Einstein-Podolsky-Rosen steering inequalities from entropic uncertainty relations

James Schneeloch,[1] Curtis J. Broadbent,[1,2] Stephen P. Walborn,[3] Eric G. Cavalcanti,[4,5] and John C. Howell[1]
[1]*Department of Physics and Astronomy, University of Rochester, Rochester, New York 14627, USA*
[2]*Rochester Theory Center, University of Rochester, Rochester, New York 14627, USA*
[3]*Instituto de Física, Universidade Federal do Rio de Janeiro, Caixa Postal 68528, Rio de Janeiro, RJ 21941-972, Brazil*
[4]*School of Physics, University of Sydney, NSW 2006, Australia*
[5]*Quantum Group, Department of Computer Science, University of Oxford, Oxford OX1 3QD, United Kingdom*
(Received 29 March 2013; published 6 June 2013)

We use entropic uncertainty relations to formulate inequalities that witness Einstein-Podolsky-Rosen (EPR)-steering correlations in diverse quantum systems. We then use these inequalities to formulate symmetric EPR-steering inequalities using the mutual information. We explore the differing natures of the correlations captured by one-way and symmetric steering inequalities and examine the possibility of exclusive one-way steerability in two-qubit states. Furthermore, we show that steering inequalities can be extended to generalized positive operator-valued measures, and we also derive hybrid steering inequalities between alternate degrees of freedom.

DOI: 10.1103/PhysRevA.87.062103 PACS number(s): 03.65.Ud, 03.67.Mn, 03.67.Bg

I. INTRODUCTION

The ability to witness explicitly quantum correlations (i.e., entanglement) between arbitrary observables without having to characterize the density operator is extremely useful and has received much attention [1–11]. Entropic witnesses of entanglement, formed from the building blocks of information theory, may play an important role in the development and implementation of superior quantum information protocols such as quantum key distribution (QKD) [12]. For certain tasks, such as verifying security in QKD with as few assumptions as possible, it is not sufficient just to demonstrate entanglement [13]. Fortunately, there are witnesses that detect stronger levels of quantum correlation (e.g., Bell nonlocality) in exchange for observing entanglement in fewer states. Between Bell nonlocality [14] and mere nonseparability [15], there is another category of nonlocality known as Einstein-Podolsky-Rosen (EPR) steering [4] corresponding to a level of quantum correlation strong enough to demonstrate the EPR paradox [16] but not strong enough to rule out all models of local hidden variables (LHVs).

In this article, we develop EPR-steering inequalities for any set of observables that share a nontrivial entropic uncertainty relation. We use those inequalities relating discrete observables to create symmetric steering inequalities based on the mutual information [17]; we examine the qualitative differences in states violating one-way vs symmetric steering inequalities; we derive steering inequalities between disparate degrees of freedom useful in studying hybrid-entangled states [18–20]; and we explore applications of these steering inequalities beyond their direct use as entanglement witnesses.

II. FOUNDATIONS AND MOTIVATION

EPR steering is the ability to nonlocally influence the set of possible quantum states of a given quantum system through the measurements on a second distant system sufficiently entangled with the first one. By choosing which observable to measure of the second system, one can "steer" the first system to be well defined in any of its observables without directly interacting with it. However, one cannot know or determine in advance what the outcome of a measurement will be, as these outcomes are intrinsically random. It is only when measurement outcomes between systems are compared that we are able to see the effect of measuring one system on the other. It is this nonlocal influence that is embodied in EPR steering. It is this randomness in measurement outcomes that reinforces the no-signaling theorem [21] (i.e., that rules out EPR steering as a possible means of faster-than-light communication).

Strong correlations across conjugate observables (e.g., in both position and momentum) are a signature of entanglement, and it is these correlations that make EPR steering possible. In the original EPR situation [16], if we assume that the effect of measurement cannot travel faster than light, then any details of the observables of system B obtained from measurements on system A must be embedded in the local state of B, independent of any measurement performed on A. Following EPR, we ascribe inferred "elements of reality" to each of these inferred properties of B. The "paradox" arises when A and B are so entangled that the inferred elements of reality of, say, position and momentum, of B are so well localized that they begin to violate uncertainty relations for single systems. If the inferred elements of reality of B violate an uncertainty relation, then there cannot be a local quantum state for B that reproduces such measurement results. If the inferred elements of reality of B rule out a local quantum state for B, then this implies that it cannot be the case both that quantum correlations are local and that conjugate observables of a given system always satisfy an uncertainty relation (as quantum theory stipulates). Unwilling to discard locality, EPR concluded that quantum mechanics must give an incomplete description of B.

Schrödinger [22] was the first to use the term "steering" in response to the original EPR paradox [16] as a generalization beyond position and momentum. It was not until recently, however, that Wiseman *et al.* [4] formalized EPR steering in terms of the violation of a *local hidden state* (LHS) model, a general class of models where, say, system B has a local quantum state classically correlated with arbitrary variables at A. An entangled pair of systems is said to be one-way or exclusively one-way steerable if only one subsystem does not admit an LHS model. If neither subsystem admits an LHS model, the entangled pair is said to be two-way or symmetrically steerable. If B has a local quantum state classically correlated with A, then the measurement probabilities of system B must not violate any single-system uncertainty relation, even when they are conditioned on the outcomes of A (or on anything else). Because of this, EPR steering is observed whenever conditional measurement probabilities violate an uncertainty relation. EPR steering requires entanglement because probability distributions in separable states can always be represented by an LHS model.

Though the concept of EPR steering was first formalized by Wiseman *et al.* [4], Reid [7] was the first to develop an experimental criterion for the EPR paradox using conditional variances and the Heisenberg uncertainty relation. A general theory of EPR-steering inequalities based on the assumption of an LHS model was developed in [9], where Reid's criterion was shown to emerge as a special case. Later, Walborn *et al.* [1] formulated a steering inequality based on Bialynicki-Birula and Mycielski's entropic position-momentum uncertainty relation [23]. Since their entropic uncertainty relation implies Heisenberg's uncertainty relation, the set of states violating Walborn *et al.*'s steering inequality contains all the states violating Reid's inequality, making Walborn *et al.*'s steering inequality more inclusive. The same is not true in the discrete case, as we show later.

