Mutual uncertainty, conditional uncertainty, and strong subadditivity

Sk Sazim,[1,*] Satyabrata Adhikari,[2] Arun K. Pati,[1] and Pankaj Agrawal[3]
[1] *Harish-Chandra Research Institute, HBNI, Chhatnag Road, Jhunsi, Allahabad 211019, India*
[2] *Delhi Technological University, Shahbad Daulatpur, Main Bawana Road, Delhi-110042, India*
[3] *Institute of Physics, HBNI, Sainik School Post, Bhubaneswar-751005, Orissa, India*

(Received 26 May 2017; revised manuscript received 13 August 2018; published 28 September 2018)

We introduce a concept, called the mutual uncertainty between two observables in a given quantum state, which enjoys features similar to those of the mutual information for two random variables. Further, we define conditional uncertainty as well as conditional variance and show that conditioning on more observables reduces the uncertainty. Given three observables, we prove a "strong subadditivity" relation for the conditional uncertainty under certain conditions. As an application, we show that by using the conditional variance one can detect bipartite higher dimensional entangled states. The efficacy of our detection method lies in the fact that it gives better detection criteria than most of the existing criteria based on geometry of the states. Interestingly, we find that for N-qubit product states, the mutual uncertainty is exactly equal to $N - \sqrt{N}$, and if it is other than this value, the state is entangled. We also show that using the mutual uncertainty between two observables, one can detect non-Gaussian steering where Reid's criterion fails to detect it. Our results may open a direction of exploration in quantum theory and quantum information using mutual uncertainty, conditional uncertainty, and the strong subadditivity for multiple observables.

DOI: 10.1103/PhysRevA.98.032123

I. INTRODUCTION

In quantum theory, Heisenberg's uncertainty relation [1] restricts the knowledge of physical observables one can have about the quantum system. The Heisenberg-Robertson uncertainty [2–5] relation suggests the impossibility of preparing an ensemble where one can measure two noncommuting observables with infinite precision. Later, Schrödinger [6] improved the lower bound of this uncertainty relation. In fact, Robertson and Schrödinger formulated mathematically the uncertainty relation for any two observables. Recently, the stronger uncertainty relations have been proved which go beyond the Robertson-Schrödinger uncertainty relation [7] and this has strengthened the notion of incompatible observables in quantum theory [8–13].

Shannon introduced entropy as a measure of information contained in a classical random variable [14]. The introduction of entropy paved a path for a new field of "Classical Information Science" [15]. Later, von Neumann extended the idea of entropy to the quantum domain where one replaces the probability distribution of random variables with the density operators for the states of quantum systems. Undoubtedly, entropy is an important quantity in quantum information science [16,17]. As entropy measures lack of information about the preparation of a system, one can also express uncertainty relations in terms of entropies [18,19]. However, in the quantum world, variance of an observable is also a measure of lack of information about the state preparation [20]. Therefore, it may be natural to ask if using the variance as an uncertainty measure, one can define analogous quantities such as mutual information, conditional entropy, and the notion of strong subadditivity.

Once we define these quantities, one immediate question is, Do they provide insight into the quantum systems? The answer to this is in the affirmative. For example, mutual information is the cornerstone in defining many important aspects in information theory, such as unveiling correlations, channel capacities, etc., in quantum information science [16,17]. Conditional entropy is also inevitably an important quantity which is relevant in quantum communication as well as quantum computation [16,17]. While these analogies are very tempting to address for quantum uncertainty related quantities, there is a major departure between these two notions. Uncertainty is a function of both a quantum state and an observable, whereas the notion of entropy depends on either of the two [16,17]. Moreover, while uncertainty captures only the second moment, entropy contains all possible moments.

In this paper, we introduce the notions of mutual uncertainty, conditional uncertainty, and strong subadditivity on the basis of quantum uncertainties expressed in terms of standard deviations and variances. Interestingly, we find that the standard deviation (quantum uncertainty) behaves in many ways like entropy. For example, we find that a chain rule for the sum uncertainty holds. Due to this fact one can easily define many important quantities like conditional mutual uncertainty as well. Another important aspect of this formalism is that one can have a version of strong subadditivity (SSA) for quantum uncertainties which may have implications in quantum information and this may be of independent interest. Also, we prove the strong subadditivity for more than three observables using mutual uncertainty.

