Can Observed Randomness Be Certified to Be Fully Intrinsic?

Chirag Dhara,[1,*] Gonzalo de la Torre,[1] and Antonio Acín[1,2]
[1]*ICFO–Institut de Ciencies Fotoniques, E–08860 Castelldefels, Barcelona, Spain*
[2]*ICREA–Institucio Catalana de Recerca i Estudis Avançats, E–08010 Barcelona, Spain*
(Received 8 July 2013; published 10 March 2014)

In general, any observed random process includes two qualitatively different forms of randomness: apparent randomness, which results both from ignorance or lack of control of degrees of freedom in the system, and intrinsic randomness, which is not ascribable to any such cause. While classical systems only possess the first kind of randomness, quantum systems may exhibit some intrinsic randomness. In this Letter, we provide quantum processes in which all the observed randomness is fully intrinsic. These results are derived under minimal assumptions: the validity of the no-signaling principle and an arbitrary (but not absolute) lack of freedom of choice. Our results prove that quantum predictions cannot be completed already in simple finite scenarios, for instance of three parties performing two dichotomic measurements. Moreover, the observed randomness tends to a perfect random bit when increasing the number of parties, thus, defining an explicit process attaining full randomness amplification.

DOI: 10.1103/PhysRevLett.112.100402 PACS numbers: 03.65.Ud, 03.67.Bg, 03.67.Mn

Physical theories aim at providing the best possible predictions for the phenomena occurring in nature. Consequently, on observing a probabilistic process, a natural question arises: how much, if any, of that is intrinsically unpredictable?

Consider an experimental setup in which a variable takes different values with different probabilities. This variable has observed randomness that can be easily estimated from the measured statistics. In general, we can distinguish two qualitatively different forms of randomness contributing to the observed randomness of a process. The first is the apparent randomness, which appears as a consequence of imperfections of the system, such as lack of knowledge and control of all the relevant degrees of freedom. Clearly, an improvement on our control of the setup reduces this form of randomness. The second form of randomness is termed intrinsic randomness and refers to the component of observed randomness that cannot be ascribed to imperfections. It is this second form of randomness that should be considered truly random, as any improvement on our control of the setup leaves it unchanged.

The quantitative contribution of each form of randomness to the observed randomness depends on the physical theory used to describe the process. In classical theories, for instance, all observed randomness is apparent, as it is always possible to explain any random classical process as the probabilistic mixture of deterministic classical processes [1,2]. Moving to the quantum domain, the axioms of quantum theory state that measurements on quantum particles yield intrinsically random outcomes. Yet, the fact that a theory makes predictions only in terms of probabilities does not necessarily imply the existence of intrinsic randomness. It may simply reflect some limitations of the formalism, in the sense that a better, more complete theory could restore determinism [3,4]. However, the nonlocal correlations observed when measuring entangled particles allow one to assess the randomness of a process independent of the full quantum formalism. Under only two assumptions, (i) the impossibility of instantaneous communication, known as the no-signaling principle, and (ii) that the measurement settings in a Bell test can be chosen at random, known as freedom of choice, do nonlocal quantum correlations necessarily imply intrinsic randomness [5]. This is because such correlations cannot be described as the probabilistic mixture of deterministic processes.

Up to now, in all Bell tests, the intrinsic randomness revealed by quantum nonlocality (under said assumptions) is also mixed with apparent randomness, resulting from the incompleteness of quantum theory. In this Letter, we ask the following fundamental question: is there any quantum process that is as intrinsically random as it is observed to be and, hence, cannot be better predicted? We answer this question in the affirmative by providing a family of quantum processes whose intrinsic randomness can be computed analytically for arbitrary system sizes and also demonstrating that this is strictly equal to the observed randomness. This implies that those events cannot be further completed, in the sense that a theory giving better predictions for these events should be either signaling or have no freedom of choice.

