alice can generate every possible input $x \in \mathcal{X}$ by applying a suitable transformation $R \in \mathcal{G}$ such that $x = Rx_0$. Mathematically, $\mathcal{X}$ is then a homogeneous space [14], which can be written $\mathcal{X} = \mathcal{G}/\mathcal{H}$, where $\mathcal{H} \subseteq \mathcal{G}$ is the subgroup of transformations R' with $R'x_0 = x_0$. In the example above, $\mathcal{G} = \text{SO}(3)$ describes the full set of rotations that Alice can apply to $\vec{x}_0$, while $\mathcal{H} = \text{SO}(2)$ describes the subset of rotations that leave $\vec{x}_0$ invariant (i.e., the axial symmetry of the magnetic field vector). Then $\mathcal{X} = \text{SO}(3)/\text{SO}(2) = S^2$ is the 2-sphere of unit vectors (i.e., directions) in three-dimensional space. Similarly, the polarizer [Fig. 1(b)] corresponds to $\mathcal{G} = \text{SO}(2)$, $\mathcal{H} = \{\mathbb{1}\}$, and $\mathcal{X} = S^1$, 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 $\mathcal{G} = (\mathbb{R}, +)$ 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 $\mathcal{H} = (\tau\mathbb{Z}, +)$, then the input domain $\mathcal{X} = \mathcal{G}/\mathcal{H} \simeq S^1$. 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 $x \in \mathcal{X}$, the outcome a is observed with probability $P(a|x)$. Then, Alice can “rotate” her apparatus by $R \in \mathcal{G}$ and induce a new black box P' with outcome probabilities $P'(a|x) = P(a|R x)$. Physically, R could be either an active rotation, within Alice's laboratory (e.g., spinning a polarizer), of the incident system (e.g., adding a phase plate) or a passive change of coordinates.

Thus, a given black box and a spatiotemporal degree of freedom defines a family of black boxes, and transformations $R \in \mathcal{G}$ 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 and then by R' is equivalent to a single rotation $R'' = R' \circ R$, it follows that 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 $\{\lambda_i\}_{i=1}^n$, $\sum_i \lambda_i = 1$, $\lambda_i \geq 0$, the experiment of first drawing i with probability λ_i and then applying black box P_i defines an effective black box P , with the statistics $P(a|x) = \sum_i \lambda_i P_i(a|x)$. 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 1. 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, the Bennett-Brassard [17] quantum cryptography protocol assumes that the information carriers are two dimensional, excluding additional degrees of freedom that could serve as a side channel for eavesdroppers [18]. Assumption 1 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 $x_R \in \mathcal{X}$ by selecting some $R \in \mathcal{G}$ and applying it to a default input x_0 , i.e., $x = Rx_0$. Then we state the following.

Theorem 1. 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 .

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 $\mathcal{G}$ as $\mathcal{G}$ 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 $\mathcal{X}_A, \mathcal{G}_A$ and $\mathcal{X}_B, \mathcal{G}_B$, respectively, then the full setup can be seen as an experiment with $\mathcal{X} = \mathcal{X}_A \times \mathcal{X}_B$ and $\mathcal{G} = \mathcal{G}_A \times \mathcal{G}_B$, to which Theorem 1 applies directly.

Second, there may be more than one transformation that generates the desired input x , i.e., both $x = Rx_0$ and $x = R'x_0$ for $R \neq R'$; this is precisely the case if $R^{-1}R' \in \mathcal{H}$. For example, a magnetic field can be rotated from the y direction to the 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 ω , initially in state ρ_0 , left to evolve for a variable time t before it is measured by a fixed positive-operator-valued measure (POVM) [19] $\{M_a\}_{a \in \mathcal{A}}$. The free dynamics are given by the Hamiltonian H , whose discrete set of eigenvalues $\{E_n = \hbar\omega(\frac{1}{2} + n)\}$ corresponds to allowed energy levels. The evolution is periodic, so (recalling earlier) $\mathcal{G} = (\mathbb{R}, +)$, $\mathcal{H} = (\frac{2\pi}{\omega}\mathbb{Z}, +)$, and $\mathcal{X} \simeq S^1$. The associated black box is thus $P(a|t) = \text{Tr}[M_a \exp(-\frac{iHt}{\hbar})\rho_0 \exp(\frac{iHt}{\hbar})]$. For any given ρ_0 and M_a , this evaluates to an affine-linear combination of terms of the form $\cos[(n-m)\hbar\omega t]$ and $\sin[(n-m)\hbar\omega t]$, involving all pairs of energy levels that have nonzero occupation probability in ρ_0 (and nonzero support in M_a). This is a linear combination of entries of the matrix representation

$$T_t = \bigoplus_{\alpha=E_n-E_m} \begin{pmatrix} \cos(\alpha t) & \sin(\alpha t) \\ -\sin(\alpha t) & \cos(\alpha t) \end{pmatrix}, \quad (1)$$

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 α 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.

B. Example: Two angles and Bell witnesses

Let us consider the simplest nontrivial spatiotemporal freedom, where Alice and Bob each have the choice of a single continuous angle $\alpha, \beta \in [0, 2\pi)$, respectively, and each obtains 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 [Fig. 1(b)].

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

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

resulting in a correlation function

$$C(\alpha, \beta) := P(+1, +1|\alpha, \beta) + P(-1, -1|\alpha, \beta) - P(+1, -1|\alpha, \beta) - P(-1, +1|\alpha, \beta) \quad (3)$$

$$= \sum_{m=0}^{2J} \sum_{n=-2J}^{2J} C_{mn} \cos(m\alpha - n\beta) + S_{mn} \sin(m\alpha - n\beta), \quad (4)$$

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

If Alice's and Bob's laboratories are spatially separated, the laws of relativity forbid Alice from sending signals to Bob instantaneously. This no-signaling principle constrains the set of valid 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 (4), there is always at least one set of valid no-signaling probabilities (see Appendix B 2), for example, those where the marginal distributions are maximally mixed such that independent of α , a is $+1$ or -1 with equal probability (likewise for β and b), consistent with an observation of Popescu and Rohrlich [20].

Consider a quantum example: two photons in a Werner state [21,22] $\rho_W := p|\psi^-\rangle\langle\psi^-| + \frac{1}{4}(1-p)\mathbb{1}_4$, where $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$ and $p \in [0, 1]$. Alice's and Bob's polarizer/detector setups are described by the observables $M_\theta := \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$ for orientations $\theta = \alpha, \beta$ respectively. Then $C(\alpha, \beta) = \text{Tr}(\rho_W M_\alpha \otimes M_\beta) = -p \cos[2(\alpha - \beta)]$. This fits the form of Eq. (4) 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 λ over some space Λ 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's and Bob's local response functions (conditioned on their input choices α and β and the particular realization of the hidden variable λ)? 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]

$$|C(\alpha_1, \beta_2) + C(\alpha_3, \beta_2) + C(\alpha_3, \beta_4) - C(\alpha_1, \beta_4)| \leq 2, \quad (5)$$

where α_1 and α_3 are two choices of Alice's angle and β_2 and β_4 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. (4) are allowed by quantum theory. For example, science fiction polarizers with the correlation function $C(\alpha, \beta) = \frac{2}{\pi} \cos[3(\alpha - \beta)] - \cos[\alpha - \beta]$ would yield a CHSH value of 3.63, under choices of angles $\alpha_1 = 1.5$, $\alpha_3 = 0$, $\beta_2 = 3.9$, and $\beta_4 = 2.3$, violating quantum theory's maximum achievable value of $2\sqrt{2}$ [25].

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 3). If the only constraint on the correlations is that it has some maximum J , then the existence of a LHV is guaranteed if the magnitude of angle-dependent changes in C is less than γ_J where

$$\gamma_J := \sqrt{2}e^{-1}[4J(2J+1)]^{-3/2}. \quad (6)$$

Subject to extra restrictions that keep the form of C simple, more permissive bounds are also derived. For instance, if there is only one nonzero coefficient in Eq. (4), then $\gamma = \sqrt{2}/\pi \approx 0.4502$. Recall the correlation function for projective measurements on a Werner state $-p \cos[2(\alpha - \beta)]$ and identify γ with p . In this case, our bound is comparable to that in [26] of $p \leq 0.6829$.

Conversely, we can give a simple sufficient criterion for nonlocality if we separate the terms in Eqs. (2) and (4) into relational and nonrelational components. The relational components where $m = n$ account for behavior that depends only on the difference between the two angles. Purely relational correlations, i.e., ones with $C(\alpha, \beta) \equiv C(\alpha - \beta)$, 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 [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_{rel} has an angle difference Θ_+ which results in near perfect (anti)correlations and another angle difference Θ_- that does not, then one can systematically construct a (Braunstein-Caves [28]) Bell inequality that will be violated (see Appendix B 4). Specifically, “near perfect” means that for a given J , $C_{\text{rel}}(\Theta_+) \geq 1 - \varepsilon_J$ with

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

FIG. 2. Two-angle relational correlation functions. A sufficiently noisy correlation function can always be reproduced exactly by a LHV model (Theorem 2a). This is represented by the green curve completely 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 2b). 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.

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 Θ_- (see Appendix B 4 for proof). We summarize these results (see also Fig. 2) as follows.

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 γ_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 Θ_+ [above $1 - \varepsilon_J$, as defined in Eq. (7)], but also sufficiently different (below $1 - \Delta$) for some other angle Θ_- , then the correlations violate a Bell inequality.

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.

(i) Alice and Bob share some random angle λ , uniformly distributed in the interval $[0, 2\pi)$.