Then we address the physical implication of all these quantities introduced here. As illustrations, we consider two

*sk.sazimsq49@gmail.com

important aspects in quantum information science: detecting entanglement [21–23] as well as quantum steering [24]. We find that using the conditional variance, we can detect entanglement of higher dimensional bipartite mixed states. The method we present here is stronger than the criteria found by Vicente [25]. Moreover, we find that for N-qubit product states, mutual uncertainty is exactly equal to $N - \sqrt{N}$. This provides a sufficient condition to detect N-qubit entanglement. The other important finding is that we derive steering criterion based on mutual uncertainty. This criterion is as powerful as Reid's steering criterion [26] for two qubits, and overpower them when we consider non-Gaussian bipartite states. These results show the efficacy of our formalism. In fact, from the perspective of experimental realizations, our formalism might be one step ahead of the usual entropic formalism because variances are easy to measure experimentally compared to entropic quantities which cannot be measured directly.

The paper is organized as follows. In the next section, we discuss the sum uncertainty relation. Then, we define mutual uncertainty and conditional uncertainty and derive some important identities and inequalities such as the chain rule and the strong subadditivity of uncertainties in Sec. III. In Sec. IV, we study the physical implication of these quantities, namely, usefulness of the conditional variance in detecting entangled states and finding steerable states using the mutual uncertainty. We conclude in the last section.

II. SETTING THE STAGE: SUM UNCERTAINTY RELATIONS

Let us consider a set of observables represented by Hermitian operators $\{A_i\}$, then the uncertainty of A_i in a given quantum state ρ is defined as the statistical variance (Δ^2) or standard deviation (Δ) of the corresponding observable, i.e., $\Delta A_i^2 = \langle A_i^2\rangle - \langle A_i\rangle^2$, where $\langle A_i\rangle = \mathrm{Tr}[\rho A_i]$ for the state ρ. This positive quantity can only be zero if ρ is an eigenstate of A_i, representing the exact predictability of the measurement outcome. Hence, a quantum state with zero uncertainty must be a simultaneous eigenstate of all A_i. The "sum uncertainty relation" [27] tells us that the sum of uncertainty of two observables is greater than or equal to the uncertainty of the sum of the observables on a quantum system. If A and B are two general observables that represent some physical quantities, then one may ask, What is the relation between $\Delta(A+B)$, ΔA, and ΔB? The following theorem answers this.

Theorem. 1 [27]. Quantum fluctuation in the sum of any two observables is always less than or equal to the sum of their individual fluctuations, i.e., $\Delta(A+B) \leqslant \Delta A + \Delta B$.

The theorem was proved for pure states only, but one can easily extend the result for the arbitrary mixed states by employing the *purification of the mixed states* in higher dimensional Hilbert space. The physical meaning of the sum uncertainty relation is that *if we have an ensemble of quantum systems then the ignorance in totality is always less than the sum of the individual ignorances*. In the case of two observables, if we prepare a large number of quantum systems in the state ρ, and then perform the measurement of A on some of those systems and B on some others, then the standard deviations in A plus B will be more than the standard deviation in the measurement of $(A+B)$ on those systems. Hence, it is always advisable to go for the "joint measurement" if we want to minimize the error. Another aspect of this theorem is that it is similar in spirit to the subadditivity of the von Neumann entropy, i.e., $S(\rho_{12}) \leqslant S(\rho_1) + S(\rho_2)$, where ρ_{12} is a two-particle density operator and $\rho_2 = \mathrm{Tr}_1(\rho_{12})$ is the reduced density for subsystem 2.

Noticing this resemblance of quantum entropy and standard deviation measure of uncertainty, it is tempting to see if we can unravel some other features. Before doing that we will first summarize the properties of the uncertainty (captured by standard deviation) [27].

Properties of $\Delta(\cdot)$. (i) $\Delta A_i \geqslant 0$ for $\{A_i\}$ in ρ. (ii) It is convex in nature, i.e., $\Delta(\sum_i p_i A_i) \leqslant \sum_i p_i \Delta(A_i)$, with $0 \leqslant p_i \leqslant 1$ and $\sum_i p_i = 1$. (iii) One cannot decrease the uncertainty of an observable by mixing several states $\rho = \sum_\ell \lambda_\ell \rho_\ell$, i.e., $\Delta(A)_\rho \geqslant \sum_\ell \lambda_\ell \Delta(A)_{\rho_\ell}$, with $\sum_\ell \lambda_\ell = 1$. This is similar to the fact that entropy is also a concave function of the density matrices, i.e., $S(\sum_\ell \lambda_\ell \rho_\ell) \geqslant \sum_\ell \lambda_\ell S(\rho_\ell)$.