An interesting open question regarding EPR steering was raised by Wiseman *et al.* [4]: Are there states which allow steering in only one direction (say, from Alice to Bob), and not vice versa? Some evidence that this may be the case was given for continuous-variable systems by Midgley *et al.* [24], who showed, at least in the case where Alice and Bob are restricted to Gaussian measurements, that there are states that demonstrate steering in one direction only. Though a proof of the existence of exclusively one-way steerable states is beyond the scope of this paper, in Sec. VI, we do extend the results of Midgley *et al.*, i.e., we show that at least in the case considering mutually unbiased measurements, there are states which can demonstrate steering using our inequalities in one way, but not in the other.

III. LOCAL HIDDEN STATE MODELS

In order to develop our new entropic steering inequalities for pairs of arbitrary observables, we use the work of Walborn *et al.* [1], which considered the case for continuous observables as follows. Let $\hat{x}^A$ and $\hat{k}^A$ be continuous observables of system A with possible outcomes $\{x^A\}$ and $\{k^A\}$, and let $\hat{x}^B$ and $\hat{k}^B$ be the corresponding observables of system B. According to its definition in [4], EPR steering occurs when the observed correlations do not admit an LHS model. The system is said to admit an LHS model if and only if the joint measurement probability density can be expressed as

$$\rho(x^A,x^B) = \int d\lambda\ \rho(\lambda)\rho(x^A|\lambda)\rho_Q(x^B|\lambda), \qquad (1)$$

where $\rho_Q(x^B|\lambda)$ is the probability density of measuring $\hat{x}^B$ to be x^B given the details of preparation in the hidden variable λ. The subscript Q denotes the fact that this is a probability density arising from a single quantum state, i.e., that it is a probability density arising from quantum system B whose details of preparation are governed only by the hidden variable λ. On the other hand, no assumptions have been made about the origin of A's probability distribution. In contrast to the similar constraint for LHV models discussed in [9], the quantum probability density we write for one set of measurements (say, position) must be compatible with the quantum probability density one assigns to measurements of momentum. Not all LHV models will satisfy this constraint, which is why states that violate an LHV criterion are a proper subset of states which violate an LHS criterion, (1) (and, in turn, a proper subset of all entangled states).

Using the positivity of the continuous relative entropy [17] between any pair of probability distributions or densities, Walborn *et al.* showed that it is always the case for continuous observables in states admitting LHS models that (since the relative entropy between $\rho(x^B,\lambda|x^A)$ and $\rho(\lambda|x^A)\rho(x^B|x^A)$ is always $\geqslant 0$)

$$h(x^B|x^A) \geqslant \int d\lambda\ \rho(\lambda)h_Q(x^B|\lambda), \qquad (2)$$

where $h_Q(x^B|\lambda)$ is the continuous Shannon entropy arising from the probability density $\rho_Q(x^B|\lambda)$.

In developing our steering inequalities for arbitrary observables, we note that the same arguments used to develop LHS constraints for continuous observables can be used to formulate LHS constraints for discrete observables as well. Consider discrete observables $\hat{R}^A$ and $\hat{S}^A$ with outcomes $\{R_i^A\}$ and $\{S_i^A\}$, respectively, and where i runs from 1 to the total number of distinct eigenstates N. Let $\hat{R}^B$ and $\hat{S}^B$ be the corresponding observables for system B. Since the positivity of the relative entropy is a fact [17] for both continuous and discrete variables, we can derive the corresponding LHS constraint for discrete observables in the same way:

$$H(R^B|R^A) \geqslant \sum_{\lambda} P(\lambda)H_Q(R^B|\lambda), \qquad (3)$$

where $H_Q(R^B|\lambda)$ is the discrete Shannon entropy of the probability distribution $P_Q(R^B|\lambda)$, where, again, the subscript Q means that it corresponds to a quantum state. All observables of systems admitting LHS models must obey inequality (3) for discrete observables or (2) for continuous observables.

IV. ENTROPIC STEERING INEQUALITIES

Consider the right-hand side of inequality (2). Where position $\hat{x}$ and wave number $\hat{k}$ are continuous observables constrained by the entropic uncertainty relation [23]

$$h_Q(x^B) + h_Q(k^B) \geqslant \log(\pi e), \qquad (4)$$

we readily see that if we take a weighted average of these entropies with weight function $\rho(\lambda)$, we get the right-hand side of (2). Note that here and throughout the paper the base of all logarithms is assumed to be 2, so that entropy is measured in bits. From there, it is straightforward to show (as Walborn *et al.* did) that any state admitting an LHS model in position and momentum must satisfy the inequality

$$h(x^B|x^A) + h(k^B|k^A) \geqslant \log(\pi e). \qquad (5)$$

Indeed, for any pair of continuous observables with an entropic uncertainty relation resembling (4), there is always the corresponding steering inequality (5).

As explained in Ref. [25], given any pair of discrete observables $\hat{R}$ and $\hat{S}$ in the same N-dimensional Hilbert space, with eigenbases $\{|R_i\rangle\}$ and $\{|S_j\rangle\}$, respectively (such as for different components of the angular momentum), there exists the entropic uncertainty relation

$$H_Q(R) + H_Q(S) \geqslant \log(\Omega) \tag{6}$$

$$: \ \Omega \equiv \min_{i,j}\left(\frac{1}{|\langle R_i|S_j\rangle|^2}\right). \tag{7}$$

When the discrete observables $\hat{R}$ and $\hat{S}$ are maximally uncertain with respect to one another, all measurement outcomes of one observable are equally likely when the system is prepared in an eigenstate of the other observable. These maximally uncertain observables (termed mutually unbiased) have an uncertainty relation where Ω obtains its maximum value given by the dimension N of the Hilbert space. The uncertainty relation is saturated when the system is prepared in an eigenstate of one of the unbiased observables.

Using the discrete entropic uncertainty relation, (6), along with our LHS constraint for discrete observables, (3), we immediately arrive at a new entropic steering inequality for pairs of discrete observables,

$$H(R^B|R^A) + H(S^B|S^A) \geqslant \log(\Omega^B), \tag{8}$$

where Ω^B is the value Ω, given in definition (7) associated with the observables $\hat{R^B}$ and $\hat{S^B}$.