(ii) Alice chooses locally freely between the two possible angles $\alpha \in \{\Theta_+, \Theta_-\}$.

(iii) Alice now inputs $\alpha + \lambda$ into her half of the box, while Bob inputs λ .

(iv) 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 λ effectively projects C onto its relational part $C_{\text{rel}}(\alpha, \beta) = \frac{1}{2\pi} \int_0^{2\pi} d\lambda C(\alpha + \lambda, \beta + \lambda)$, which only depends on $\alpha - \beta$. The protocol above set β equal 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 Θ_+ and Θ_- 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 1, 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_{rel} as above) without any additional assumption on J is not sufficient to obtain this reduction, as we show in Appendix B 5.

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 Bell witnesses. This opens up the possibility of alternative methods of experimentally certifying nonlocal behavior, 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 nonlocality. In our next example, we move from angles [SO(2)] to directions [SO(d)], but consider arguably the simplest nontrivial response.

C. Example: Characterizing quantum correlations

For our last example, we will 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) behaviors. The set of quantum (2,2,2) behaviors $\mathcal{Q}$ is a strict superset of the classical (2,2,2) behaviors $\mathcal{C}$ (i.e., those admitting a LHV model). However, the set of all no-signaling behaviors $\mathcal{NS}$ is strictly larger: $\mathcal{C} \subsetneq \mathcal{Q} \subsetneq \mathcal{NS}$ [20,30]. 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 nontrivial 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 $P(a|\vec{x})$ is said to transform fundamentally if the representation matrix T_R in Theorem 1 can be chosen as the block matrix $\mathbb{1}_1 \oplus R$, where $\mathbb{1}_1 := (1)$ 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 $P(a|\vec{x}) = c_0^a + \vec{c}^a \cdot$

$\vec{x}$, where $\vec{x} \in S^{d-1}$ is the input, $c_0^a \in \mathbb{R}^+$, and $\vec{c}^a \in \mathbb{R}^d$ (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 $c_0^a = 1/|A|$ 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 nonsignaling box $P(a, b|\vec{x}, \vec{y})$, where both inputs $\vec{x}, \vec{y} \in S^{d-1}$ are spatial directions and a and b each can take two values. Suppose that their conditional boxes transform fundamentally and are unbiased. A conditional box $P_A^{b,\vec{y}}(a|\vec{x}) := P(a, b|\vec{x}, \vec{y})/P_B(b|\vec{y})$ describes the local black box Alice would have if she was told Bob's measurement choice $\vec{y}$ 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, $P(a, b|\vec{x}, \vec{y})$ 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) behaviors.

Theorem 3. The quantum (2,2,2) behaviors are exactly those that can be realized by binary-outcome bipartite SO(d) $\times$ 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 order. 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 behavior is unbiased in the sense described above, the resulting (2,2,2) behavior can be biased. Second, this unbiasedness of the underlying SO(d) $\times$ SO(d) box is necessary to recover the quantum correlations; without it, one can realize arbitrary nonsignaling correlations, including Popescu-Rohrlich (PR) box [20] behavior, in a way that still transforms locally fundamentally (we give an example in Appendix C). Finally, shared randomness is necessary to realize explicitly nonextremal quantum correlations by such boxes, following the observation that the set of (2,2,2) behaviors realizable by POVMs on two qubits is not convex [35,36]. Namely, if both parties share the (2,2,2) behaviors P_0 and P_1 and a random bit $c \in \{0, 1\}$ that equals 0 with probability λ , they can statistically implement the mixed behavior $\lambda P_0 + (1 - \lambda) P_1$ 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) behaviors [37] without modification, this result shows that our framework of $\mathcal{G}$ boxes offers a very natural perspective on physical correlations and reinforces earlier observations that hint at a deep fundamental link between the structures of space-time 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 behavior can certify technologically important properties such as the presence or absence of Bell correlations.

Specifically, we have shown that the quantum (2,2,2) behaviors 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 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 [44–46], our assumption on the devices’ symmetry behavior 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.

Second, our framework informs 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 space-time 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 space-time 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 this kind of question 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 financial support 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 program CoQuS (Project No. W1210-N25). 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.

APPENDIX A: 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 $\mathcal{H} = SO(d-1) \subset \mathcal{G}$ 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 $\vec{x} = R_{\vec{x}}\vec{x}_0$ for some suitable transformation $R_{\vec{x}} \in \mathcal{G}$.

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 $R_{\vec{x}}$. In general, $R_{\vec{x}}$ is not unique and Alice's freedom of choice of transformation is given by $\mathcal{H}$.

A black box P is then a map $P : \mathcal{X} \rightarrow \mathbb{R}^{|\mathcal{A}|}$ such that for $\vec{x} \in \mathcal{X}$, $P^a : \vec{x} \mapsto P(A = a | X = \vec{x})$, where P^a is the a th element of the vector map. Since for probabilities $0 \leq P(A = a | X = \vec{x}) \leq 1$, 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 simplexes (a compact convex subspace of $\mathbb{R}^{|\mathcal{A}|}$). 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 ($\mathcal{G}$ 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 behavior can be characterized by a finite number of parameters (Assumption 1). 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' 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., $P'(a | \vec{x}) = P(a | R\vec{x})$.

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

Consider the linear extension $\Omega_{\mathcal{G}}^{\mathbb{R}} := \text{span}(\Omega_{\mathcal{G}})$, a linear subspace of $\mathcal{B}(\mathcal{X})^{|\mathcal{A}|}$, with elements $Q = \sum_{i=1}^n \lambda_i P_i$, where $n \in \mathbb{N}$ is arbitrary but finite, all $\lambda_i \in \mathbb{R}$, and $P_i \in \Omega_{\mathcal{G}}$. Note that $Q : \mathcal{X} \rightarrow \mathbb{R}^{|\mathcal{A}|}$, 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 $R : \vec{x} \mapsto R\vec{x}$ gives us $Q \circ R : \vec{x} \mapsto \sum_i \lambda_i P_i(a | R\vec{x})$, 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 $\tilde{T}_R : \Omega_{\mathcal{G}}^{\mathbb{R}} \rightarrow \Omega_{\mathcal{G}}^{\mathbb{R}}$ via $\tilde{T}_R Q := Q \circ R$ as an extension of the map T_R . By construction, every $\tilde{T}_R$ is a linear map and

$$\tilde{T}_R \tilde{T}_S(Q) = Q \circ R \circ S = Q \circ (R \circ S) = \tilde{T}_{RS}(Q); \quad (\text{A1})$$

hence $R \mapsto \tilde{T}_R$ is a real linear representation of $\mathcal{G}$. Since $\tilde{T}_R$ is an extension of T_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 $\Omega_{\mathcal{G}}^{\mathbb{R}}$ 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 $T_t := \begin{pmatrix} 1 & \\ 0 & t \end{pmatrix}$. To this end, let $P_1, \dots, P_D \in \Omega_{\mathcal{G}}$ be a linearly independent set of boxes that spans $\Omega_{\mathcal{G}}^{\mathbb{R}}$ (that is, a basis of boxes, hence $D = \dim \Omega_{\mathcal{G}}^{\mathbb{R}}$). Then every $P \in \Omega_{\mathcal{G}}^{\mathbb{R}}$ has a unique representation $P = \sum_{i=1}^D \alpha_i P_i$ and

$\|P\|_1 := \sum_{i=1}^D |\alpha_i|$ defines a norm on $\Omega_{\mathcal{G}}^{\mathbb{R}}$. We can define another norm on this space via

$$\|P\| := \sup_{\vec{x} \in \mathcal{X}} \sum_{a \in \mathcal{A}} |P(a | \vec{x})|. \quad (\text{A2})$$

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 $\|\bullet\|_1 \leq c \|\bullet\|$. Furthermore, all $P' \in \Omega_{\mathcal{G}}$ satisfy $\|P'\| = 1$. Thus, noting that $T_R P_i \in \Omega_{\mathcal{G}}$ for all $i = 1, \dots, D$, we get

$$\begin{aligned} \|T_R P\| &= \left\| \sum_{i=1}^D \alpha_i T_R P_i \right\| \leq \sum_{i=1}^D |\alpha_i| \|T_R P_i\| \\ &= \|P\|_1 \leq c \|P\|. \end{aligned} \quad (\text{A3})$$

This establishes that the operator norm of all T_R with respect to $\|\bullet\|$ (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 $\Omega_{\mathcal{G}}^{\mathbb{R}}$ in which the T_R are orthogonal matrices.

Consider now the evaluation functional $\delta_{\vec{x}}^a : \Omega_{\mathcal{G}}^{\mathbb{R}} \rightarrow \mathbb{R}$, 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 $P(a | \vec{x}) = P(a | R\vec{x}_0) = T_R P^a(\vec{x}_0) = \delta_{\vec{x}_0}^a(T_R P)$. 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 $\delta_{\vec{x}_0}^a$ such that the only element that changes is the representation matrix T_R . ■

Arguing via harmonic analysis on homogeneous spaces [51], 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 8, but since the formulation of Theorem 1 is sufficient for the purpose of this article, we defer this extension to future work.