In fact, it is not difficult to see that if we have more than two observables (say three observables A, B, and C), then the sum uncertainty relation will read as $\Delta(A+B+C) \leqslant \Delta A + \Delta B + \Delta C$. In general, for observables $\{A_i\}$, we will have the sum uncertainty relation as $\Delta(\sum_i A_i) \leqslant \sum_i \Delta A_i$ [27].

III. MUTUAL UNCERTAINTY

For any two observable A and B, mutual uncertainty in the quantum state ρ is defined as

$$M(A:B) := \Delta A + \Delta B - \Delta(A+B). \tag{1}$$

We name $M(A:B)$ as the *mutual uncertainty* in the same spirit as that of the mutual information. [The mutual information for a bipartite state ρ_{12} is defined as $I(\rho_{12}) = S(\rho_1) + S(\rho_2) - S(\rho_{12})$.] The quantity $M(A:B)$ captures how much overlap two observables can have in a given quantum state.

Properties of $M(A:B)$. (i) $M(A:B) \geqslant 0$, (ii) it is symmetric in A and B, i.e., $M(A:B) = M(B:A)$, and (iii) $M(A:A) = 0$. Note that $I(\rho_{12})$ also satisfies similar properties.

The above definition of mutual uncertainty can be generalized for n number of observables. Thus, given a set of observables $\{A_i; i = 1, 2, ..., n\}$, we have

$$M(A_1 : A_2 : \cdots : A_n) := \sum_{i=1}^{n} \Delta A_i - \Delta\left(\sum_{i=1}^{n} A_i\right). \tag{2}$$

The above relation is analogous to the mutual information for n-particle quantum state $\rho_{12\ldots n}$ which is defined as $I(\rho_{12\ldots n}) = \sum_{i=1}^{n} S(\rho_i) - S(\rho_{12\ldots n})$ [28].

Note that all the observables may not have the same physical dimension but one can make them of the same dimension by multiplying them with proper dimensional quantities. Although in this article we have omitted this possibility by considering dimensionless observables.

A. Conditional uncertainty and chain rule for uncertainties

We define a quantity called the conditional uncertainty [similar to the conditional entropy $S(\rho_{1|2}) = S(\rho_{12}) - S(\rho_2)$]

as

$$\Delta(A|B) := \Delta(A+B) - \Delta B. \tag{3}$$

This suggests how much uncertainty in $(A+B)$ remains after we remove the uncertainty in B.

Properties of $\Delta(A|B)$. (i) $\Delta(A|B) \leqslant \Delta A$, i.e., conditioning on more observables reduces the uncertainty. (ii) $\Delta(A|B) \geqslant 0$ but can be negative if $\Delta(A+B) < \Delta B$ or vice versa. (iii) $\Delta(A|A) = \Delta A$.

By noting that $\Delta(A|B) = \Delta A - M(A:B)$ and $M(A:B) \geqslant 0$, we have property (i). A simple example will illustrate property (ii) [29].

Now we will derive some useful results using mutual uncertainty and conditional uncertainty.

Theorem 2. Chain rule for the sum uncertainty holds, i.e., $\Delta(\sum_{i=1}^{n} A_i) = \sum_{i=1}^{n} \Delta(A_i|A_{i-1} + \cdots + A_1)$.

Proof. For three observables, the chain rule reads as

$$\Delta(A+B+C) = \Delta A + \Delta(B|A) + \Delta(C|A+B).$$

Now consider

$$\begin{aligned}\text{RHS} &= \Delta A + \Delta(B|A) + \Delta(C|A+B)\\ &= \Delta A + \Delta(B|A) + \Delta(C+A+B) - \Delta(A+B)\\ &= \Delta(C+A+B) = \text{LHS}.\end{aligned}$$

Similarly, one can prove by mathematical induction that the theorem holds for all positive integers n. ■

This tells us that the sum uncertainty of two observables is equal to the uncertainty of one observable plus the conditional uncertainty of the other observables, i.e., $\Delta(A+B) = \Delta(A) + \Delta(B|A)$, which is similar to the entropy of the joint random variables or the bipartite systems. We can also define the following quantity as well.