Our results are related to recent attempts to prove the completeness of quantum physics. In [6], Colbeck and Renner claimed that no no-signaling theory can have a better predictive power than quantum theory. However, the proof, which is based on the quantum violation of the chained Bell inequality, only works in an asymptotic regime where the number of measurements by the

observers tends to infinite. That is, any finite scenario in [6] is such that quantum predictions can be completed. Moreover, the proof assumes that the settings in the inequality can be chosen freely. This last assumption leaves a significant space for improvement from a logical perspective since the free process needed in the proof is already assumed to be complete. A similar reasoning can be applied to the regular Bell theorem where the assumption of availability of initial perfect randomness is referred to as the free-will assumption [7–11]. A possible way to strengthen the results on the completeness of quantum predictions is, hence, to weaken the said assumption by considering protocols for randomness amplification [12]. There, the intrinsic randomness of a quantum process could be proven using a source of imperfect randomness. In fact, the protocol for full randomness amplification given in [13] provides a Bell test in which a measured variable has an intrinsic randomness that tends to be equal to the observed randomness in the limit of an infinite number of parties. All these proofs, then, left open a fundamental question: could it be the case that, for all finite scenarios, there always exists a gap between the randomness that we observe and that we can certify? What if completeness of quantum theory is only an asymptotic property and, therefore, quantum predictions can be completed in any finite setup?

Our work answers these questions in the negative by providing finite-size Bell setups in which observed and intrinsic randomness are strictly equal. In fact, already an extremely simple Bell scenario consisting of three observers performing two dichotomic measurements produces events that cannot be completed. Moreover, our proof works using arbitrarily small randomness for the choice of measurements. In this sense, our results provide the strongest proof of completeness of quantum predictions.

Preliminaries.—Suppose that a Bell test is performed repeatedly among N parties and the resulting statistics is given by $P_{\text{obs}}(\mathbf{a}|\mathbf{x})$, where $\mathbf{a} = (a_1, \ldots, a_N)$ and $\mathbf{x} = (x_1, \ldots, x_N)$ are the string of outcomes and measurement inputs of the parties involved. Let g be a function acting on the measurement results $\mathbf{a}$. As previously explained, there are different physically relevant notions of randomness.

First, the observed randomness of g for measurements $\mathbf{x}$ is the randomness computed directly from the statistics. Operationally, this may be defined as the optimal probability of guessing the outcome of g for input $\mathbf{x}$

$$G_{\text{obs}}(g, \mathbf{x}, P_{\text{obs}}) = \max_{k \in \text{Im}(g)} P_{\text{obs}}(g(\mathbf{a}) = k|\mathbf{x}). \tag{1}$$

where $\text{Im}(g)$ is the image of function g.

Moving to the definition of the intrinsic randomness, one should consider all possible preparations of the observed statistics in terms of no-signaling probability distributions. In our context, a particular preparation reads

$$P_{\text{obs}}(\mathbf{a}|\mathbf{x}) = \sum_e p(e|\mathbf{x}) P_e^{\text{ex}}(\mathbf{a}|\mathbf{x}), \tag{2}$$

where the P_e^{ex} are extremal points of the no-signaling set [14]. The terms $p(e|\mathbf{x})$ may depend on $\mathbf{x}$, which accounts for possible correlations between the preparation e and the measurement settings $\mathbf{x}$, given that the choice of measurements are not assumed to be free. Hence, we define the intrinsic randomness of a function g by optimizing over all possible nonsignaling preparations of P_{obs} so as to minimize the randomness of g. In other words,

$$G_{\text{int}}(g, \mathbf{x}, P_{\text{obs}}) = \max_{\{p(e|\mathbf{x}), P_e^{\text{ex}}\}} \sum_e p(e|\mathbf{x}) G_{\text{obs}}(g, \mathbf{x}, P_e^{\text{ex}}),$$

subject to

$$\sum_e p(e|\mathbf{x}) P_e^{\text{ex}}(\mathbf{a}|\mathbf{x}) = P_{\text{obs}}(\mathbf{a}|\mathbf{x}), \tag{3}$$

$$p(\mathbf{x}|e) \geq \delta \quad \text{with} \quad \delta > 0; \forall \mathbf{x}, e, \tag{4}$$