APPENDIX B: THE $\text{SO}(2) \times \text{SO}(2)$ BELL EXPERIMENT SETTING

1. General form of correlations

Lemma 1. Consider a bipartite $\text{SO}(2) \times \text{SO}(2)$ 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 1 is

$$\begin{aligned} P(a, b | \alpha, \beta) &:= \sum_{m=0}^{2J} \sum_{n=-2J}^{2J} c_{mn}^{ab} \cos(m\alpha - n\beta) \\ &\quad + s_{mn}^{ab} \sin(m\alpha - n\beta), \end{aligned} \quad (\text{B1})$$

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

Proof. While the representation $T_R = T_{\alpha, \beta}$ from Theorem 1 acts on a real vector space V of finite dimension D , we can also regard it as a representation on the complexification $W = V \oplus iV$. Since $\text{SO}(2) \times \text{SO}(2)$ is an Abelian group, all its irreducible representations are one dimensional [42]. 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 $T_{\alpha,\beta} = \bigoplus_{j=1}^D \exp[i(m_j\alpha - n_j\beta)]$ with suitable integers $m_j, n_j \in \mathbb{Z}$ [to see this, write $T_{\alpha,\beta}$ as a composition of the $\text{SO}(2)$ representations $T_{\alpha,0}$ and $T_{0,\beta}$]. Then, due to Theorem 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 (B1). ■

2. Generic no-signaling correlations

It is well known (see, e.g., [20]) that the no-signaling 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 $\mathcal{X}$ and $\mathcal{Y}$ denote two arbitrary sets of inputs, given an arbitrary function $C : \mathcal{X} \times \mathcal{Y} \rightarrow \mathbb{R}$ with $-1 \leq C(x, y) \leq 1$ for all $x, y \in \mathcal{X}, \mathcal{Y}$, the simple prescription

$$P(a, b|x, y) := \frac{1}{4} + \frac{1}{4}abC(x, y) \quad (\text{B2})$$

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

3. Local hidden-variable models for $\text{SO}(2) \times \text{SO}(2)$ settings

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

Lemma 2. Consider any two-angle function

$$f(\alpha, \beta) = \sum_{j=1}^N [c_j \cos(m_j\alpha - n_j\beta) + s_j \sin(m_j\alpha - n_j\beta)] \quad (\text{B3})$$

for $(m_j, n_j) \in \mathbb{Z} \times \mathbb{Z} \setminus (0, 0)$ (i.e., disallowing constant terms). Without loss of generality¹ in $f(\alpha, \beta)$, we disallow $(m_i, n_i) = (m_j, n_j)$ when $i \neq j$, choose $m_j \geq 0$, and if $m_j = 0$ then we choose $n_j > 0$. Suppose $-1 \leq f(\alpha, \beta) \leq 1$ for all α, β . 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

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

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

$$\cos(m_j\alpha - n_j\beta), \quad \sin(m_j\alpha - n_j\beta) \quad (\text{B5})$$

(with m_j and n_j defined as above) is an orthonormal system [this follows from Schur orthonormality for $\text{SO}(2) \times \text{SO}(2)$ and can be verified by direct integration]. Hence the L^2 -norm

$\|f\|^2 := \langle f, f \rangle$ satisfies

$$\|f\|^2 = \int_{-\pi}^{\pi} d\alpha \int_{-\pi}^{\pi} d\beta \frac{f(\alpha, \beta)^2}{2\pi^2} = \sum_{j=1}^N (c_j^2 + s_j^2) \leq 2, \quad (\text{B6})$$

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 $\lambda = (\vec{\lambda}_1, \vec{\lambda}_2, \dots, \vec{\lambda}_N)$, where each $\vec{\lambda}_j = (\cos \phi_j, \sin \phi_j)^T$ is independently and uniformly distributed on the unit circle, hence $d\mu(\lambda) = (2\pi)^{-N} d\phi_1 \cdots d\phi_N$. This measure is invariant under $\text{SO}(2)$ rotations of the individual $\vec{\lambda}_j$.

We will construct local probabilities that implement the dependence on α, β , and λ in the form

$$P_A(\pm|\alpha, \lambda) = q_A(\pm|R_{m_1\alpha}\vec{\lambda}_1, \dots, R_{m_N\alpha}\vec{\lambda}_N), \quad (\text{B8})$$

$$P_B(\pm|\beta, \lambda) = q_B(\pm|R_{n_1\beta}\vec{\lambda}_1, \dots, R_{n_N\beta}\vec{\lambda}_N), \quad (\text{B9})$$

where q_A and q_B are response functions defined as $q_A(-|\vec{\lambda}'_1, \dots, \vec{\lambda}'_N) = 1 - q_A(+|\vec{\lambda}'_1, \dots, \vec{\lambda}'_N)$,

$$q_A(+|\vec{\lambda}'_1, \dots, \vec{\lambda}'_N) := \begin{cases} 1 & \text{if } \phi'_j \in [-\xi, \xi] \text{ for all } j \\ 0 & \text{otherwise,} \end{cases} \quad (\text{B10})$$

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

$$q_B(\pm|\vec{\lambda}'_1, \dots, \vec{\lambda}'_N) := \frac{1}{2} \left(1 \pm \frac{1}{\sqrt{2N}} \sum_{j=1}^N \vec{b}_j \cdot \vec{\lambda}'_j \right), \quad (\text{B11})$$

where $\vec{b}_j := (c_j, -s_j)^T$. Note that $\sum_j \vec{b}_j \cdot \vec{\lambda}'_j = \vec{b} \cdot \vec{\lambda}'$, where $\vec{b} := \bigoplus_j \vec{b}_j$ and $\vec{\lambda}' := \bigoplus_j \vec{\lambda}'_j$; however, since $|\vec{b}|^2 = \sum_j |\vec{b}_j|^2 = \sum_j (c_j^2 + s_j^2) \leq 2$ and $|\vec{\lambda}'|^2 = \sum_j |\vec{\lambda}'_j|^2 = N$, 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

$$\begin{aligned} P(+, \pm|\alpha, \beta) &= \int_{\Lambda} d\mu(\lambda) P_A(+|\alpha, \lambda) P_B(\pm|\beta, \lambda) \\ &= \int_{\Lambda} d\mu(\lambda) q_A(+|R_{m_1\alpha}\vec{\lambda}_1, \dots, R_{m_N\alpha}\vec{\lambda}_N) \\ &\quad \times q_B(\pm|R_{n_1\beta}\vec{\lambda}_1, \dots, R_{n_N\beta}\vec{\lambda}_N). \end{aligned} \quad (\text{B12})$$

We apply the substitution $\vec{\lambda}'_j := R_{m_j\alpha}\vec{\lambda}_j$ and $\lambda' := (\vec{\lambda}'_1, \dots, \vec{\lambda}'_N)$, noting that this does not change the integral due to our choice of measure:

$$\begin{aligned} P(+, \pm|\alpha, \beta) &= \int_{\Lambda} d\mu(\lambda') q_A(+|\vec{\lambda}'_1, \dots, \vec{\lambda}'_N) \\ &\quad \times q_B(\pm|R_{n_1\beta-m_1\alpha}\vec{\lambda}'_1, \dots, R_{n_N\beta-m_N\alpha}\vec{\lambda}'_N). \end{aligned} \quad (\text{B13})$$

¹These restrictions ensure that the coefficients c_j and s_j are associated with unique trigonometric functions.

Due to the definition of q_A and q_B , this equals

$$\int_{-\xi}^{\xi} \frac{d\phi'_1}{2\pi} \dots \int_{-\xi}^{\xi} \frac{d\phi'_N}{2\pi} \frac{1}{2} \left(1 \pm \frac{1}{\sqrt{2N}} \sum_j f_j(\phi'_j) \right), \quad (\text{B14})$$

where

$$f_j(\phi'_j) = c_j \cos(\phi'_j + n_j \beta - m_j \alpha) - s_j \sin(\phi'_j + n_j \beta - m_j \alpha). \quad (\text{B15})$$

Noting that

$$\int_{-\xi}^{\xi} f_j(\phi'_j) d\phi'_j = 2 \sin \xi [c_j \cos(m_j \alpha - n_j \beta) + s_j \sin(m_j \alpha - n_j \beta)], \quad (\text{B16})$$

we can evaluate the integral explicitly, obtaining

$$P(+\pm|\alpha, \beta) = \frac{1}{2} \left(\frac{\xi}{\pi} \right)^N \pm \frac{1}{2\sqrt{2N}} \left(\frac{\xi}{\pi} \right)^{N-1} \frac{\sin \xi}{\pi} f(\alpha, \beta). \quad (\text{B17})$$

Next let us look at the other probabilities

$$\begin{aligned} P(-, \pm|\alpha, \beta) &= \int_{\Lambda} d\mu(\lambda) P_A(-|\alpha, \lambda) P_B(\pm|\beta, \lambda) \\ &= \int_{\Lambda} d\mu(\lambda) [1 - P_A(+|\alpha, \lambda)] P_B(\pm|\beta, \lambda) \\ &= -P(+, \pm|\alpha, \beta) \\ &\quad + \int_{\Lambda} d\mu(\lambda) q_B(\pm|R_{n_1\beta}\vec{\lambda}_1, \dots, R_{n_N\beta}\vec{\lambda}_N), \end{aligned} \quad (\text{B18})$$

and the final integral vanishes on all $\vec{b}_j \cdot \vec{\lambda}'_j$ terms of q_B , leaving only the constant term $\frac{1}{2}$, that is,

$$P(-, \pm|\alpha, \beta) = \frac{1}{2} - P(+, \pm|\alpha, \beta). \quad (\text{B19})$$

These give the correlation function

$$C(\alpha, \beta) = \sqrt{\frac{2}{N}} \left(\frac{\xi}{\pi} \right)^{N-1} \frac{\sin \xi}{\pi} f(\alpha, \beta). \quad (\text{B20})$$

Finally, we define γ_N as the largest admissible prefactor among all possible choices of ξ . ■

Let us now introduce a constant term.