For quantum systems in which conjugate bases are discrete and continuous, such as with angular position and angular momentum, the entropic uncertainty relation will have a sum of both discrete and continuous entropies. This does not give rise to any complications because the LHS constraints deal with only one measured observable at a time. Given a continuous observable $\hat{x}$ and a discrete observable $\hat{R}$ with uncertainty relation [26]

$$h_Q(x) + H_Q(R) \geqslant C, \tag{9}$$

where C is a real-valued placeholder dependent on the particular uncertainty relation, we readily find a new steering inequality between a discrete and a continuous observable:

$$h(x^B|x^A) + H(R^B|R^A) \geqslant C. \tag{10}$$

In fact, an EPR-steering inequality of this type has recently been experimentally tested for discrete and continuous components of position and momentum variables of entangled photons [27,28].

V. SYMMETRIC STEERING INEQUALITIES

Up until now, all the EPR-steering inequalities discussed here have been asymmetric between parties; they rely on conditional probability distributions, and their violation rules out LHS models from describing only one of the parties' measurements. Violating a more restrictive EPR steering inequality that is symmetric between parties would allow one to rule out LHS models for both parties at the same time.

Cavalcanti *et al.* [9] were the first to develop such a symmetric steering inequality by showing that the variance of sums and differences always exceeds the largest of the conditional variances in Reid's inequality [7]. For position and momentum, the sum or difference steering inequality takes the form

$$\sigma^2(x^A \pm x^B)\sigma^2(k^A \mp k^B) \geqslant \tfrac{1}{4}, \tag{11}$$

which is just Mancini *et al.*'s separability inequality [29] with the tighter bound of $\frac{1}{4}$ instead of 1.

It turns out that we can also create an entropic steering inequality using sums and differences for the same reason that we now show. The entropy of a sum or difference of two random variables is never less than the larger of the two conditional entropies:

$$\begin{aligned} h(x^A \pm x^B) &\geqslant \max\{h(x^A \pm x^B|x^A), h(x^A \pm x^B|x^B)\} \\ &= \max\{h(x^A|x^B), h(x^B|x^A)\}. \end{aligned} \tag{12}$$

This is true for both discrete and continuous random variables, which allows us to assert that both

$$h(x^A \pm x^B) + h(k^A \mp k^B) \geqslant \log(\pi e) \tag{13}$$

and

$$H(R^A \pm R^B) + H(S^A \mp S^B) \geqslant \log(\Omega) \tag{14}$$

are valid steering inequalities coming from (5) and (8), respectively, but are symmetric between parties and witness EPR steering both ways at the same time. We note also that inequality (13) is just Walborn *et al.*'s 2009 separability inequality [2] with the tighter bound $\log(\pi e)$ instead of $\log(2\pi e)$. Whether the symmetric steering inequality (14) is similarly a separability inequality with a tighter bound is the subject of ongoing investigation.

These new symmetric steering inequalities, (13), have the added benefit of not needing to measure full joint probability distributions, let alone reconstruct density operators to witness that a state is EPR steerable. The functions $x^A \pm x^B$ and $k^A \mp k^B$ as well as their discrete counterparts are commuting observables that can be measured directly in many physical systems, which means that, in those cases where these inequalities can be violated, it takes fewer measurements to witness that a state is EPR steerable.

However, there is a subtle but important point to be noted here. Demonstration of EPR steering through these sum or difference inequalities requires that the observables x^A, x^B, k^A, and k^B be measured individually; violation of these inequalities through a direct measurement of $x^A \pm x^B$ does not, strictly speaking, demonstrate EPR steering (or, equivalently, demonstrate the EPR paradox). This is because: (i) determining which experimental procedure corresponds to $x^A \pm x^B$, etc., requires extra assumptions about the quantum operators corresponding to Alice's measurements which goes beyond the assumption of an LHS model; and (ii) measurements of the sum or difference observables require that systems A and B interact, undermining the assumption of locality. On the other hand, violation of these sum or difference inequalities does imply that the state is EPR steerable in the sense that *if* the individual measurements were performed instead, those statistics would not be describable by an LHS model. This might be useful when the objective of the experiment is to characterize the state rather than a fundamental demonstration of nonlocality.

A useful property of discrete observables and discrete approximations to continuous ones [30] is that the Shannon entropies are bounded above either by the logarithm of the dimensionality of the system N or by the number of discrete windows into which the observable is partitioned. With this upper bound, we can create symmetric EPR steering inequalities using the mutual information.

The mutual information of the joint probability distribution of measurement outcomes of $\hat{R}^A$ and $\hat{R}^B$ is defined as

$$\begin{aligned} I(R^A:R^B) &\equiv H(R^A)+H(R^B)-H(R^A,R^B) \\ &= H(R^B)-H(R^B|R^A). \end{aligned} \tag{15}$$

We can express the steering inequality, (8), in terms of the mutual information and use the maximum possible values of the marginal entropies to arrive at a general symmetric steering inequality:

$$I(R^A:R^B)+I(S^A:S^B)\leqslant \log\left(\frac{N^2}{\min\{\Omega^A,\Omega^B\}}\right). \tag{16}$$

This mutual information inequality yields some important insights. We choose the minimum of $\{\Omega^A,\Omega^B\}$ since we want this symmetric steering inequality to witness steering both ways, i.e., to rule out LHS models for both parties.

Consider the case where $\hat{R}^A$ and $\hat{S}^A$ (and, similarly, $\hat{R}^B$ and $\hat{S}^B$) are mutually unbiased observables. Their uncertainty relation reaches the maximum lower bound, where $\Omega^A = \Omega^B = N$, which makes the bound on the right-hand side of (16) $\log(N)$. This maximal bound is also equal to the largest possible value of the mutual information $I(R^A:R^B)$ or $I(S^A:S^B)$. If $\hat{R}$ and $\hat{S}$ (for either A or B) were somewhere between being mutually unbiased and simultaneously measurable, the mutual information bound would be between $\log(N)$ and $2\log(N)$; at the upper limit, the observables commute.

Though a pair of quantum systems can be classically prepared (i.e., with local operations and classical communication) to be strongly correlated in one variable, quantum entanglement is required to have strong simultaneous correlations in observables which are mutually unbiased, that is, strong enough to violate an EPR-steering inequality. Indeed, if a pair of systems were perfectly correlated in one observable, any correlation in a conjugate observable is sufficient to demonstrate symmetric EPR steering in particular and entanglement in general.