where $G_{\text{obs}}(g, \mathbf{x}, P_e^{\text{ex}}) = \max_k P_e^{\text{ex}}(g(\mathbf{a}) = k|\mathbf{x})$is also the intrinsic randomness of P_e^{ex}, since intrinsic and observed randomness must coincide for extremal points of the nonsignaling set. Note that the condition $p(\mathbf{x}|e) \geq \delta > 0$ allows for an arbitrary (but not absolute) relaxation of the freedom of choice assumption by allowing for arbitrary (yet not complete) correlations between the preparation and the measurement settings. Physically, this condition ensures that all measurement combinations appear for all possible preparations e (See [15] for the significance of this condition). An example of a source of randomness fulfilling this condition is a source of partially random bits, in which the bits can be partially predicted. This source is known in classical computer science as a Santha-Vazirani source [16]. Note, however, that our definition allows sources more general than Santha-Vazirani sources.

From a cryptographic point of view, the observed randomness is the one perceived by the parties performing the Bell test, whereas the intrinsic randomness is that perceived by a nonsignaling eavesdropper possessing knowledge of the preparation of the observed correlations and with the ability to arbitrarily (yet not fully) bias the choice of the measurement settings.

In general, G_{obs} is strictly larger than G_{int}, as the set of nonsignaling correlations is larger than the quantum. When expressed in terms of these quantities, the results in [17,18] provide a Bell test in which G_{int} approaches G_{obs} (and to $1/2$) in the limit of an infinite number of measurements and assuming free choices, that is, $p(\mathbf{x}|e)$ in (2) is independent of e. The results in [12] allow some relaxation of this last condition. The results in [13] arbitrarily relaxed the free-choice condition and give a Bell test in which G_{int} tends to G_{obs} (and both tend to $1/2$) in the limit of an infinite number of parties. Here, we provide a significantly stronger

proof, as we allow the same level of relaxation on free choices and provide Bell tests in which $G_{\text{int}} = G_{\text{obs}}$ for any number of parties. Moreover, a perfect random bit is obtained in the limit of an infinite number of parties.

Scenario.—Our scenario consists of N parties where each performs two measurements of two outcomes. In what follows, we adopt a spinlike notation and label the outputs by ± 1. Then, any nonsignaling probability distribution can be written as (for simplicity, we give the expression for three parties, but it easily generalizes to an arbitrary number)

$$\begin{aligned} P(a_1,a_2,a_3|x_1,x_2,x_3) = \frac{1}{8}(1 &+ a_1\langle A_1^{(x_1)}\rangle + a_2\langle A_2^{(x_2)}\rangle \\ &+ a_3\langle A_3^{(x_3)}\rangle + a_1a_2\langle A_1^{(x_1)}A_2^{(x_2)}\rangle \\ &+ a_1a_3\langle A_1^{(x_1)}A_3^{(x_3)}\rangle \\ &+ a_2a_3\langle A_2^{(x_2)}A_3^{(x_3)}\rangle \\ &+ a_1a_2a_3\langle A_1^{(x_1)}A_2^{(x_2)}A_3^{(x_3)}\rangle), \end{aligned} \tag{5}$$

where $A_i^{(x_i)}$ denotes the outputs of measurement x_i by each party i.

In this scenario, we will test a specific family of Bell inequalities introduced by Mermin [19] and, hence, known as Mermin inequalities. These inequalities can be described in a recursive way through the description of the function related to that inequality. The Mermin function reads

$$M_N = \frac{1}{2}M_{N-1}(A_N^{(0)} + A_N^{(1)}) + \frac{1}{2}M'_{N-1}(A_N^{(0)} - A_N^{(1)}), \tag{6}$$