Lemma 3. Consider any two-angle correlation function

$$\begin{aligned} C(\alpha, \beta) &= c_0 + \sum_{j=1}^N [c_j \cos(m_j \alpha - n_j \beta) \\ &\quad + s_j \sin(m_j \alpha - n_j \beta)], \end{aligned} \quad (\text{B21})$$

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 $(m_i, n_i) = (m_j, n_j)$ if $i \neq j$. If

$$\max_{\alpha, \beta} |C(\alpha, \beta) - c_0| \leq \gamma_N (1 - |c_0|) \quad (\text{B22})$$

with constant γ_N given by

$$\gamma_N = \begin{cases} \sqrt{2}/\pi & \text{if } N = 1 \\ 0.184\,375\dots & \text{if } N = 2 \\ 0.103\,893\dots & \text{if } N = 3 \\ \sqrt{2}e^{-1}N^{-3/2} & \text{if } N \geq 4, \end{cases} \quad (\text{B23})$$

then this correlation function has a local hidden-variable model.

Proof. First, we obtain the form of γ_N by solving the optimization problem of Lemma 2 exactly for $N = 1, 2, 3$, substituting $x = \pi(1 - \frac{1}{N})$, and using

$$\left(1 - \frac{1}{N}\right)^{N-1} \sin \left[\pi \left(1 - \frac{1}{N}\right) \right] \geq \frac{\pi}{Ne} \quad \text{for } N \geq 4. \quad (\text{B24})$$

We can add the constant function $1/\sqrt{2}$ to the orthonormal system in Eq. (B5); similar reasoning as in the proof of Lemma 2 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

$$C(\alpha, \beta) = c_0 \mathbf{1} + (1 - c_0) f(\alpha, \beta), \quad (\text{B25})$$

where $\mathbf{1}$ 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 2. If the inequality (B22) holds, then

$$\max_{\alpha, \beta} |f(\alpha, \beta)| = \frac{1}{1 - c_0} \max_{\alpha, \beta} |C(\alpha, \beta) - c_0| \leq \gamma_N, \quad (\text{B26})$$

and so Lemma 2 proves that $f(\alpha, \beta)$ is a classical correlation function. Moreover, $\mathbf{1}$ is trivially a classical correlation function, and thus $C(\alpha, \beta)$ must be, which is a convex combination of the two. Then case $-1 < c_0 < 0$ can be treated analogously, using that $-\mathbf{1}$ is a classical correlation function too. ■

Proof of Theorem 2a. Consider an $\text{SO}(2) \times \text{SO}(2)$ box, with a correlation function in the form of Eq. (4) with maximum (half-)integer $J \neq 0$. If

$$\max_{\alpha, \beta} |C(\alpha, \beta) - C_{00}| \leq \gamma_J (1 - |C_{00}|), \quad (\text{B27})$$

where C_{00} is the angle-independent contribution to the correlation function [as in Eq. (4)] and γ_J is a given by

$$\gamma_J = \sqrt{2}e^{-1} [4J(2J+1)]^{-3/2}, \quad (\text{B28})$$

then there is a LHV model that accounts for these correlations.

Proof. This follows as a corollary of Lemma 3. We convert between the form of correlations in Eqs. (4) and (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 $\gamma_J = \sqrt{2}e^{-1} [4J(2J+1)]^{-3/2}$. ■

4. Witnessing nonlocality

Bell inequalities can be chained by direct addition. For instance, suppose one takes a CHSH inequality (5) with measurements $\{x_1, y_2, x_3, y_4\}$ and a second with measurements $\{x_1, y_4, x_5, y_6\}$. Adding these together yields $|C(x_1, y_2) + C(x_3, y_2) + C(x_3, y_4) + C(x_5, y_4) + C(x_5, y_6) - C(x_1, y_6)| \leq 4$. 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 Braunstein-Caves inequality (BCI) [28]:

$$|C(x_1, y_2) + C(x_3, y_2) + C(x_3, y_4) + \dots + C(x_{N-1}, y_N) - C(x_1, y_N)| \leq N - 2. \quad (\text{B29})$$

If such an equation is violated, then no LHV can account for these statistics.²

Recall that Eq. (4) gives the generic $\text{SO}(2) \times \text{SO}(2)$ correlation function. If we restrict ourselves to relational correlations, this amounts to setting $S_{mn} = C_{mn} = 0$ when $m \neq n$, such that the correlation function has a single parameter form

$$C(\beta - \alpha) = \sum_{m=0}^{2J} C_m \cos[m(\beta - \alpha)] + S_m \sin[m(\beta - \alpha)], \quad (\text{B30})$$

where J is some positive (half-)integer and $C_m := C_{mm}$, $S_m := S_{mm}$.

Lemma 4. Consider relational $\text{SO}(2) \times \text{SO}(2)$ 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

$$\delta_N := \frac{(\Theta_- - \Theta_+) \bmod 2\pi}{N - 1}. \quad (\text{B31})$$

We use the notation $x \bmod 2\pi$ 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.

We construct an 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

$$\begin{aligned} a_i &= (i - 1)\delta_N \quad \text{for odd } i, \\ b_i &= \Theta_+ + (i - 1)\delta_N \quad \text{for even } i \end{aligned} \quad (\text{B32})$$

(illustrated in Fig. 3). This amounts to setting the arguments of the correlation functions featured in the BCI to

$$\begin{aligned} b_2 - a_1 &= \dots = b_{2m} - a_{2m-1} = \Theta_+ + \delta_N, \\ b_2 - a_3 &= \dots = b_{2m} - a_{2m+1} = \Theta_+ - \delta_N, \\ b_N - a_1 &= \Theta_-, \end{aligned} \quad (\text{B33})$$

where equality is taken modulo 2π .

²The BCI can also be directly justified, just as the CHSH inequality. One writes $\sigma_{x_1}(\sigma_{y_2} - \sigma_{y_N}) + \sigma_{x_3}(\sigma_{y_2} + \sigma_{y_4}) + \dots + \sigma_{x_{N-1}}(\sigma_{y_{N-2}} + \sigma_{y_N})$ for spins $\{\sigma_i \in \{+1, -1\}\}$ and notes that if $\sigma_{y_2} = \sigma_{y_4} = \dots = \sigma_{y_N}$, then $\sigma_{y_2} - \sigma_{y_N} = 0$. This bounds the expression to $N - 2$. Convex combinations, such as Eq. (B29), cannot exceed this value.

FIG. 3. Measurement angles for generic correlation function. The first choice of measurement angles is chosen such that $b_2 - a_1 = \Theta_+ + \delta$. Subsequent choices then precess by 2δ such that ultimately $b_N - a_1 = \Theta_-$.

With such assignments, the BCI is then written

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

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

$$\begin{aligned} (N - 1)[1 - k\delta_N^2 + O(\delta_N^3)] + 1 &\leq N - 2, \\ N + O((N - 1)^{-1}) &\leq N - 2, \end{aligned} \quad (\text{B35})$$

which for large enough N will eventually be violated. ■

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 5. Consider relational $\text{SO}(2) \times \text{SO}(2)$ correlations [of the form of Eq. (B30)] for finite (half-)integer J . Expressed as a single parameter function $C(\beta - \alpha)$, the second derivative is everywhere bounded:

$$\left| \frac{d^2 C(\beta - \alpha)}{d(\beta - \alpha)^2} \right| \leq \frac{\sqrt{2}J(2J + 1)(4J + 1)}{3}. \quad (\text{B36})$$

Proof. In polar form, the correlation function is

$$C(\beta - \alpha) = A_0 + \sum_{m=1}^{2J} A_m \cos[m(\beta - \alpha) - \phi_m], \quad (\text{B37})$$

where $A_0 = C_0$, $A_m = \sqrt{C_m^2 + S_m^2}$, and

$$\phi_m = \begin{cases} \arctan(S_m/C_m) & \text{if } C_m \neq 0 \\ \pi/2 & \text{if } C_m = 0, S_m \geq 0 \\ -\pi/2 & \text{if } C_m = 0, S_m < 0. \end{cases} \quad (\text{B38})$$

The second derivative with respect to $\beta - \alpha$ is

$$\frac{d^2}{d(\beta - \alpha)^2} C(\beta - \alpha) = \sum_{m=1}^{2J} -m^2 A_m \cos[m(\beta - \alpha) - \phi_m]. \quad (\text{B39})$$

Because $C(\beta - \alpha)$ is bounded everywhere to $[-1, 1]$, its L^2 -norm $\|C\|^2 := \frac{1}{2\pi} \int_0^{2\pi} d\theta |C(\theta)|^2$ is bounded within $[0, 1]$.

Thus we may determine a maximum value over all m for the amplitude A_m . Using the orthonormality of the functions 1 , $\sqrt{2}\cos(m\theta + a)$, and $\sqrt{2}\cos(n\theta + b)$ under the corresponding inner product $\langle f, g \rangle := \frac{1}{2\pi} \int_0^{2\pi} d\theta f(\theta)g(\theta)$, we get $\|C\|^2 = A_0^2 + \frac{1}{2} \sum_{m=1}^{2J} A_m^2$. Since this is upper bounded by 1, we get $A_m^2 \leq 2$ for all $m \geq 1$ and so

$$\left| \frac{d^2 C(\beta - \alpha)}{d(\beta - \alpha)^2} \right| \leq \sum_{m=1}^{2J} \sqrt{2} m^2 = \frac{\sqrt{2} J(2J+1)(4J+1)}{3}. \quad (\text{B40})$$

Lemma 6. Consider relational $\text{SO}(2) \times \text{SO}(2)$ correlations [of the form of Eq. (B30)] for finite positive (half-)integer J . Let there be some angle difference Θ_+ , where $C(\Theta_+) \geq 1 - \varepsilon$, and some other angle difference Θ_- , where $C(\Theta_-) \leq 1 - \Delta$, with $\varepsilon \geq 0$ and $\Delta > 0$. If

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

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 Θ'_+ . Since $C(\Theta'_+) \geq C(\Theta_+) \geq 1 - \varepsilon$, the premises of this lemma are also satisfied if Θ_+ is replaced by Θ'_+ , i.e., we can assume without loss of generality that C attains its global maximum at Θ_+ .