Conditional and symmetric steering inequalities witness different levels of nonlocality. While violating a conditional steering inequality rules out an LHS model for either party A or party B, violating a symmetric steering inequality rules out LHS models for both party A and party B. It is important to know whether these steering inequalities witness entanglement in qualitatively different sets of states or if their violation is merely a signpost of progressively stronger entanglement. To answer this question, we must determine what differences there are in the sets of states that violate each inequality.

Let V_C be the difference between the bound and the sum of conditional entropies in the discrete conditional steering inequality on party B (8) [i.e., the violation of (8) in number of bits], and let V_M be the difference between the sum of mutual informations and the bound in the discrete symmetric steering inequality, (16). Here, V_C and V_M are positive for positive violation and we limit ourselves, for simplicity, to observables where $\Omega^A = \Omega^B \equiv \Omega$. The difference, $V_C - V_M$, is expressed as

$$V_C - V_M = 2\log(N) - [H(R^B)+H(S^B)]. \tag{17}$$

From this we know immediately that the violations are the same, $V_C = V_M$, if and only if the marginal measurement probability distributions are both uniform (e.g., when the density operator is one whose marginal states are maximally mixed).

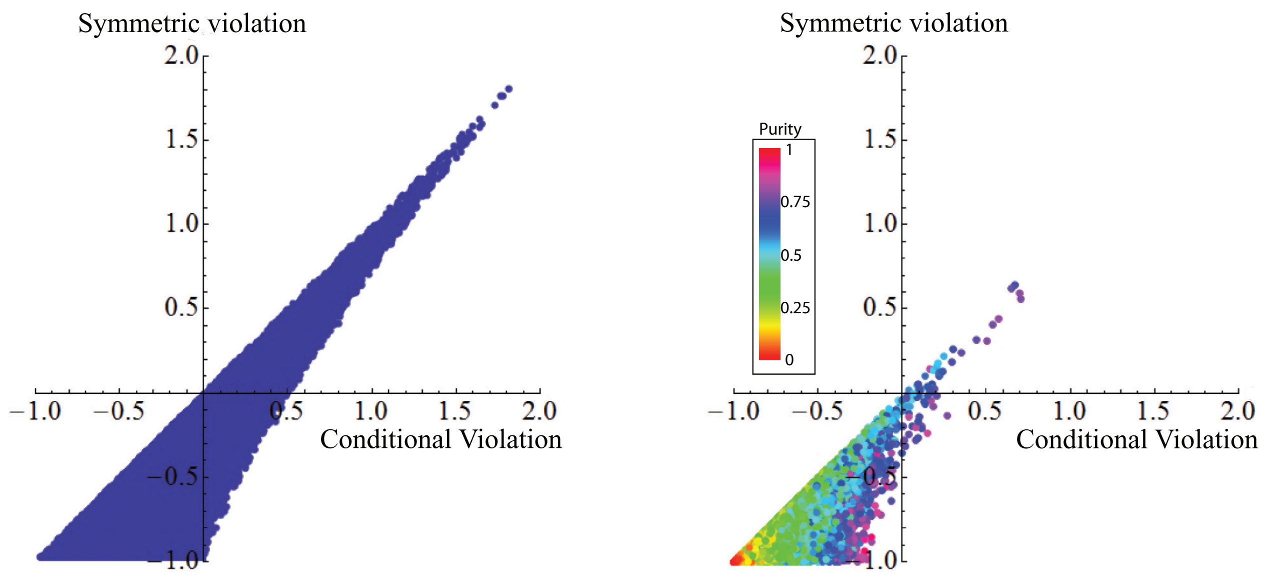
Since the Shannon entropies $H(\hat{R}^B)$ and $H(\hat{S}^B)$ are bounded below by the underlying von Neumann entropy $S(\hat{\rho}^B)$ [31], which in turn is bounded below by the entanglement of formation $E(\hat{\rho})$ [31], we see that the largest possible difference in violations decreases with increasing entanglement:

$$V_C - V_M \leqslant 2[\log(N) - S(\hat{\rho}^B)] \leqslant 2[\log(N) - E(\hat{\rho})]. \tag{18}$$

This agrees with our previous result since maximally entangled states also have maximally mixed marginal probability distributions. Indeed, since the largest possible value for the violations is the same in both inequalities, we expect there to be no difference in violations for maximally entangled states. This is particularly well illustrated in Figs. 1(a) and 1(b), where we have simulated random two-qubit states to compare V_C and V_M for the conditional and symmetric steering inequalities, (21) and (22), using all mutually unbiased observables as discussed in the next section. In order to generate random two-qubit states, we use the methods discussed in Ref. [6].

It is important to note that these inequalities are only *witnesses* for steering. Because violation of these inequalities is a sufficient, but not necessary condition for EPR steering, we can have states that are symmetrically steerable but which fail to violate both kinds of steering inequalities presented here. If a state violates a conditional steering inequality but not a symmetric steering inequality, we know that it is at least one-way steerable, but it may yet violate a different symmetric steering inequality or, indeed, a different one-way steering inequality in the other direction.

One is tempted to think that because all EPR steerable states form a proper subset of all entangled states (and a proper superset of all Bell nonlocal states), there might be some finite nonzero threshold to the entanglement needed in a state to demonstrate EPR steering. In fact, it turns out that at least pure states with very little entanglement can, in principle, demonstrate EPR steering. This was effectively proven [32] by generalizing Gisin's theorem [33] for any pair of discrete quantum systems, which states that any pure bipartite state that is not a product state is Bell nonlocal (and so also EPR steerable), even for very low entropies of entanglement. A proof of Gisin's theorem for continuous variables remains an open topic for investigation.



(a) Scatterplot for pure states

(b) Scatterplot for uniformly-sampled two-qubit states

FIG. 1. (Color online) Scatterplots of the violation of the conditional and symmetric steering inequalities which use all mutually unbiased bases. Each point is a random two-qubit state. The plot in (b) is color coded according to purity, P, as measured by the von Neumann entropy, scaled, and inverted so that 0 is maximally mixed and 1 is pure: $P = 1 - \frac{S(\rho)}{2}$. The well-defined diagonal line through the origin indicates that regardless of the orientation of the mutually unbiased bases, the symmetric violation never exceeds the conditional violation. The plots thin out to the upper right since maximally entangled states are rare when uniformly sampling over pure states and rarer still when uniformly sampling over all states.