where $M_1 = A_1^{(0)}$ and the function M'_{N-1} is that obtained from M_{N-1} after swapping $A_i^{(0)} \leftrightarrow A_i^{(1)}$. It can be seen that the function M_N consists of the sum, up to some signs, of 2^N (2^{N-1}) products of local observables for even (odd) N. Local models are such that $M_N \leq 1$. The maximal nonsignaling violation of the inequality is equal to 2^N (2^{N-1}) for even (odd) N, that is, all the products of observables appearing in the inequality are equal to ± 1. We study probability distributions that give this maximal violation and focus our analysis on a function f that maps the N measurement results into one bit as follows

$$f(\mathbf{a}) = \begin{cases} +1 & n_-(\mathbf{a}) = (4j+2); \quad \text{with } j \in \{0,1,2,\ldots\} \\ -1 & \text{otherwise} \end{cases}, \tag{7}$$

where $n_-(\mathbf{a})$ denotes the number of results in $\mathbf{a}$ that are equal to -1.

Results.—Our goal in what follows is to quantify the intrinsic randomness of the bit defined by $f(\mathbf{a})$ for those distributions maximally violating the Mermin inequality for odd N. We first prove the following

Lemma 1.— Let $P_{\text{M}}(\mathbf{a}|\mathbf{x})$ be an N-partite (odd N) nonsignaling probability distribution maximally violating the corresponding Mermin inequality. Then, for the input $\mathbf{x_m} = (0,\ldots,0,1)$ appearing in the inequality,

$$P_{\text{M}}(f(\mathbf{a}) = h_N|\mathbf{x_m}) \geq 1/2, \quad \text{with} \quad h_N = \sqrt{2}\cos\left(\frac{\pi(N+4)}{4}\right). \tag{8}$$

Note that, as N is odd, $h_N = \pm 1$. Operationally, the Lemma implies that, for all points maximally violating the Mermin inequality, the bit defined by f is biased towards the same value h_N. Since the proof of the Lemma for arbitrary odd N is convoluted, we give the explicit proof for $N = 3$ here, which already conveys the main ingredients of the general proof, and relegate the generalization to the Supplemental Material [20].

Proof for three parties.—With some abuse of notation, the tripartite Mermin inequality may be expressed as

$$M_3 = \langle 001\rangle + \langle 010\rangle + \langle 100\rangle - \langle 111\rangle \leq 2, \tag{9}$$

where $\langle x_1x_2x_3\rangle = \langle A_1^{(x1)}A_2^{(x2)}A_3^{(x3)}\rangle$ and similarly for the other terms. The maximal nonsignaling violation assigns $M_3 = 4$ which can only occur when the first three correlators in (9) take their maximum value of $+1$ and the last takes its minimum of -1.

Let us take the corresponding input combination appearing in the inequality (9), $\mathbf{x_m} = (0,0,1)$. Maximal violation of M_3 imposes the following conditions: (i) $\langle 001\rangle = 1$. This further implies $\langle 0\rangle_1 = \langle 01\rangle_{23}$, $\langle 0\rangle_2 = \langle 01\rangle_{13}$, and $\langle 1\rangle_3 = \langle 00\rangle_{12}$. (ii) $\langle 010\rangle = 1$ implying $\langle 0\rangle_1 = \langle 10\rangle_{23}$, $\langle 1\rangle_2 = \langle 00\rangle_{13}$, and $\langle 0\rangle_3 = \langle 01\rangle_{12}$. (iii) $\langle 100\rangle = 1$ implying $\langle 1\rangle_1 = \langle 00\rangle_{23}$, $\langle 0\rangle_2 = \langle 10\rangle_{13}$, and $\langle 0\rangle_3 = \langle 10\rangle_{12}$. (iv) $\langle 111\rangle = -1$ implying $\langle 1\rangle_1 = -\langle 11\rangle_{23}$, $\langle 1\rangle_2 = -\langle 11\rangle_{13}$, and $\langle 1\rangle_3 = -\langle 11\rangle_{12}$.