With these Θ_+ and Θ_- , we use the prescription in Lemma 4, 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:

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

Let us write $\delta\Theta := \Theta_- - \Theta_+ \bmod 2\pi$ such that $\delta_N = \frac{\delta\Theta}{N-1}$. Let $K \in \mathbb{R}$ be any constant such that $C''(x) \geq -K$ for all x ; it follows from Lemma 5 that such K exists, and we will fix K later in accordance with that lemma. Since Θ_+ 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

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

Thus, Eq. (B42) implies that

$$(N-1) \left(1 - \varepsilon - K \frac{\delta_N^2}{2} \right) - (1 - \Delta) \leq N - 2. \quad (\text{B44})$$

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 $(N-1)$:

$$\varepsilon(N-1)^2 - \Delta(N-1) + \frac{K}{2}(\delta\Theta)^2 < 0. \quad (\text{B45})$$

If this equation has a solution for some even integer N , then the nonexistence of a LHV model follows. If $\varepsilon = 0$, then there will always be a solution for large enough N , recovering

Lemma 4. 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 zeros over the real numbers. The zeros are

$$N_{\pm} - 1 = \frac{\Delta \pm \sqrt{\Delta^2 - 2\varepsilon K(\delta\Theta)^2}}{2\varepsilon}, \quad (\text{B46})$$

and so the following inequality is necessary for the existence of a solution of Eq. (B45):

$$\Delta^2 > 2\varepsilon K(\delta\Theta)^2. \quad (\text{B47})$$

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. (B45) is negative for all real numbers $N \in (N_-, N_+)$, where $0 < N_- < N_+$. Now this interval definitely contains an even integer N if $N_+ - N_- > 2$. Since $N_+ - N_- = \sqrt{\Delta^2 - 2\varepsilon K(\delta\Theta)^2}/\varepsilon$, this difference is larger than 2 if and only if

$$4\varepsilon^2 + 2\varepsilon K(\delta\Theta)^2 - \Delta^2 < 0. \quad (\text{B48})$$

The two solutions of the corresponding quadratic equation are

$$\varepsilon_{\pm} = \frac{-K(\delta\Theta)^2 \pm \sqrt{K^2(\delta\Theta)^4 + 4\Delta^2}}{4}. \quad (\text{B49})$$

They are both real, and $\varepsilon_- < 0 < \varepsilon_+$. Thus, $\varepsilon < \varepsilon_+$ implies a suitable solution of Eq. (B45), i.e., rules out the existence of a LHV model.

In fact, if $\varepsilon < \varepsilon_+$, then we automatically get

$$4\varepsilon < -K(\delta\Theta)^2 + K(\delta\Theta)^2 \sqrt{1 + \frac{4\Delta^2}{K^2(\delta\Theta)^4}} \leq \frac{2\Delta^2}{K(\delta\Theta)^2}, \quad (\text{B50})$$

i.e., Eq. (B47) is automatically satisfied. Now considering ε_+ as a function in $\delta\Theta$, this function is decreasing for $\delta\Theta > 0$. Since $\delta\Theta \leq 2\pi$, $\varepsilon < \varepsilon_+(2\pi)$ implies that $\varepsilon < \varepsilon_+(\delta\Theta) \equiv \varepsilon_+$. Thus, the inequality

$$\varepsilon < \frac{-K(2\pi)^2 + \sqrt{K^2(2\pi)^4 + 4\Delta^2}}{4} \quad (\text{B51})$$

implies a violation of a BCI. The statement of the lemma now follows from taking the value of K from Lemma 5 and by substituting $K_J := \pi^2 K$. ■

This has consequence for generic (possibly nonrelational) $\text{SO}(2) \times \text{SO}(2)$ settings.

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

$$\varepsilon < -K_J + \sqrt{K_J^2 + \frac{\Delta^2}{4}} = \frac{\Delta^2}{8K_J} + O(K_J^{-2}), \quad (\text{B52})$$

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

Proof. Subtracting the nonrelational parts of $C(\alpha, \beta)$ is equivalent to performing the following integration:

$$C_{\text{rel}}(\alpha, \beta) = \frac{1}{2\pi} \int_0^{2\pi} d\phi C(\alpha + \phi, \beta + \phi). \quad (\text{B53})$$

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 ϕ 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 6 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. ■

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 $C_A(\alpha, \lambda) := \sum_{a \in \{-1, +1\}} a P_A(a|\alpha, \lambda)$ and $C_B(\beta, \lambda) := \sum_{b \in \{-1, +1\}} b P_B(b|\beta, \lambda)$ such that

$$C(\alpha, \beta) = \int_\Lambda d\lambda P_\Lambda(\lambda) C_A(\alpha, \lambda) C_B(\beta, \lambda). \quad (\text{B54})$$

Suppose that there are two angles θ'_+ and θ'_- such that our protocol gives correlation values $C_{\text{rel}}(\theta'_\pm)$ very close to ± 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 7. Suppose that $\theta_+, \theta_- \in [0, 2\pi)$ are such that $\theta_- - \theta_+ = \frac{m}{n}\pi$, 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

$$C(\theta_+) = +1, \quad C(\theta_-) = -1. \quad (\text{B55})$$

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 α and β to make this the case). Define $C_A(x, \lambda) = C_B(x, \lambda) := f(x + \lambda)$, where $f: \mathbb{R} \rightarrow \{-1, +1\}$ is the 2π -periodic extension of

$$f(x) := \begin{cases} +1 & \text{if } \frac{x}{\pi} \in [0, \frac{1}{n}) \cup [\frac{2}{n}, \frac{3}{n}) \cup \dots \cup [\frac{2n-2}{n}, \frac{2n-1}{n}) \\ -1 & \text{for all other } x \in [0, 2\pi). \end{cases} \quad (\text{B56})$$

That is, f is a square-wave function of period $\frac{2\pi}{n}$. This f is piecewise continuous and satisfies $f(x + \frac{\pi}{n}) = -f(x)$ for all x . Thus, $f(x + \frac{3}{n}\pi) = -f(x + \frac{2}{n}\pi) = f(x + \frac{1}{n}\pi) = -f(x)$ for all x , and in particular, by induction, $f(x + \frac{m}{n}\pi) = -f(x)$ for all x since m is odd by assumption. Now, defining $C(\alpha, \beta)$ as in Eq. (B54), this correlation function is relational, since

$$\begin{aligned} C(\alpha + x, \beta + x) &= \frac{1}{2\pi} \int_0^{2\pi} f(\alpha + x + \lambda) f(\beta + x + \lambda) d\lambda \\ &= \frac{1}{2\pi} \int_0^{2\pi} f(\alpha + \lambda') f(\beta + \lambda') d\lambda' \\ &= C(\alpha, \beta) \end{aligned} \quad (\text{B57})$$

by substitution and due to the 2π periodicity of f . Furthermore,

$$\begin{aligned} C(\theta_+) &= C(0, 0) = \frac{1}{2\pi} \int_0^{2\pi} [f(\lambda)]^2 d\lambda = 1, \\ C(\theta_-) &= C\left(\frac{m}{n}\pi, 0\right) = \frac{1}{2\pi} \int_0^{2\pi} f\left(\frac{m}{n}\pi + \lambda\right) f(\lambda) d\lambda \\ &= -\frac{1}{2\pi} \int_0^{2\pi} [f(\lambda)]^2 d\lambda = -1. \end{aligned} \quad (\text{B58})$$

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 behavior under rotations.

Definition 2 (transforming fundamentally). Consider an $\text{SO}(d)$ box $P(a|x)$, where $d \geq 2$. Let $x_0 \in \mathcal{X}$. We say that this box transforms fundamentally under rotations if for all $x \in \mathcal{X}$ and all $R_x \in \mathcal{G}$ with $R_x x_0 = x$ one finds

$$P(a|x) \equiv P(a|R_x x_0) = c_0^a + \sum_{i,j=1}^d (R_x)_{i,j} c_{i,j}^a, \quad (\text{C1})$$

where $(R_x)_{i,j}$ is the fundamental matrix representation of $R_x \in \mathcal{G}$, and c_0^a and $c_{i,j}^a$ 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 $\mathcal{G} = \text{SO}(d)$. Since $\mathcal{G}$ is transitive on $\mathcal{X}$, the existence of the above representation is independent of the particular x_0 : any alternative $x'_0 \in \mathcal{X}$ satisfies $x'_0 = Sx_0$ for some $S \in \mathcal{G}$, satisfying the above with $R' = RS^{-1}$.