VI. EPR STEERING USING ALL UNBIASED OBSERVABLES

Up to this point, the discussion has been limited to uncertainty relations between pairs of observables. We must remember that for any entropic uncertainty relation, even those relating more than two observables, there is a corresponding EPR-steering inequality. Sanchez-Ruiz [34] developed entropic uncertainty relations for complete sets of pairwise complementary (mutually unbiased) observables $\{\hat{R}_i\}$, where $i = \{1,\ldots,N\}$. When N, the dimensionality of the system, is a positive integer power of a prime number, it has been shown [35] that there are complete sets of $N+1$ mutually unbiased observables.

When N is even, we have the uncertainty relation

$$\sum_{i=1}^{N+1} H(R_i) \geqslant \frac{N}{2}\log\left(\frac{N}{2}\right) + \left(\frac{N}{2}+1\right)\log\left(\frac{N}{2}+1\right) \equiv G_{\text{even}}, \tag{19}$$

and for odd N, we have

$$\sum_{i=1}^{N+1} H(R_i) \geqslant (N+1)\log\left(\frac{N+1}{2}\right) \equiv G_{\text{odd}}. \tag{20}$$

Here, G_{even} and G_{odd} are defined as the bounds for these uncertainty relations to condense these expressions later. These uncertainty relations can be adapted into EPR-steering inequalities readily by substituting conditional entropies for marginal ones.

In the same way as done to derive (8), we see that, for N even, we have the EPR steering inequality

$$\sum_{i=1}^{N+1} H\left(R_i^B \middle| R_i^A\right) \geqslant G_{\text{even}}, \tag{21}$$

and in the same way as done to derive (16), we have, for even N,

$$\sum_{i=1}^{N+1} I\left(R_i^A : R_i^B\right) \leqslant (N+1)\log(N) - G_{\text{even}}. \tag{22}$$

For odd N, we have the same expressions (21) and (22) with G_{odd} substituted in for G_{even}.

As a particular example, consider the case of a pair of qubits. $N = 2$, which makes $G_{\text{even}} = 2$. The full symmetric steering inequality for a pair of qubits becomes

$$\sum_{i=1}^{3} I\left(R_i^A : R_i^B\right) \leqslant 1, \tag{23}$$

which not only proves the entanglement witness first postulated by Starling *et al.* [6], but also shows that it is a symmetric steering inequality whose violation demonstrates the EPR paradox.

We note that while similar EPR-steering inequalities exist for measuring the strength of linear correlations [37], they do not register the same information-significant behavior as inequality (22) for the same reason that variances do not capture as much of the necessary information about the uncertainty in a probability distribution as entropies can. Covariance and other measures of correlation are sensitive to specific functional dependence between random variables (particularly linear dependence), while the mutual information captures correlations between random variables whose dependence may be entirely arbitrary but still well-determined.

VII. VIOLATIONS OF STEERING INEQUALITIES BY QUANTUM STATES

For simplicity, we now look for violations of our inequalities in entangled two-qubit states. We first examine the Werner states [15], defined as

$$W_p = p|\Phi_s\rangle\langle\Phi_s| + (1-p)\frac{\mathbb{1}}{4}, \tag{24}$$

where $|\Phi_s\rangle$ is the maximally entangled singlet state, $\mathbb{1}/4$ is the maximally mixed state for two qubits, and p is the weight of the singlet state in W_p. These states were shown in [4] to be steerable in principle (i.e., with an infinite number of measurements) for all values of $p > 1/2$. In practice (i.e., with finite numbers of measurements), this is not achievable. In [9] it was shown that these states violate a linear steering inequality, with two measurement settings at each side for $p > 1/\sqrt{2} \approx 0.71$ and with three measurement settings for $p > 1/\sqrt{3} \approx 0.58$, and violates a variance-based steering inequality for $p > (\sqrt{5}-1)/2 \approx 0.62$ and $p > 1/\sqrt{3} \approx 0.58$, with three and four measurement settings for Bob, respectively (the latter inequality was introduced in [38]).

We first apply the Werner state to our conditional steering inequality, (8), with measurements in the Pauli X and Z bases on each side. The inequality then reads

$$H(\sigma_x^B|\sigma_x^A) + H(\sigma_z^B|\sigma_z^A) \geqslant 1. \tag{25}$$

For the Werner state, the left-hand side of inequality (25) reduces to

$$H(\sigma_x^B|\sigma_x^A) + H(\sigma_z^B|\sigma_z^A) = -\{(1+p)\log[(1+p)/2] + (1-p)\log[(1-p)/2]\} \tag{26}$$

and violation occurs for all values of $p \gtrsim 0.78$. For our three-setting inequality, (21), we use measurements in the X, Y, and Z bases, and thus for $N = 2$, inequality (21) reads

$$H(\sigma_x^B|\sigma_x^A) + H(\sigma_y^B|\sigma_y^A) + H(\sigma_z^B|\sigma_z^A) \geqslant 2. \tag{27}$$

Applied to the Werner state, the left side is now $-3/2\{(1+p)\log[(1+p)/2] + (1-p)\log[(1-p)/2]\}$, and the inequality is violated for all $p \gtrsim 0.65$.

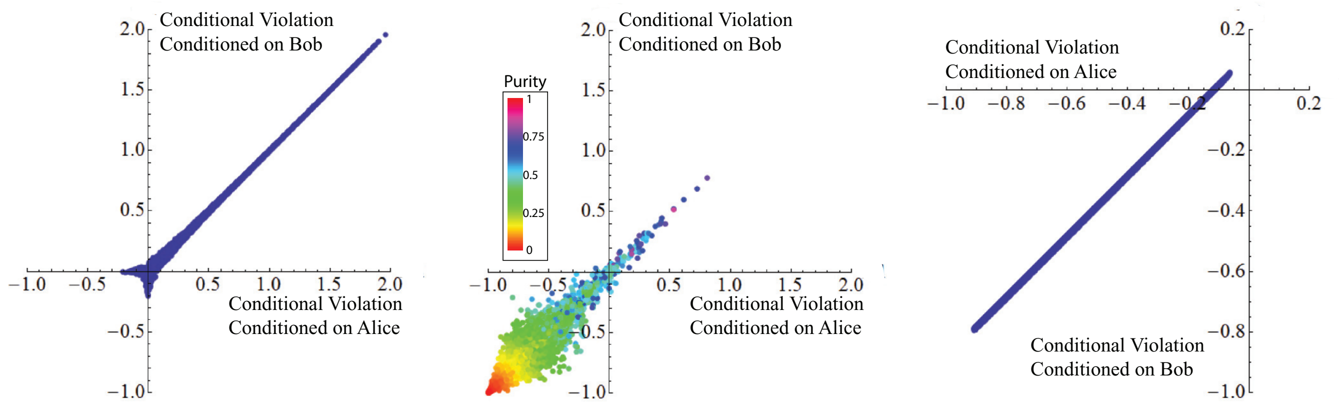
For states with completely mixed marginals, and when $\Omega^B = \Omega^A$, there is no difference between the violation of our symmetric inequality, (16), and the violation of our conditional steering inequality, (8). This is also true for our steering inequalities using complete sets of mutually unbiased bases, (22) and (21). The Werner state thus violates the symmetric inequalities (16) and (22) in the same regimes that it violates the corresponding conditional inequalities, as calculated above. This is not surprising, since the Werner state is symmetric between parties.