Conditional mutual uncertainty. We define another quantity which we call the conditional mutual uncertainty in the same spirit of the conditional mutual information. This is defined as $M(A:B|C) := \Delta(A|C) + \Delta(B|C) - \Delta(A+B|C)$, which can be simplified as

$$M(A:B|C) = \Delta(B|C) - \Delta(B|C+A), \tag{4}$$

using the chain rule for the mutual uncertainty.

B. Strong subadditivity relations

The strong subadditivity of entropy is an important result in information science. It gives a fundamental limitation to the distribution of entropy in a composite system [30,31]. In the classical case it implies the non-negativity of the mutual information. For the relative entropy based quantum mutual information, $I(\rho_{12\ldots n}) = S(\rho_{12\ldots n} \| \otimes_{i=1}^{n} \sigma_i)$ [32], the strong subadditivity of entropy guarantees the positivity [33] but not for the other versions of mutual information [34]. In a broad sense, the strong subadditivity of entropy implies that *conditioning will not increase the entropy*, i.e., $S(\rho_{1|23}) \leqslant S(\rho_{1|2})$. Moreover, beyond three-particle systems we do not know the actual form of strong subadditivity of quantum entropy. Here, we will prove a strong subadditivity type of relation concerning the uncertainties for multiple observables in a given quantum state.

Theorem 3. If $M(B:C) = 0$, then $\Delta(A|B+C) \leqslant \Delta(A|B)$, i.e., conditioning on more observables reduces the uncertainty.

Proof. Lets start with the sum uncertainty relation, i.e.,

$$\begin{aligned}\Delta(A+B+C) &\leqslant \Delta(A+B) + \Delta C,\\ \Delta(A+B+C) - \Delta(B+C) &\leqslant \Delta(A+B) - \Delta B + \Delta B\\ &\quad + \Delta C - \Delta(B+C),\\ \Delta(A|B+C) &\leqslant \Delta(A|B) + M(B:C).\end{aligned}$$

Hence, the proof ■

The above relation can be understood as the "strong subadditivity" of uncertainty. The strong subadditivity relation for uncertainty also ensures that the mutual uncertainty is always positive. For an arbitrary number of observables, the strong subadditivity relation says that if $M(A_2 + \cdots + A_{n-1} : A_n) = 0$, then $\Delta(A_1|A_2 + \cdots + A_n) \leqslant \Delta(A_1|A_2 + \cdots + A_{n-1})$. Next we will prove two important relations concerning the mutual uncertainty.

Inequality 1. Discarding the observables, one cannot increase the mutual uncertainty, i.e., $M(A:B) \leqslant M(A:B+C)$.

Proof. To prove this, let us start with the quantity $M(A:B+C)$.

$$\begin{aligned}M(A:B+C) &= \Delta A + \Delta(B+C) - \Delta(A+B+C),\\ \Delta(A+B+C) &= \Delta A + \Delta(B+C) - M(A:B+C),\\ &\leqslant \Delta A + \Delta B + \Delta C - M(A:B+C),\\ &\leqslant M(A:B) + \Delta(A+B) + \Delta C\\ &\quad - M(A:B+C),\\ &\leqslant (\Delta A + \Delta B + \Delta C)\\ &\quad - [M(A:B+C) - M(A:B)].\end{aligned}$$

Using the sum uncertainty relation for three observables

$$\Delta(A+B+C) \leqslant \Delta A + \Delta B + \Delta C$$

and Eq. (5), we get

$$M(A:B+C) - M(A:B) \geqslant 0.$$

Hence the proof. ■

This is another form of strong subadditivity in terms of mutual uncertainty. Interestingly, mutual information also satisfies $I(\rho_{12}) \leqslant I(\rho_{1(23)})$ [15]. Similarly, there is another total correlation measure, called the entanglement of purification [35], that satisfies $E(\rho_{12}) \leqslant E(\rho_{1(23)})$ [36]. These observations provide added motivation to explore these quantities in greater detail.

All these inequalities resemble the well-known inequalities concerning entropy, which are the cornerstone of quantum information science. However, we note that these similarities are structural; actual interpretations of these inequalities might be completely different.