Lemma 8. Suppose that $\mathcal{X} = S^{d-1}$ (the unit sphere) and $P(a|\vec{x})$ transforms fundamentally under rotations in $\mathcal{G} = \text{SO}(d)$. Then

$$P(a|\vec{x}) = c_0^a + \vec{c}^a \cdot \vec{x}, \quad (\text{C2})$$

where constants $c_0^a \in \mathbb{R}$ and $\vec{c}^a \in \mathbb{R}^d$ satisfy

$$\sum_{a \in \mathcal{A}} c_0^a = 1, \quad \sum_{a \in \mathcal{A}} \vec{c}^a = \vec{0} \quad (\text{C3})$$

such that for all a , $c_0^a \geq 0$ and $|\vec{c}^a| \leq \min(c_0^a, 1 - c_0^a)$.

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 $\vec{x}_0 := \vec{e}_1 = (1, 0, \dots, 0)^T$. Set some choice of rotations $\vec{x} \mapsto R_{\vec{x}}$ with $R_{\vec{x}}\vec{x}_0 = \vec{x}$. Consider the stabilizer subgroup $\mathcal{G}_{\vec{e}_1} := \{R \in \text{SO}(d) \mid R\vec{e}_1 = \vec{e}_1\}$:

$$\mathcal{G}_{\vec{e}_1} = \left\{ \begin{pmatrix} 1 & \vec{0}^T \\ \vec{0} & T \end{pmatrix} \mid T \in \text{SO}(d-1) \right\}. \quad (\text{C4})$$

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 $\mathcal{X} = \text{SO}(d)/\text{SO}(d-1)$, i.e., the $(d-1)$ sphere. For $d \geq 3$, we have $\int_{\text{SO}(d-1)} T dT = 0$, and thus

$$\int_{\mathcal{G}_{\vec{e}_1}} S dS = Q := \begin{pmatrix} 1 & \vec{0}^T \\ \vec{0} & \mathbf{0} \end{pmatrix}. \quad (\text{C5})$$

Since $R_{\vec{x}}S\vec{e}_1 = \vec{x}$ for every $S \in \mathcal{G}_{\vec{e}_1}$, every rotation matrix $R_{\vec{x}}S$ can be substituted for $R_{\vec{x}}$ into Definition 2. Thus $P(a|\vec{x}) = c_0^a + \sum_{i,j=1}^d (R_{\vec{x}}S)_{i,j} c_{i,j}^a$. By taking the average over all $S \in \mathcal{G}_{\vec{e}_1}$ according to the Haar measure, we get

$$P(a|\vec{x}) = c_0^a + \sum_{i,j=1}^d \left(R_{\vec{x}} \int_{\mathcal{G}_{\vec{e}_1}} S dS \right)_{i,j} c_{i,j}^a. \quad (\text{C6})$$

However, $R_{\vec{x}}Q = (\vec{x}, \vec{0}, \dots, \vec{0})$, i.e., a matrix with the 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 $R_{\vec{x}}$, namely, $R_{\vec{x}} = \begin{pmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{pmatrix}$. Then $P(a|\vec{x})$ being affine linear in $R_{\vec{x}}$ is equivalent to being affine linear in $\vec{x}$.

From normalization, $\sum_a P(a|\vec{x}) = 1 \forall \vec{x} \in \mathcal{X}$, which by transitivity of $\mathcal{G}$ on $\mathcal{X}$ can be rewritten $\sum_a P(a|R\vec{x}_0) = 1 \forall R \in \mathcal{G}$. Suppose we take the Haar average of $\mathcal{G}$ over both sides of this constraint,

$$\begin{aligned} \int_{\text{SO}(d)} dR \sum_a P(a|R\vec{x}_0) &= \sum_a \left(c_0^a + \vec{c}^a \cdot \int_{\text{SO}(d)} dR R \vec{x}_0 \right) \\ &= \sum_a c_0^a = 1, \end{aligned} \quad (\text{C7})$$

where we have used $\int_{\text{SO}(d)} R dR = 0$. Since $\sum_a P(a|R\vec{x}_0) = 1$ for each individual $R \in \mathcal{G}$, we have $(\sum_a \vec{c}^a) \cdot (R\vec{x}_0) = 0$. Since by transitivity $\dim[\text{span}(\{R\vec{x}_0\}_{R \in \mathcal{G}})] = d$, it follows that $\sum_a \vec{c}^a = \vec{0}$.

For any $\vec{x}$, one may find some $R \in \text{SO}(d)$ such that $R\vec{x} = -\vec{x}$ [since both $\vec{x}$ and $-\vec{x} \in S^{d-1}$ and $\text{SO}(d)$ is transitive on S^{d-1}]. Hence, for the black box $P(a|\vec{x})$, there is always another black box $P(a|-\vec{x})$ such that the average statistics of these two boxes is given by $\frac{1}{2}[P(a|\vec{x}) + P(a|-\vec{x})] = c_0^a$. Clearly, then $c_0^a \geq 0$. Finally, from the definition of the dot product, $\min_{\vec{x} \in S^{d-1}} (\vec{c} \cdot \vec{x}) = -|\vec{c}|$. Thus, if $|\vec{c}^a| > c_0^a$, there will be some $\vec{x}$ such that $P(a|\vec{x}) = c_0^a - |\vec{c}^a| < 0$, which is not a valid probability. Similarly, $\max_{\vec{x} \in S^{d-1}} (\vec{c} \cdot \vec{x}) = |\vec{c}|$, so if $|\vec{c}^a| > 1 - c_0^a$, there will be some $\vec{x}$ such that $P(a|\vec{x}) = c_0^a + |\vec{c}^a| \geq 1$. Hence $|\vec{c}^a| \leq \min(c_0^a, 1 - c_0^a)$.

The converse follows from the transitivity of $\text{SO}(d)$ on S^{d-1} : Any $\vec{x}$ can be expressed as $R\vec{x}_0$ for some fixed $\vec{x}_0$ and $R \in \text{SO}(d)$. Thus Eq. (C2) can be written $P(a|\vec{x}) = c_0^a + \vec{c}^a \cdot R\vec{x}_0$, which has the form of Eq. (C1). ■

We can formally define the concept of an unbiased black box where if the input orientation is randomized, no particular outcome is preferred.

Definition 3 (unbiased). Consider a $\mathcal{G}$ box $P(a|x)$ for some compact group $\mathcal{G}$. We say that this box is unbiased if the Haar average of $P(a|R\vec{x})$ over $R \in \mathcal{G}$ is the same for all $a \in \mathcal{A}$.

It follows from normalization that if a black box transforms fundamentally under rotations and is unbiased, it may be written in the form $P(a|\vec{x}) = \frac{1}{|\mathcal{A}|} + \vec{c}^a \cdot \vec{x}$.

We extend both these definitions to the local parts of a bipartite system by considering the conditional boxes

$$P_A^{b,\vec{y}}(a|\vec{x}) := P(a, b|\vec{x}, \vec{y})/P_B(b|\vec{y}) \quad (b, \vec{y} \text{ fixed}), \quad (\text{C8})$$

$$P_B^{a,\vec{x}}(b|\vec{y}) := P(a, b|\vec{x}, \vec{y})/P_A(a|\vec{x}) \quad (a, \vec{x} \text{ fixed}), \quad (\text{C9})$$

defined whenever $P_B(b|\vec{y}) > 0$ and $P_A(a|\vec{x}) > 0$, respectively.

A conditional box can be thought of as the black box Alice has if she is told Bob's measurement and outcome. (This is in contrast to a marginal black box, which quantifies Alice's statistics when she knows nothing of Bob's measurement or outcome.) No signaling implies the existence of well-defined marginal boxes $P_B(b|\vec{y})$ and $P_A(a|\vec{x})$.

Definition 4. We say that a no-signaling bipartite box $P(a, b|\vec{x}, \vec{y})$ transforms fundamentally locally (is locally unbiased) if all conditional boxes transform fundamentally (are unbiased).

The next two lemmas show that these properties are preserved by convex combinations of boxes.

Lemma 9. Let $\{P_i(a, b|\vec{x}, \vec{y})\}_{i=1, \dots, N}$ be a set of nonsignaling bipartite black boxes that transform fundamentally locally. Any convex combination $P(a, b|\vec{x}, \vec{y}) := \sum_i \lambda_i P_i(a, b|\vec{x}, \vec{y})$ where all $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$ also transforms fundamentally locally.

Proof. First, we calculate the marginal distribution $P_A(a|\vec{x}) := \sum_b P(a, b|\vec{x}, \vec{y}) = \sum_b \sum_i \lambda_i P_i(a, b|\vec{x}, \vec{y}) = \sum_i \lambda_i \sum_b P_i(a, b|\vec{x}, \vec{y}) = \sum_i \lambda_i P_{A,i}(a|\vec{x})$. Similarly, $P_B(b|\vec{y}) = \sum_i \lambda_i P_{B,i}(b|\vec{y})$. First, we note that $P_B(b|\vec{y}) = 0$ only if $P_{B,i}(b|\vec{y}) = 0$ 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 $P_B(b|\vec{y}) > 0$.

With $P(a, b|\vec{x}, \vec{y}) = \sum_i \lambda_i P_i(a, b|\vec{x}, \vec{y}) = \sum_i' \lambda_i P_{B,i}(b|\vec{y}) P_A^{b,\vec{y}}(a|\vec{x})$ we obtain

$$P_A^{b,\vec{y}}(a|\vec{x}) = \sum_i' \frac{\lambda_i P_{B,i}(b|\vec{y})}{P_B(b|\vec{y})} P_{A,i}^{b,\vec{y}}(a|\vec{x}). \quad (\text{C10})$$

Here $\sum_i'$ denotes a sum over all those i for which $P_{B,i}(b|\vec{y}) > 0$. These are exactly the i for which $P_{A,i}^{b,\vec{y}}(a|\vec{x})$ is well defined. Meanwhile, $\sum_i' \frac{\lambda_i P_{B,i}(b|\vec{y})}{P_B(b|\vec{y})} = 1$, and hence we may define $\mu_i := \frac{\lambda_i P_{B,i}(b|\vec{y})}{P_B(b|\vec{y})}$ for those i with $P_{B,i}(b|\vec{y}) > 0$, 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 $P_B^{a,\vec{x}}(b|\vec{y})$.