It is somewhat surprising, however, that the violations of the entropic steering inequalities presented here occur for a smaller range of Werner states than do the variance-based inequalities in [9]. This is fundamentally different from the result shown for the continuous-variable case by Walborn *et al*. Those authors showed that the entropic steering inequality reproduced here as Eq. (5) detects steering in a larger class of states than the variance-based Reid criterion. In the continuous-variable case, Heisenberg's variance uncertainty relation is implied by Bialynicki-Birula and Mycielski's entropic uncertainty relation (4). Because of this, all states violating Reid's criterion must also violate Walborn *et al*.'s steering inequality. The same is not true for finite discrete variables since the maximum-entropy state with a well-defined variance is no longer a Gaussian, but a uniform distribution. Certainly for two-level discrete systems, there is not much qualitative difference in characterizing the uncertainty with entropies or with variances. For higher dimensions, however, entropic measures of uncertainty are superior because a sharply peaked bimodal distribution is much more well-determined (and so has a much lower entropy) than a single-peaked distribution of the same variance.

While the Werner states violate both symmetric and conditional entropic steering inequalities in the same manner, the same does not happen for all entangled states, as illustrated in Figs. 1(a) and 1(b), which survey the violation of the symmetric inequality, (22), vs the violation of the asymmetric (conditional) inequality, (21), for large distributions of random two-qubit states. Figure 1(a) examines these violations for 10^5 uniformly sampled pure states, while Fig. 1(b) examines these violations for 10^5 uniformly sampled arbitrary states. The sampling method is described in [6]. States in the lower right quadrant violate the conditional inequality but not the symmetric inequality. The well-defined diagonal line in these plots shows that a state never violates the symmetric steering inequality, (22), by a larger amount than the conditional steering inequality, (21), as expected.

To further demonstrate the asymmetry between parties, we surveyed the violation of the conditional inequality, (21), in the Alice-Bob direction versus the violation of the conditional inequality in the Bob-Alice direction [shown in Figs. 2(a) and 2(b)] for a large distribution of states whose set of measurement bases has been chosen to maximize violation in both directions. In Fig. 2(a), each point is one of 5×10^3 pure two-qubit states sampled uniformly, each of which is measured in 500 different sets of measurement bases, chosen randomly and independently by Alice and Bob, to find the one which maximizes violation in both directions. Figure 2(b) samples 5×10^3 general (not necessarily pure) two-qubit states, each one similarly optimized using 500 different sets of measurement bases.

The states in the second and fourth quadrants in Figs. 2(a) and 2(b) violate our entropic conditional steering inequality in only one direction. Note, however, that these results do not imply that there are no other inequalities which could witness steering in the other direction. We know *a priori* that no pure state is exclusively one-way steerable because pure states are fundamentally symmetric between parties. As shown by a Schmidt decomposition, the sets of eigenvalues of the reduced density operators of a pure bipartite state are identical, which means that their marginal statistics must be identical as well in the right set of measurement bases. In particular, for every



(a) Scatterplot for optimal pure states

(b) Scatterplot for optimal uniformly sampled two-qubit states

(c) Scatterplot for local transformations of a candidate state

FIG. 2. (Color online) Scatterplots of the violation in number of bits of the conditional steering inequalities when using an optimal set of mutually unbiased bases. The violation of the inequality conditioned on Alice's measurements is plotted against the violation of the inequality conditioned on Bob's measurements. (a, b): Each point is a random two-qubit state whose set of measurement bases have been selected for maximum violation. For higher violation, the scatterplots approach a diagonal line, where more entangled states tend to be more symmetric between parties. (c): Examination of the violation of a candidate two-qubit state in many different independently random sets of measurement bases. States in the upper left quadrants are ones where Alice's uncertainty is less than Bob's uncertainty. In the lower right quadrants, Bob's uncertainty is less than Alice's. The color coding in (b) is according to purity as defined in Fig. 1(b).

set of measurement bases giving a particular value for the sum of conditional entropies $H(A|B)$, there must exist another set of measurement bases giving the same value for the sum of conditional entropies $H(B|A)$. An optimal choice of local measurement basis requires that if the pure state is steerable one way, it must be steerable the other way as well. Those points in the off-diagonal quadrants in Fig. 2(a) are due to our inequalities being sufficient, but not necessary criteria for EPR steering. What is not clear is whether there are mixed states that may be exclusively one-way steerable.

As shown in Fig. 2(b), we find some mixed states which are candidates for being exclusively one-way steerable, that is, which may allow only one-way steering even when all possible sets of measurement bases are considered. In Fig. 2(c), we plot the violations of one of these mixed states in 10^5 different measurement bases chosen randomly and independently by Alice and Bob to see what effect measurement basis has on an experimenter's ability to violate our steering inequalities. There is a striking linear trend in this plot, which suggests that the difference between violations in either direction is nearly constant, that either Alice's or Bob's advantage in demonstrating EPR steering is nearly independent of her or his choice of measurement basis (and therefore fundamental to the state itself). We examined this trend in more than 300 arbitrary random density matrices, and it is found to a varying degree in all states observed. The same trend is also seen when Alice and Bob's measurement bases are fixed to be equal to one another, though without the extra degree of freedom, finding optimal measurement bases is less likely. The trend is more pronounced for states with higher optimal violation and diminishes in states with lower maximal violation. Though our inequalities cannot demonstrate exclusive one-way steering, our studies suggest that there is a fundamental asymmetry between parties in two-qubit systems whose marginal states have different purities, a property exclusive to mixed states. Again, we must reiterate that since the violation of an EPR steering inequality is a sufficient, but not necessary condition for the state to be EPR steerable, what we do is rule out all but those candidate states from being exclusively one-way steerable.