Conditional variance. Here, we define conditional variance (similar to conditional entropy) as

$$\Delta(A|B)^2 := \Delta(A+B)^2 - \Delta B^2. \tag{5}$$

This quantity is equivalent to $\Delta A^2 + 2\,\mathrm{Cov}(A,B)$, where $\mathrm{Cov}(A,B) = \frac{1}{2}\mathrm{Tr}[\rho(AB+BA)] - \mathrm{Tr}[\rho A]\,\mathrm{Tr}[\rho B]$ is the covariance of A and B. It says that if the covariance is nonzero then the uncertainty in A may increase or decrease due to the knowledge of the uncertainty of B since covariance can take both positive (correlation) and negative (anticorrelation) values. This is in some sense different from conditional uncertainty.

IV. PHYSICAL IMPLICATIONS

In this section, we will focus on some applications of the quantities we introduced in the main text, e.g., mutual uncertainty, conditional uncertainty, and conditional variance. We will study these quantities for discrete systems such as qubit systems as well as higher dimensional systems and continuous variable systems also.

A. Detection of entangled states

Entanglement is a crucial resource for many quantum information protocols (e.g., see [22]). Hence, detection and quantification of entanglement is an important task. Several ways to detect entanglement have been proposed in the recent past [23]. In the literature, uncertainty relations have been employed to detect entanglement where operators can be either locally applied on the subsystems [37] or globally applied on the system as a whole [38]. This motivates us to ask the natural question here, Can we detect entanglement using the conditional variance or other introduced quantities here? In the subsequent analysis, we answer this question in the affirmative.

There exist many elegant methods to detect entanglement using the local uncertainty relations [37,39–41] or using geometry of quantum states [25,42–48]. It is worthwhile to mention that by using local uncertainty relations, one can detect a more general form of entanglement, known as generalized entanglement, which includes standard entanglement as a special case [49–52].

In the following we use conditional variance to derive a criterion that will detect the entanglement of two qudit mixed states. We find that the criterion based on conditional variance is better than the existent criteria based on the geometry of the quantum states [25,39,40,47,48]. We also consider N-qubit pure states and find a sufficient criterion for detecting its entanglement using mutual uncertainty.

Bloch representation of N-particle quantum systems and the condition for its separability. To express quantum states in higher dimension geometrically, one needs to understand the structure of the SU(d) group. It contains d^2-1 generators termed as σ_i, which form the basis of the Lie algebra with commutation and anticommutation relations, respectively,

$$[\sigma_i,\sigma_j] = 2i\sum_k f_{ijk}\sigma_k,$$

$$\{\sigma_i,\sigma_j\} = \frac{4}{d}\delta_{ij} + 2\sum_k d_{ijk}\sigma_k.$$

Here f_{ijk} and d_{ijk} are the antisymmetric and symmetric structure constants. All σ_i are traceless Hermitian matrices which satisfy $\sigma_i\sigma_j = \frac{2}{d}\delta_{ij}\mathbb{I}_d + \sum_k (if_{ijk}+d_{ijk})\sigma_k$. For $d=2$, the symmetric structure constants d_{ijk} are ideally zero and the generators are well-known Pauli matrices, whereas for $d=3$, the generators are Gell-Mann matrices.

Any arbitrary single-particle quantum state in d dimensions can be expressed as $\varrho = \frac{1}{d}\mathbb{I}_d + \frac{1}{2}\vec{r}\cdot\vec{\sigma}$, where $\mathbb{I}_n$ is the identity matrix of order n and $|\vec{r}|^2 \leqslant \frac{2(d-1)}{d}$. The density matrix ϱ is a Hermitian matrix with $\varrho \geqslant 0$, $\varrho \geqslant \varrho^2$ (equality holds when ϱ is pure), and $\mathrm{Tr}[\varrho]=1$.

The N-qudit state can be expressed in the generalized Bloch vector representation as

$$\begin{aligned}\rho =& \frac{1}{d^N}\mathbb{I}_{d^N} + \frac{1}{2d^{N-1}}\big[\vec{\sigma}\cdot\vec{r}\otimes\mathbb{I}_d^{\otimes N-1} + \cdots \\ &+ \mathbb{I}_d^{\otimes N-1}\otimes\vec{\sigma}\cdot\vec{r_N}\big] + \frac{1}{4d^{N-2}}\sum_{ij}\big[t_{ij0\cdots0}\sigma_i\otimes\sigma_j \\ &\times\otimes\mathbb{I}_d^{\otimes N-2} + \cdots + t_{0\cdots0ij}\mathbb{I}_d^{\otimes N-2}\otimes\sigma_i\otimes\sigma_j\big] + \cdots \\ &+ \frac{1}{2^N}\sum_{i_1\cdots i_N} t_{i_1\cdots i_N}\sigma_{i_1}\otimes\cdots\otimes\sigma_{i_N},\end{aligned} \tag{6}$$