Since the constituent conditional boxes transform fundamentally, from Lemma 8 we write $P_{A,i}^{b,\vec{y}}(a|\vec{x}) = c_{i,0}^{(b,\vec{y}),a} + \vec{c}_i^{(b,\vec{y}),a} \cdot \vec{x}$. Then $P_A^{b,\vec{y}}(a|\vec{x}) = \sum_i \mu_i (c_{i,0}^{(b,\vec{y}),a} + \vec{c}_i^{(b,\vec{y}),a} \cdot \vec{x}) = c_0^{(b,\vec{y}),a} + \vec{c}^{(b,\vec{y}),a} \cdot \vec{x}$, where $c_0^{(b,\vec{y}),a} := \sum \mu_i c_{i,0}^{(b,\vec{y}),a}$ and $\vec{c}^{(b,\vec{y}),a} := \sum \mu_i \vec{c}_i^{(b,\vec{y}),a}$. By the converse part of Lemma 8, $P_A^{b,\vec{y}}(a|\vec{x})$ is thus a valid black box that transforms fundamentally. The same argument holds for Bob's conditional boxes. ■

Lemma 10. Let $\{P_i(a, b|\vec{x}, \vec{y})\}_{i=1,\dots,N}$ be a set of nonsignaling black boxes that are locally unbiased with respect to $\mathcal{G}$. Any convex combination $P(a, b|\vec{x}, \vec{y}) := \sum_i \lambda_i P_i(a, b|\vec{x}, \vec{y})$ 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 9 we have seen that there exists a probability distribution $\{\mu_i\}_i$ such that $P_A^{b,\vec{y}}(a|\vec{x}) = \sum_i \mu_i P_{A,i}^{b,\vec{y}}(a|\vec{x})$. Thus we find

$$\begin{aligned} \int P_A^{b,\vec{y}}(a|R\vec{x}) dR &= \sum_i \mu_i \int P_{A,i}^{b,\vec{y}}(a|R\vec{x}) dR \\ &= \frac{\sum_i \mu_i}{|\mathcal{A}|} = \frac{1}{|\mathcal{A}|}, \end{aligned} \quad (C11)$$

and similarly for Bob's conditional boxes, and hence $P(a, b|\vec{x}, \vec{y})$ is also locally unbiased. ■

Lemma 11. Consider a bipartite black box with inputs $\mathcal{X} = \mathcal{Y} = S^{d-1}$ and binary outcomes $\mathcal{A} = \mathcal{B} = \{+1, -1\}$. If this box transforms fundamentally locally and is locally unbiased, then it describes quantum correlations.

Proof. From Lemma 8, binary-outcome conditional boxes that transform fundamentally and are unbiased can be written

$$P_A^{b,\vec{y}}(a|\vec{x}) := \begin{pmatrix} \frac{1}{2} \\ a\vec{c}^{(b,\vec{y})} \end{pmatrix} \begin{pmatrix} 1 \\ \vec{x} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \vec{c}^{(b,\vec{y})} \end{pmatrix} \begin{pmatrix} 1 \\ a\vec{x} \end{pmatrix}, \quad (C12)$$

$$P_B^{a,\vec{x}}(b|\vec{y}) := \begin{pmatrix} \frac{1}{2} \\ b\vec{c}^{(a,\vec{x})} \end{pmatrix} \begin{pmatrix} 1 \\ \vec{y} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \vec{c}^{(a,\vec{x})} \end{pmatrix} \begin{pmatrix} 1 \\ b\vec{y} \end{pmatrix} \quad (C13)$$

such that the joint probability distribution is given by

$$P(a, b|\vec{x}, \vec{y}) = P_B(b|\vec{y}) \begin{pmatrix} \frac{1}{2} \\ \vec{c}^{(b,\vec{y})} \end{pmatrix} \begin{pmatrix} 1 \\ a\vec{x} \end{pmatrix}, \quad (C14)$$

$$P(a, b|\vec{x}, \vec{y}) = P_A(a|\vec{x}) \begin{pmatrix} \frac{1}{2} \\ \vec{c}^{(a,\vec{x})} \end{pmatrix} \begin{pmatrix} 1 \\ b\vec{y} \end{pmatrix}. \quad (C15)$$

This defines a map $\tilde{\omega}_{AB}$ acting on $\vec{e}_{a,\vec{x}} := (1, a\vec{x})^\top$ and $\vec{e}_{b,\vec{y}} := (1, b\vec{y})^\top$ such that $\tilde{\omega}_{AB}(\vec{e}_{a,\vec{x}}, \vec{e}_{b,\vec{y}}) = P(a, b|\vec{x}, \vec{y})$. 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 $(1, \vec{z})^\top$ for $\vec{z} \in S^{d-1}$. We may then define an Archimedean order unit (AOU) [52] $\vec{u} := (2, 0, \dots, 0)^\top \in \mathbb{R}^{d+1}$ 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 will employ a result from Kleinmann *et al.* [52] (generalizing a result by Barnum *et al.* [53]) that pertains to bilinear maps on positive Euclidean cones. If a bilinear map ω_{AB} on such cones is both unital and positive, then there exists a bipartite quantum system ρ_{AB} and a map from each point $\vec{a} \in A^+$ and $\vec{b} \in B^+$ onto local quantum POVM elements M_a and M_b such that $\omega_{AB}(\vec{a}, \vec{b}) = \text{tr}(\rho_{AB} M_a \otimes M_b)$.

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

$$\vec{e}_{+a,\vec{x}} + \vec{e}_{-a,\vec{x}} = \vec{u} = \vec{e}_{+b,\vec{y}} + \vec{e}_{-b,\vec{y}}, \quad (C16)$$

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

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_0 be any nonsignaling (2,2,2) behavior (for example, a PR box) and define

$$\begin{aligned} P(a, b|\vec{x}, \vec{y}) &:= \lambda_A \lambda_B P_0(a, b|0, 0) + \lambda_A \bar{\lambda}_B P_0(a, b|0, 1) \\ &\quad + \bar{\lambda}_A \lambda_B P_0(a, b|1, 0) + \bar{\lambda}_A \bar{\lambda}_B P_0(a, b|1, 1), \end{aligned} \quad (C17)$$

where $a, b \in \{-1, +1\}$, $\vec{x}, \vec{y} \in S^{d-1}$, $\lambda_A := \frac{1}{2}(1 + x_1)$, $\bar{\lambda}_A := 1 - \lambda_A$, $\lambda_B := \frac{1}{2}(1 + y_1)$, and $\bar{\lambda}_B := 1 - \lambda_B$. 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_0 . This defines a valid nonsignaling box and the linear dependence of the outcome probabilities on $\vec{x}$ ($\vec{y}$) demonstrate, via Lemma 8, that P transforms fundamentally locally. However, it reproduces P_0 via $P_0(a, b|r, t) = P(a, b|\vec{x}_r, \vec{y}_t)$, where $\vec{x}_0 = \vec{y}_0 = (1, 0, \dots, 0)$ and $\vec{x}_1 = \vec{y}_1 = (-1, 0, \dots, 0)$.

Now we show a converse statement so that we get an exact classification of the quantum (2,2,2) behaviors; 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 12. Let $d \geq 2$. Then all extremal quantum (2,2,2) behaviors can be realized by locally unbiased $\text{SO}(d)$ boxes that transform fundamentally locally with $\mathcal{X}_A = \mathcal{X}_B = S^{d-1}$; the two settings (inputs) correspond to two choices of directions.

Proof. It has been shown [25,34,54,55] that the extremal quantum (2,2,2) behaviors can be realized by rank-1 projective measurements on two-qubit pure states. Any extremal quantum (2,2,2) behavior $P(a, b|r, t)$ can then be written in the form $P(a, b|r, t) = \text{Tr}[\rho_{AB}(E_r^{(a)} \otimes F_t^{(b)})]$, where ρ is a pure state of two qubits and $E_r^{(a)}$ and $F_t^{(b)}$ are qubit rank-1 projectors, $a, b \in \{-1, +1\}$ and $r, t \in \{1, 2\}$. We will show that there exists a nonsignaling $\text{SO}(d) \times \text{SO}(d)$ 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 $E := E_1^{(+1)}$ and $\tilde{E} := E_2^{(+1)}$. As $\text{Tr } E = 1$, its expansion in the Pauli operator basis is of the form $E = \frac{1}{2}(\mathbb{1}_2 + E_x \sigma_x + E_y \sigma_y + E_z \sigma_z)$ and the associated Bloch vector $\vec{x}'_1 := (E_x, E_y, E_z)^T$ has Euclidean norm 1. Let $\vec{x}'_2$ be the Bloch vector similarly associated with $\tilde{E}$. 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 $F_t^{(b)}$.