Imposing these relations on (5) for input $\mathbf{x_m} = (0,0,1)$ one gets

$$\begin{aligned} P_{\text{M}}(a_1,a_2,a_3|0,0,1) &= \frac{1}{8}(1 + a_1a_2a_3 + (a_1 + a_2a_3)\langle 0\rangle_1 \\ &\quad + (a_2 + a_1a_3)\langle 0\rangle_2 + (a_3 + a_1a_2)\langle 1\rangle_3). \end{aligned} \tag{10}$$

Using all these constraints and the definition of the function (7), Eq. (8) can be expressed as

$$\begin{aligned} P_M(f(\mathbf{a}) = +1|\mathbf{x_m}) &= P_{\text{M}}(1,-1,-1|\mathbf{x_m}) \\ &\quad + P_{\text{M}}(-1,1,-1|\mathbf{x_m}) \\ &\quad + P_{\text{M}}(-1,-1,1|\mathbf{x_m}) \\ &= \frac{1}{4}(3 - \langle 0\rangle_1 - \langle 0\rangle_2 - \langle 1\rangle_3). \end{aligned} \tag{11}$$

Proving that $P(f(\mathbf{a})=+1|\mathbf{x_m})\geq 1/2$ then amounts to showing that $\langle 0\rangle_1+\langle 0\rangle_2+\langle 1\rangle_3\leq 1$. This form is very convenient since it reminds one of a positivity condition of probabilities.

We, then, consider the input combination $\bar{\mathbf{x}}_\mathbf{m}$ such that all the bits in $\bar{\mathbf{x}}_\mathbf{m}$ are different from those in $\mathbf{x_m}$. We call this the swapped input, which, in the previous case, is $\bar{\mathbf{x}}_\mathbf{m}=(1,1,0)$. Note that this is not an input appearing in the Mermin inequality. However, using the previous constraints derived for distributions P_M maximally violating the inequality, one has

$$\begin{aligned}P_\mathrm{M}(a_1,a_2,a_3|1,1,0)=&\frac{1}{8}(1+a_1\langle 1\rangle_1+a_2\langle 1\rangle_2+a_3\langle 0\rangle_3\\&+a_1a_2\langle 11\rangle_{12}+a_1a_3\langle 10\rangle_{13}\\&+a_2a_3\langle 10\rangle_{23}+a_1a_2a_3\langle 110\rangle_{123})\\=&\frac{1}{8}(1+a_1\langle 1\rangle_1+a_2\langle 1\rangle_2+a_3\langle 0\rangle_3\\&-a_1a_2\langle 1\rangle_3+a_1a_3\langle 0\rangle_2\\&+a_2a_3\langle 0\rangle_1+a_1a_2a_3\langle 110\rangle_{123}),\end{aligned}\tag{12}$$

where the second equality results from the relations $\langle 11\rangle_{12}=-\langle 1\rangle_3$, $\langle 10\rangle_{13}=\langle 0\rangle_2$, and $\langle 10\rangle_{23}=\langle 0\rangle_1$.

It can be easily verified that summing the two positivity conditions $P_\mathrm{M}(1,1,-1|\bar{\mathbf{x}}_\mathbf{m})\geq 0$ and $P_\mathrm{M}(-1,-1,1|\bar{\mathbf{x}}_\mathbf{m})\geq 0$ gives the result we seek, namely $1-\langle 0\rangle_1-\langle 0\rangle_2-\langle 1\rangle_3\geq 0$, which completes the proof. ∎

Using the previous Lemma, it is rather easy to prove the following

Theorem 1.— Let $P_\mathrm{obs}(\mathbf{a}|\mathbf{x})$ be an N-partite (odd N) nonsignaling probability distribution maximally violating the corresponding Mermin inequality. Then the intrinsic and the observed randomness of the function f are equal for the input $\mathbf{x_m}$ appearing in the Mermin inequality

$$G_\mathrm{int}(f,\mathbf{x_m},P_\mathrm{obs})=G_\mathrm{obs}(f,\mathbf{x_m},P_\mathrm{obs}),$$

where

$$G_\mathrm{obs}(f,\mathbf{x_m},P_\mathrm{obs})=\max_{k\in\{+1,-1\}}P_\mathrm{obs}(f(\mathbf{a})=k|\mathbf{x_m}).$$