where $\vec{r_i}$ are the Bloch vectors for the ith subsystem, $\{[t_{ij0\cdots0}],\ldots,[t_{0\cdots0ij}]\}$ are pairwise correlation tensors, and $[t_{i_1\cdots i_N}]$ is the N-way correlation tensor. There are other types of correlation tensors, such as three-way, four-way, and $\cdots$, $N-1$-way, which will not play a role in our analysis. For notational simplicity, we will call $T^{(k)}$ the k-way correlation tensor, where, for example, $T^{(2)}$ forms a set $\{[t_{ij0\cdots0}],\ldots,[t_{0\cdots0ij}]\}$ and so on. The conditions required to approve the above matrix as a valid density matrix are – $|\vec{r_i}|^2 \leqslant \frac{2(d-1)}{d}$, $\rho\geqslant 0$, $\rho\geqslant\rho^2$ (equality holds when ρ is pure), and $\mathrm{Tr}[\rho]=1$.

Now we are ready to address the separability of the N-particle quantum state expressed in Eq. (6). This problem can easily be addressed by exploiting the Bloch-vector representation of quantum systems as shown in Refs. [53–58]. In order to describe the separability criteria, one can make use of the Ky-Fan norm [59]. The Ky-Fan norm of a matrix, X, is defined as the sum of the singular values (λ_i) of X, i.e., $\|X\|_{\mathrm{KF}} := \sum_i \lambda_i(X) = \mathrm{Tr}[\sqrt{X^\dagger X}]$, where $\dagger$ denotes complex conjugation. In the Bloch-vector representation, for the state ρ, if the reduced density matrix of a subsystem consisting of k $(2\leqslant k\leqslant N)$ out of N parts is separable then $\|T^{(k)}\|_{\mathrm{KF}} \leqslant \sqrt{(1/2^k)d^k(d-1)^k}$ [53]. This is a set of conditions which leads to the hierarchy of entanglement structures [22]. However, in this work, we are restricting our analysis to two-qudit states and multiqubit states. Note that for $N=2$, the separability condition is [25]

$$\|T\|_{\mathrm{KF}} \leqslant \frac{d(d-1)}{2}, \tag{7}$$

and for N-qubit states ($d=2$), the separability conditions become $\|T^{(k)}\|_{\mathrm{KF}} \leqslant 1$ [53].

1. Detecting entanglement in higher dimensional bipartite quantum systems using conditional variance

A bipartite quantum state of d dimensions is entangled when it cannot be expressed as $\rho = \sum_i p_i\rho_1^i\otimes\rho_2^i$. This means, for separable states, the correlation matrix can be expressed as $T = \sum_i p_i\vec{r}_{1i}\vec{r}_{2i}^{\mathsf{T}}$, where p_i is the classical mixing parameter and T denotes the transposition. Here, we shed some light on the separability of the bipartite state using quantities like the conditional variance and by exploiting the Bloch-vector representation of the state.

Let $\mathcal{A} = \{\tilde{A}_i = \vec{a}_i \cdot \vec{\sigma};\ i = 1, \ldots, d^2-1\}$ are a complete set of orthogonal observables such that $\mathrm{Tr}[\tilde{A}_i\tilde{A}_j] = 2\delta_{ij}$. We can express these observables in a compact form like $\tilde{A}_i = \sum_j \Theta_{ij}\sigma_j$, where $\Theta \in SO(d^2-1)$. Similarly, consider another such set of observables, $\mathcal{B} = \{\tilde{B}_i = \vec{b}_i \cdot \vec{\sigma};\ i = 1, \ldots, d^2-1\}$, where $\vec{a}_i(\vec{b}_i)$ denotes the Bloch vector of the orthogonal operators $\tilde{A}_i$ $(\tilde{B}_i)$ with unit norm. For observables like $A_i = \tilde{A}_i \otimes \mathbb{I}_d$ and $B_i = \mathbb{I}_d \otimes \tilde{B}_i$, the sum of all conditional variances is

$$\sum_i \Delta(A_i|B_i)^2 = \sum_i \Delta(A_i + B_i)^2 - \sum_i \Delta B_i^2. \tag{8}$$

For two-qudit separable states and the choice of the above observables, we state the following theorem.