Define a linear map $\Pi : \mathbb{R}^d \rightarrow \mathbb{R}^3$ in the following way. If $d = 2$, set $\Pi(v_1, v_2)^T := (v_1, v_2, 0)^T$; if $d \geq 3$, set $\Pi(v_1, \dots, v_d)^T := (v_1, v_2, v_3)^T$, which is an orthogonal projection (and the identity if $d = 3$). Furthermore, for $\vec{v} \in \mathbb{R}^3$, define $E_{\vec{v}} := \frac{1}{2}(\mathbb{1}_2 + \vec{v} \cdot \vec{\sigma})$, which is positive-semidefinite whenever $|\vec{v}| \leq 1$. Consider the nonsignaling $\text{SO}(d) \times \text{SO}(d)$ box

$$P(a, b|\vec{x}, \vec{y}) := \text{Tr}[\rho_{AB} E_{a\Pi\vec{x}} \otimes E_{b\Pi\vec{y}}]. \quad (\text{C18})$$

Since $|a\Pi\vec{x}| \leq |\vec{x}| = 1$ for $\vec{x} \in S^{d-1}$ (and similarly for $b\Pi\vec{y}$), this defines a valid (quantum) behavior. The conditional boxes are

$$P_A^{b,\vec{y}}(a|\vec{x}) = \frac{\frac{1}{2} \text{Tr}\{\rho_{AB}[\mathbb{1} + a\vec{x} \cdot (\Pi^T \vec{\sigma})] \otimes E_{b\Pi\vec{y}}\}}{\text{Tr}(\rho_B E_{b\Pi\vec{y}})}. \quad (\text{C19})$$

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 8, $P(a, b|\vec{x}, \vec{y})$ 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 $d - 2$ com-

ponents 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 $(2, 2, 2)$ behaviors are exactly those that can be realized 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.

Lemma 11 tells us that $(2, S^{d-1}, 2)$ behaviors that transform fundamentally locally, and are locally unbiased, can be realized 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 $(2, 2, 2)$ behaviors, and since they can be realized by a quantum system, they are quantum $(2, 2, 2)$ behaviors.

The other direction follows from Lemma 12: All extremal quantum $(2, 2, 2)$ behaviors can be realized 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 behaviors, yielding all further quantum $(2, 2, 2)$ behaviors. ■

Theorem 3 cannot hold for all $d \geq 2$ without allowing shared randomness. For example, suppose that $d = 3$; then the proof of Lemma 11 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 ordinary two-qubit quantum state space. However, Donohue and Wolfe [36] (extending results by Pál and Vértesi [35]) have shown that the set of $(2, 2, 2)$ behaviors realizable on two qubits via POVMs is not convex and thus not equal to the convex set of quantum $(2, 2, 2)$ behaviors.

-
- [1] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777 (1935).
 - [2] J. S. Bell, On the Einstein Podolsky Rosen paradox, *Phys. Phys. Fiz.* **1**, 195 (1964).
 - [3] J. Clauser, M. Horne, A. Shimony, and R. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, *Phys. Rev. Lett.* **23**, 880 (1969).
 - [4] A. Aspect, P. Grangier, and G. Roger, Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities, *Phys. Rev. Lett.* **49**, 91 (1982).
 - [5] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenbergh, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, 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 (London)* **526**, 682 (2015).
 - [6] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419 (2014).
 - [7] D. Mayers and A. Yao, *Proceedings of the 39th Annual Symposium on Foundations of Computer Science, Palo Alto, 1998* (IEEE, Piscataway, 1998).
 - [8] J. Barrett, L. Hardy, and A. Kent, No Signaling and Quantum Key Distribution, *Phys. Rev. Lett.* **95**, 010503 (2005).
 - [9] R. Colbeck and R. Renner, Free randomness can be amplified, *Nat. Phys.* **8**, 450 (2012).
 - [10] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **113**, 140501 (2014).
 - [11] J. Tura, R. Augusiak, A. B. Sainz, T. Vértesi, M. Lewenstein, and A. Acín, Detecting nonlocality in many-body quantum states, *Science* **344**, 1256 (2014).
 - [12] R. Schmied, J.-D. Bancal, B. Allard, M. Fadel, V. Scarani, P. Treutlein, and N. Sangouard, Bell correlations in a Bose-Einstein condensate, *Science* **352**, 441 (2016).
 - [13] J. Pearl, *Causality: Models, Reasoning, and Inference* (Cambridge University Press, Cambridge, 2000).
 - [14] M. Nakahara, *Geometry, Topology and Physics* (IOP, Bristol, 2003).
 - [15] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani, Testing the Dimension of Hilbert Spaces, *Phys. Rev. Lett.* **100**, 210503 (2008).

- [16] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, *Phys. Rev. A* **84**, 010302(R) (2011).
- [17] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 1984* (IEEE, Piscataway, 1984), Vol. 3, pp. 175–179.
- [18] A. Acín, N. Gisin, and L. Masanes, From Bell’s Theorem to Secure Quantum Key Distribution, *Phys. Rev. Lett.* **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 (1994).
- [21] R. F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, *Phys. Rev. A* **40**, 4277 (1989).
- [22] R. Augusiak, M. Demianowicz, and A. Acín, Local hidden-variable models for entangled quantum states, *J. Phys. A: Math. Theor.* **47**, 424002 (2014).
- [23] M. Żukowski, Bell theorem involving all settings of measuring apparatus, *Phys. Lett. A* **177**, 290 (1993).
- [24] A. Sen(De), U. Sen, and M. Żukowski, Functional Bell inequalities can serve as a stronger entanglement witness than conventional Bell inequalities, *Phys. Rev. A* **66**, 062318 (2002).
- [25] B. S. Cirel’son, Quantum generalizations of Bell’s inequality, *Lett. Math. Phys.* **4**, 93 (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 $K_G(3)$, *Quantum* **1**, 3 (2017).
- [27] K. Nagata, W. Laskowski, M. Wieśniak, and M. Żukowski, Rotational Invariance as an Additional Constraint on Local Realism, *Phys. Rev. Lett.* **93**, 230403 (2004).
- [28] S. L. Braunstein and C. M. Caves, Wringing out better Bell inequalities, *Ann. Phys. (NY)* **202**, 22 (1990).
- [29] Z. Wang, S. Singh, and M. Navascués, Entanglement and Nonlocality in Infinite 1D Systems, *Phys. Rev. Lett.* **118**, 230401 (2017).
- [30] L. A. Khalfin and B. S. Tsirelson, in *Symposium on the Foundations of Modern Physics*, edited by P. Lahti and P. Mittelstaedt (World Scientific, Singapore, 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 (London)* **461**, 1101 (2009).
- [32] T. H. Yang, M. Navascués, L. Sheridan, and V. Scarani, Quantum Bell inequalities from macroscopic locality, *Phys. Rev. A* **83**, 022105 (2011).
- [33] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial, *Phys. Rev. Lett.* **96**, 250401 (2006).
- [34] M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín, Almost quantum correlations, *Nat. Commun.* **6**, 6288 (2015).
- [35] K. F. Pál and T. Vértesi, Concavity of the set of quantum probabilities for any given dimension, *Phys. Rev. A* **80**, 042114 (2009).
- [36] J. M. Donohue and E. Wolfe, Identifying nonconvexity in the sets of limited-dimension quantum correlations, *Phys. Rev. A* **92**, 062120 (2015).
- [37] A. Acín, R. Augusiak, D. Cavalcanti, C. Hadley, J. K. Korbicz, M. Lewenstein, L. Masanes, and M. Piani, Unified Framework for Correlations in Terms of Local Quantum Observables, *Phys. Rev. Lett.* **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 L. Masanes, Three-dimensionality of space and the quantum bit: An information-theoretic approach, *New J. Phys.* **15**, 053040 (2013).
- [40] P. A. Höhn and M. P. Müller, An operational approach to spacetime symmetries: Lorentz transformations from quantum communication, *New J. Phys.* **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, *Proc. R. Soc. 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, *Found. Phys.* **48**, 982 (2018).
- [44] T. van Himbeek, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Semi-device-independent framework based on natural physical assumptions, *Quantum* **1**, 33 (2017).
- [45] T. Van Himbeek and S. Pironio, Correlations and randomness generation based on energy constraints, [arXiv:1905.09117](https://arxiv.org/abs/1905.09117).
- [46] D. Rusca, T. van Himbeek, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, Self-testing quantum random-number generator based on an energy bound, *Phys. Rev. A* **100**, 062338 (2019).
- [47] R. D. Sorkin, Quantum mechanics as quantum measure theory, *Mod. Phys. Lett. A* **09**, 3119 (1994).
- [48] C. Ududec, H. Barnum, and J. Emerson, Three slit experiments and the structure of quantum theory, *Found. Phys.* **41**, 396 (2010).
- [49] U. Sinha, C. Couteau, T. Jennewein, R. Laflamme, and G. Weihs, Ruling out multi-order interference in quantum mechanics, *Science* **329**, 418 (2010).
- [50] Finite-dimensional representation, *Encyclopedia of Mathematics*, 2016 (unpublished), available at https://www.encyclopediaofmath.org/index.php?title=Finite-dimensional_representation&oldid=39848
- [51] V. F. Molchanov, A. U. Klimyk, and N. Y. Vilenkin, in *Representation Theory and Noncommutative Harmonic Analysis II*, edited by A. A. Kirillov (Springer, Berlin, 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, *Phys. Rev. Lett.* **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] L. Masanes, Extremal quantum correlations for N parties with two dichotomic observables per site, [arXiv:quant-ph/0512100](https://arxiv.org/abs/quant-ph/0512100).
- [55] B. Toner and F. Verstraete, Monogamy of Bell correlations and Tsirelson’s bound, [arXiv:quant-ph/0611001](https://arxiv.org/abs/quant-ph/0611001).