VIII. STEERING WITH POSITIVE OPERATOR-VALUED MEASURES (POVMs)

Before going farther, we note that Maassen and Uffink's uncertainty relation, (6), relies on $\hat{R}$ and $\hat{S}$ having nondegenerate eigenvalues. Since then, more general entropic uncertainty relations have been discovered [39] which allow $\hat{R}$ and $\hat{S}$ to be any pair of discrete observables (without changing the form of the uncertainty relation). In addition, Krishna and Parasarathy [39] have shown that for any set of generalized measurements, i.e., any POVMs), with measurement operators $\{F_i\}$ and $\{G_j\}$

$$H(F) + H(G) \geqslant \log(\Omega_{\rm POVM}) \tag{28}$$

$$: \ \Omega_{\rm POVM} \equiv \min_{i,j}\left(\frac{1}{\|F_i G_j\|^2}\right) \tag{29}$$

$$: \ \|F\| \equiv \max_{|\psi\rangle}\sqrt{|\langle\psi|F^\dagger F|\psi\rangle|}. \tag{30}$$

This uncertainty relation, (28), allows us to create steering inequalities for POVMs in the same way as done for projective measurements. The LHS constraints are contingent only upon measurement probabilities adhering to entropic uncertainty relations, not on those measurements being projective. If we let $\{F_i^A\}$ and $\{G_j^A\}$ be discrete sets of POVMs on party A, and let $\{F_i^B\}$ and $\{G_j^B\}$ be sets of POVMs obeying entropic uncertainty relation (28), it can be readily shown that

$$H(F^B|F^A) + H(G^B|G^A) \geqslant \log\left(\Omega^B_{\rm POVM}\right) \tag{31}$$

is a valid steering inequality for POVMs, where Ω^B_{POVM} is Ω_{POVM} for measurements on party B. Since we no longer have to restrict ourselves to projective von Neumann measurements, we can study EPR steering when we can only interact indirectly with the system as with weak measurements [40].

IX. HYBRID STEERING INEQUALITIES

Our steering inequalities were formed from pairs or sets of noncommuting observables on a single quantum system conditioned on the corresponding observables of another quantum system. However, the derivation of our steering inequalities does not require the observables on the second system to be the same as those on the first. For example, in the inequality derived by Walborn *et al.,* (5), we require that x^B and k^B be conjugate to one another in accordance with uncertainty relation (4). The observables x^A and k^A need not be the position and momentum of system A, respectively, to have a valid steering inequality; any pair of observables for system A will do. In fact, we can even condition both x^B and k^B on the same observable; this would make a valid steering inequality, though it would be impossible to violate in principle because conditioning on only one observable of system A only changes what would be the local state of system B from which one draws measurement probabilities. In this case, all measurements are made on the same state of system B, which must satisfy uncertainty relation (4).

With this additional freedom in deriving steering inequalities, we can examine entanglement between different degrees of freedom. For example, violation of

$$h(x_B|\sigma_{zA}) + h(k_B|\sigma_{yA}) \geqslant \log(\pi e) \tag{32}$$

or

$$H(\sigma_{zA}|x_B) + H(\sigma_{yA}|k_B) \geqslant 1 \tag{33}$$

demonstrates EPR steering between the position-momentum degree of freedom of one system and the spin-polarization of the other. By using the discrete uncertainty relation for coarse-grained position and momentum [30], we can witness such entanglement in the laboratory. We call these steering inequalities between different degrees of freedom *hybrid*-steering inequalities. Hybrid-steering inequalities may prove useful in the study of hybrid-entangled states, i.e., states which are entangled across different degrees of freedom [20].

X. STEERING AND QKD

In classical information theory [17], the mutual information can be interpreted as the channel capacity of a communication system with source at party A and receiver at party B (and also the other way around), giving our EPR-steering inequalities special utility in quantum information protocols. In particular, security in QKD schemes requires that Alice and Bob are able to prove that the quantum systems transmitted on quantum channels have not been intercepted by Eve.

Recently, it was shown that EPR steering is linked to the secret key rate in one-sided device-independent quantum key distribution (1sDIQKD) [41]. 1sDIQKD lies between conventional QKD and full device-independent QKD [13,42] in that only one of the users trusts his or her measurement device. This connection was shown for asymmetric EPR steering. It is thus an interesting question what link can be made between the symmetric EPR-steering inequalities and the secure transmission rates in a quantum channel.

Intuitively, violating a symmetric EPR-steering inequality rules out the possibility that Eve performs independent (incoherent) attacks on either Alice's or Bob's channel all of the time, since enough of the joint states shared by Alice and Bob must be correlated enough to rule out LHSs for both parties. Thus if Eve is constrained to perform only incoherent attacks on either party, violating a symmetric steering inequality should guarantee a nonzero secret key rate, since some of Alice's and Bob's shared systems would have to have been untouched by Eve, meaning that Eve could not have a perfect LHS model for all of Alice and Bob's systems.

In the more general situation, Eve cannot be limited to incoherent attacks, though it is still possible to formulate secret key rates in terms of the mutual information [43]. For now it remains an open question whether the degree of violation of our symmetric EPR-steering inequalities (in bits) provides a lower bound to the secure key transmission rate.

XI. CONCLUSION

In this paper, we have shown how any set of operators obeying an entropic uncertainty relation can give rise to an entropic steering inequality. Specifically, we have derived steering inequalities for pairs of arbitrary observables; we have derived steering inequalities for complete sets of mutually unbiased observables; we have derived symmetric steering inequalities and hybrid steering inequalities; and we have derived steering inequalities for POVMs. In addition, we have examined the possibility of exclusive one-way steering in two-qubit states and looked at possible applications for these steering inequalities in QKD.