Proof of Theorem 1.—Since P_obs maximally and algebraically violates the Mermin inequality, all the extremal distributions P_e^ex appearing in its decomposition must also necessarily lead to the maximal violation of the Mermin inequality (see Supplemental Material [20] for details). Hence, the randomness of f in these distributions as well satisfies Eq. (8) of Lemma 1. Using this, we find

$$\begin{aligned}G_\mathrm{obs}(f,\mathbf{x_m},P_e^\mathrm{ex})&=\max_{k\in\{+1,-1\}}P_e^\mathrm{ex}(f(\mathbf{a})=k|\mathbf{x_m})\\&=|P_e^\mathrm{ex}(f(\mathbf{a})=h_N|\mathbf{x_m})-1/2|+1/2\\&=P_e^\mathrm{ex}(f(\mathbf{a})=h_N|\mathbf{x_m}),\end{aligned}\tag{13}$$

for every e. Therefore,

$$\begin{aligned}&G_\mathrm{int}(f,\mathbf{x_m},P_\mathrm{obs})\\&\quad=\max_{\{p(e|\mathbf{x_m}),P_e^\mathrm{ex}\}}\sum_e p(e|\mathbf{x_m})G_\mathrm{obs}(f,\mathbf{x_m},P_e^\mathrm{ex})\\&\quad=\max_{\{p(e|\mathbf{x_m}),P_e^\mathrm{ex}\}}\sum_e p(e|\mathbf{x_m})P_e^\mathrm{ex}(f(\mathbf{a})=h_N|\mathbf{x_m})\\&\quad=P_\mathrm{obs}(f(\mathbf{a})=h_N|\mathbf{x_m}).\end{aligned}\tag{14}$$

Likewise, the last equality follows from the constraint $\sum_e p(e|\mathbf{x})P_e(\mathbf{a}|\mathbf{x})=P_\mathrm{obs}(\mathbf{a}|\mathbf{x})$. On the other hand, the observed randomness for f is, $G_\mathrm{obs}(f,\mathbf{x_m},P_\mathrm{obs})=P_\mathrm{obs}(f(\mathbf{a})=h_N|\mathbf{x_m})$. ∎

The previous technical results are valid for any nonsignaling distribution maximally violating the Mermin inequality. For odd N, this maximal violation can be attained by a unique quantum distribution, denoted by $P_\mathrm{GHZ}(\mathbf{a}|\mathbf{x})$, resulting from measurements on a Greenberger-Horne-Zeilinger (GHZ) state. When applying Theorem 1 to this distribution, one gets

Main result.—Let $P_\mathrm{GHZ}(\mathbf{a}|\mathbf{x})$ be the N-partite (odd N) quantum probability distribution attaining the maximal violation of the Mermin inequality. The intrinsic and observed randomness of f for the Mermin input $\mathbf{x_m}$ satisfy

$$G_\mathrm{int/obs}(f,\mathbf{x_m},P_\mathrm{GHZ})=\frac{1}{2}+\frac{1}{2^{(N+1)/2}}.\tag{15}$$

This follows straightforwardly from Theorem 1, since $P_\mathrm{GHZ}(\mathbf{a}|\mathbf{x})=1/2^{N-1}$ for outcomes $\mathbf{a}$ with an even number of results equal to -1 and for those measurements appearing in the Mermin inequality.

It is important to remark that $f(\mathbf{a}|\mathbf{x_m})$ approaches a perfect random bit exponentially with the number of parties. In fact, this bit defines a process in which full randomness amplification takes place. Yet, it is not a complete protocol as, contrary to the existing proposal in [13], no estimation part is provided.

Discussion.—We have identified the first family of quantum processes whose observed randomness can be proven to be fully intrinsic. In other words, for the considered processes, quantum theory gives predictions as accurate as any no-signaling theory, possibly supra-quantum, can give and, hence, admit no further completion. Our results hold under the minimal assumptions: the validity of the no-signaling principle and an arbitrary (but not complete) relaxation of the freedom of choice.