Theorem 4. For two-qudit separable states and the set of observables $\{A_i\}$ and $\{B_i\}$ described above, $\sum_i \Delta(A_i|B_i)^2 \geqslant 2(d-1)$. This criterion is equivalent to $\|T\|_{\mathrm{KF}} \leqslant \frac{2(d-1)}{d} - \frac{1}{2}(|\vec{r}_1| - |\vec{r}_2|)^2$.

Proof. For the two-qudit states, the sum of conditional variances can be expressed as

$$\begin{aligned}\sum_i \Delta(A_i|B_i)^2 &= \frac{2}{d}(d^2-1) + 2\sum_i \vec{a}_i^{\intercal} T \vec{b}_i \\ &\quad - \sum_i (\vec{r}_{1i}\cdot\vec{a}_i + \vec{r}_{2i}\cdot\vec{b}_i)^2 + |\vec{r}_2|^2, \\ &\leqslant \frac{2}{d}(d^2-1) + 2\sum_i \vec{a}_i^{\intercal} T \vec{b}_i - (|\vec{r}_1|^2 - 2|\vec{r}_1\|\vec{r}_2|).\end{aligned} \tag{9}$$

While deriving the above relation, we have employed the fact that the symmetric structure constant d_{ijk} follows $\sum_{i=1}^{d^2-1} d_{iik} = 0, \forall\, k$.

However, for two-qudit separable states, the sum of conditional variances can directly be calculated as

$$\begin{aligned}\sum_i \Delta(A_i|B_i)^2 &= \frac{2}{d}(d^2-1) + 2\sum_{i,j} p_j(\vec{r}_{1j}\cdot\vec{a}_i)(\vec{r}_{2j}\cdot\vec{b}_i) \\ &\quad - \sum_i \left[\sum_j p_j(\vec{r}_{1j}\cdot\vec{a}_i + \vec{r}_{2j}\cdot\vec{b}_i)\right]^2 + |\vec{r}_2|^2, \\ &\geqslant \frac{2}{d}(d^2-1) - \sum_j p_j(|\vec{r}_{1j}|^2 + |\vec{r}_{2j}|^2) + |\vec{r}_2|^2, \\ &\geqslant 2(d-1),\end{aligned} \tag{10}$$

where we used the relation, $2\sum_j p_j(\vec{r}_{1j}\cdot\vec{a}_i)(\vec{r}_{2j}\cdot\vec{b}_i) = \sum_j p_j[(\vec{r}_{1j}\cdot\vec{a}_i + \vec{r}_{2j}\cdot\vec{b}_i)^2 - \{(\vec{r}_{1j}\cdot\vec{a}_i)^2 + (\vec{r}_{2j}\cdot\vec{b}_i)^2\}]$. Equation (10) proves one part of Theorem 4.

Now from Eqs. (9) and (10), one could easily find that for two-qudit separable states,

$$\sum_i \vec{a}_i^{\intercal} T \vec{b}_i \geqslant -\frac{2(d-1)}{d} + \frac{1}{2}(|\vec{r}_1| - |\vec{r}_2|)^2. \tag{11}$$

Equation (11) will be valid for any basis vector $\vec{a}_i$ and $\vec{b}_i$. If we choose $\vec{a}_i = \vec{u}_i$ and $\vec{b}_i = -\vec{v}_i$, where $\vec{u}_i$ and $\vec{v}_i$ are left and right singular vectors of T respectively, then Eq. (12) can be cast as

$$\|T\|_{\mathrm{KF}} \leqslant \frac{2(d-1)}{d} - \frac{1}{2}(|\vec{r}_1| - |\vec{r}_2|)^2. \tag{12}$$

Hence, the theorem is proved. ∎

To show the efficacy of the proposed criterion, we have considered the following examples.

Example 1. Let us consider a two-qubit state considered in canonical form, $\rho = \frac{1}{4}[\mathbb{I}_4 + \frac{2}{5}(1-\alpha)\sigma_3 \otimes \mathbb{I}_2 - \frac{3}{5}(1-\alpha)\mathbb{I}_2 \otimes \sigma_3 - \alpha\sum_{i=1}^{3}\sigma_i \otimes \sigma_i]$, which is entangled for $\alpha > \frac{1}{19(5\sqrt{6}-6)} \simeq 0.3288$ as predicted by Peres-Horodecki criterion [60]. According to the proposed criterion, the above state is entangled when $\alpha > \frac{49}{74+5\sqrt{221}} \simeq 0.3303$, whereas the criterion in Eq. (7) detects it for $\alpha > \frac{1}{3}$. This example displays that the separability criterion derived in Eq. (12) is weaker than the Peres-Horodecki criterion in $2 \otimes 2$ dimension, but it is stronger than the criterion in Eq. (7).