These steering inequalities provide a new general means of witnessing entanglement and EPR steering. Given an entangled pair of N-dimensional quantum systems, tomographic reconstruction of the density matrix requires on the order of N^4 measurements, though it offers a complete description of the bipartite state. Violating our steering inequalities, on the other hand, requires only on the order of N^2 measurements and, in some cases, only on the order of N measurements for our sum or difference steering inequalities, (14).

Though our entropic steering inequalities are general, they are not superior to all other forms of steering inequality. As shown in Sec. VII and Ref. [9], for two-qubit systems, there are states which will violate a variance-based EPR-steering inequality and fail to violate the corresponding entropic steering inequality with the same set of measurements. The strength of our inequalities rests in their being expressed in terms of entropies, used in information theory. Other entropic inequalities have been used to show that EPR steering proves security in 1sDIQKD [41].

Our entropic steering inequalities also provide further evidence that there may exist states which exhibit steering in only one direction. Some states [i.e., those in either off-diagonal quadrant in Figs. 2(a) and 2(b)], violate our entropic steering inequality in one direction, but not in the other, even when using an optimal set of measurement bases. This is an analogue, for the discrete case, of a phenomenon that has been shown to occur in continuous-variable systems by Midgley *et al.* [24]. Neither of these results is definitive proof of the existence of exclusively one-way steerable states. There could be inequalities that demonstrate one-way steering where our entropic inequalities fail to do so. A general proof would require a necessary and sufficient criterion for one-way and for two-way steering, but the inequalities presented here could provide a direction for further research.

ACKNOWLEDGMENTS

We gratefully acknowledge insightful discussions with Gregory A. Howland, as well as support from DARPA DSO InPho Grant No. W911NF-10-1-0404. C.J.B. acknowledges support from ARO Grant No. W911NF-09-1-0385 and NSF Grant No. PHY-1203931. S.P.W. acknowledges funding support from the Future Emerging Technologies FET-Open Program, within the 7th Framework Programme of the European Commission, under Grant No. 255914, PHORBITECH, and Brazilian agencies CNPq, CAPES, FAPERJ, and INCT-Informação Quântica. E.G.C. acknowledges funding support from ARC Grant No. DECRA DE120100559.

[1] S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro, Phys. Rev. Lett. **106**, 130402 (2011).

[2] S. P. Walborn, B. G. Taketani, A. Salles, F. Toscano, and R. L. de Matos Filho, Phys. Rev. Lett. **103**, 160505 (2009).

[3] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).

[4] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).

[5] J. C. Howell, R. S. Bennink, S. J. Bentley, and R. W. Boyd, Phys. Rev. Lett. **92**, 210403 (2004).

[6] D. J. Starling, C. J. Broadbent, and J. C. Howell, Phys. Rev. A **84**, 032305 (2011).

[7] M. D. Reid, Phys. Rev. A **40**, 913 (1989).

[8] M. D. Reid, P. D. Drummond, W. P. Bowen, E. G. Cavalcanti, P. K. Lam, H. A. Bachor, U. L. Andersen, and G. Leuchs, Rev. Mod. Phys. **81**, 1727 (2009).

[9] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Phys. Rev. A **80**, 032112 (2009).

[10] M. P. Edgar, D. S. Tasca, F. Izdebski, R. E. Warburton, J. Leach, M. Agnew, G. S. Buller, R. W. Boyd, and M. J. Padgett, Nat. Commun. **3**, 984 (2012).

[11] V. Händchen, T. Eberle, S. Steinlechner, A. Samblowski, T. Franz, R. F. Werner, and R. Schnabel, Nat. Photon. **6**, 596 (2012).

[12] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, December 10–12, 1984* (IEEE, New York, 1984), p. 175.

[13] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[14] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[15] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[16] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[17] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. (Wiley and Sons, New York, 2006).

[18] M. Ukowski and A. Zeilinger, Phys. Lett. A **155**, 69 (1991).

[19] X.-s. Ma, A. Qarry, J. Kofler, T. Jennewein, and A. Zeilinger, Phys. Rev. A **79**, 042101 (2009).

[20] L. Neves, G. Lima, A. Delgado, and C. Saavedra, Phys. Rev. A **80**, 042322 (2009).

[21] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).

[22] E. Schrdinger, Math. Proc. Cambridge Philos. Soc. **32**, 446 (1936).

[23] I. Bialynicki-Birula and J. Mycielski, Commun. Math. Phys. **44**, 129 (1975).

[24] S. L. W. Midgley, A. J. Ferris, and M. K. Olsen, Phys. Rev. A **81**, 022101 (2010).

[25] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

[26] I. Bialynicki-Birula and J. Madajczyk, Phys. Lett. A **108**, 384 (1985).

[27] J. Leach, B. Jack, J. Romero, A. K. Jha, A. M. Yao, S. Franke-Arnold, D. G. Ireland, R. W. Boyd, S. M. Barnett, and M. J. Padgett, Science **329**, 662 (2010).

[28] M. A. D. Carvalho, J. Ferraz, G. F. Borges, P.-L. de Assis, S. Pádua, and S. P. Walborn, Phys. Rev. A **86**, 032332 (2012).

[29] S. Mancini, V. Giovannetti, D. Vitali, and P. Tombesi, Phys. Rev. Lett. **88**, 120401 (2002).

[30] I. Bialynicki-Birula, Phys. Lett. A **103**, 253 (1984).

[31] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[32] S. Yu, Q. Chen, C. Zhang, C. H. Lai, and C. H. Oh, Phys. Rev. Lett. **109**, 120402 (2012).

[33] N. Gisin, Phys. Lett. A **154**, 201 (1991).

[34] J. Sanchez-Ruiz, Phys. Lett. A **201**, 125 (1995).

[35] T. Durt, B.-G. Englert, I. Bengtsson, and K. Zyczkowski, Int. J. Quantum. Inform. **8**, 535 (2010).

[36] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).

[37] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Nat. Phys. **6**, 845 (2010).

[38] E. G. Cavalcanti, P. D. Drummond, H. A. Bachor, and M. D. Reid, Opt. Express **17**, 18693 (2009).

[39] M. Krishna and K. R. Parthasarathy, Ind. J. Stat. **64**, 842 (2002).

[40] Y. Aharonov, D. Z. Albert, and L. Vaidman, Phys. Rev. Lett. **60**, 1351 (1988).

[41] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301 (2012).

[42] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science FOCS '98* (IEEE Computer Society, Washington, DC, 1998), p. 503.

[43] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).