The latter is subtle, and much attention in recent years has focused on relaxing it in Bell experiments [7–11].

Our work raises several questions. Our main motivation here has been to understand the ultimate limits on the completeness of quantum theory for finite tests, and thus, we have worked in a noiseless regime. It is interesting to consider how our results would have to be modified to encompass scenarios including noise and, hence, be amenable to experiments. The presence of noise modifies our results from two different viewpoints.

First, noise is due to lack of control of the setup and, thus, a source of apparent randomness, which immediately implies a gap between intrinsic and observed randomness. Second, in a noisy situation, it is impossible to arbitrarily relax the freedom of choice assumption, quantified by δ in Eq. (4). In fact, there is a tradeoff between the amount of relaxation of this condition and the violation needed to certify the presence of any intrinsic randomness. The reason is that, for a sufficiently small value of δ, any correlations not attaining the maximal nonsignaling violation of a Bell inequality can be reproduced using purely deterministic local strategies. It seems natural, in a practical context, to extend the definition of intrinsic randomness by considering bounded relaxations of the freedom of choice assumption and nonmaximal violations of Bell inequalities. These investigations could lead to stronger experimental tests on the completeness of quantum predictions, given that they would rely on significantly more relaxed assumptions than any other quantum experiment performed to date.

From a purely theoretical perspective, our results certify a maximum of one bit of randomness for any system size. It would be interesting to extend these analytical results to certify randomness that scales with the number of parties. This could, for instance, be accomplished with functions of increasing outcomes. In a related context, it would also be interesting to explore whether similar results are possible in a bipartite scenario or, on the contrary, whether an asymptotic number of parties is necessary for full randomness amplification.

We acknowledge support from the ERC Starting Grant PERCENT, the EU Projects Q-Essence and QCS, the Spanish MICIIN through a Juan de la Cierva Grant and the Spanish FPI Grant (No. FIS2010-14830), an FI Grant of the Generalitat de Catalunya and Projects No. FIS2010-14830, Explora-Intrinqra, and CHIST-ERA DIQIP. C. D. and G. d. l. T. contributed equally to this work.

*Present address: Max-Planck-Institute for Biogeochemistry, Hans-Knöll-Str. 10, 07745 Jena, Germany.

[1] J. Bell Physics **1**, 195 (1964).
[2] A. Fine, Phys. Rev. Lett. **48**, 291 (1982).
[3] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[4] N. Bohr, Phys. Rev. **48**, 696 (1935).
[5] E. G. Cavalcanti and H. M. Wiseman, Found. Phys. **42**, 1329 (2012).
[6] R. Colbeck and R. Renner, Nat. Commun. **2**, 411 (2011).
[7] J. Kofler, T. Paterek, and C. Brukner, Phys. Rev. A **73**, 022104 (2006).
[8] M. J. W. Hall, Phys. Rev. A **84**, 022102 (2011).
[9] M. J. W. Hall, Phys. Rev. Lett. **105**, 250404 (2010).
[10] J. Barrett and N. Gisin, Phys. Rev. Lett. **106**, 100406 (2011).
[11] D. E. Koh, M. J. W. Hall, Setiawan, J. E. Pope, C. Marletto, A. Kay, V. Scarani, and A. Ekert, Phys. Rev. Lett. **109**, 160404 (2012).
[12] R. Colbeck and R. Renner, Nat. Phys. **8**, 450 (2012).
[13] R. Gallego, L. Masanes, G. de la Torre, C. Dhara, L. Aolita, and A. Acín, Nat. Commun. **4**, 2654 (2013).
[14] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).
[15] L. P. Thinh, L. Sheridan, and V. Scarani, arXiv:1304.3598.
[16] M. Santha and U. V. Vazirani, J. Comput. Syst. Sci. **33**, 75 (1986).
[17] J. Barrett, A. Kent, and S. Pironio, Phys. Rev. Lett. **97** 170409 (2006).
[18] R. Colbeck and R. Renner, arXiv:1208.4123.
[19] D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
[20] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.112.100402 for the general proof of Lemma 1.