Example 2. Now, we consider the bound entangled state in $3 \otimes 3$ from Ref. [61], i.e., $\rho = \frac{1}{4}[\mathbb{I}_9 - \sum_i^4 |\psi_i\rangle\langle\psi_i|]$, where $|\psi_0\rangle = |0\rangle(|0\rangle - |1\rangle)/\sqrt{2}$, $|\psi_1\rangle = (|0\rangle - |1\rangle)|2\rangle/\sqrt{2}$, $|\psi_2\rangle = |2\rangle(|1\rangle - |2\rangle)/\sqrt{2}$, $|\psi_3\rangle = (|1\rangle - |2\rangle)|0\rangle/\sqrt{2}$, and $|\psi_2\rangle = (|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle)/3$. For this state one readily finds that $\|T\|_{\mathrm{KF}} \simeq 3.1603$, which violates both conditions (12) and (7). Hence, for this state, both the present criterion and the criterion in Eq. (7) are able to detect its entanglement. Note that in this case, the Peres-Horodecki criterion fails.

2. Mutual uncertainty and the N-qubit pure states

Before proceeding toward N-qubit pure states, we consider two-qubit pure states. Let us consider two observables $A = \vec{a}\cdot\vec{\sigma} \otimes \mathbb{I}_2$ and $B = \mathbb{I}_2 \otimes \vec{a}\cdot\vec{\sigma}$ with $\vec{a}\cdot\vec{r}_1 = \vec{b}\cdot\vec{r}_2 = 0$ and $|\vec{a}|^2 = |\vec{b}|^2 = 1$, where $\vec{\sigma}$ contains Pauli matrices only [62]. Then for arbitrary pure two-qubit states the mutual uncertainty reads as $M(A:B) = 2 - \sqrt{2 + 2\vec{a}^{\intercal} T \vec{b}}$, where $T = [t_{ij}]$ is the correlation matrix. For a pure product state, $T = \vec{r}_1\vec{r}_2^{\,\intercal}$, the mutual uncertainty turns out to be $M(A:B) = 2 - \sqrt{2}$. This result tells us that if the mutual uncertainty for a given pure state is found to be other than $2 - \sqrt{2} \approx 0.586$, then the given pure state is entangled. This gives a sufficient condition for the detection of a pure entangled state. Thus, we can say that the mutual uncertainty between two observables can detect pure entangled states. This may provide direct detection of pure entangled states in real experiments. Moreover, this is a state-independent and observable-independent universal value for mutual uncertainty.

There is another important aspect to this analysis for qubit systems. To show it, we consider an arbitrary two-qubit entangled state in Schmidt decomposition form as $|\Psi\rangle = \sqrt{\lambda}|00\rangle + \sqrt{1-\lambda}|11\rangle$. The mutual uncertainty for the arbitrary pure two-qubit entangled state is given by

$$M(A:B)_{|\Psi\rangle} = 2 - \sqrt{2 + 2Ct}, \tag{13}$$

where C is the concurrence of $|\Psi\rangle$ [63] and $t = a_1b_1 - a_2b_2$. Note that the concurrence of any arbitrary $|\Psi\rangle$ is defined as

$C = |\langle\Psi|\sigma_2 \otimes \sigma_2|\Psi^*\rangle|$, where $*$ indicates complex conjugation. Interestingly, from the above relation one can see that by measuring the mutual uncertainty between two observables, one can directly infer the concurrence as $C = \frac{1}{2t}[2 + M(M - 4)]$. Note that t depends on the choice of observables.

The above analysis paves the way to extending the results for N qubits. The mutual uncertainty expression for an N-qubit state is $M(A_1 : \cdots : A_N) = N - \sqrt{N + 2\sum_{ij} \vec{a}_i^{\mathsf{T}} T^{(2)} \vec{a}_j}$, where we have considered $A_i = \cdots \otimes \vec{a}_i \cdot \vec{\sigma} \otimes \cdots$, where i denotes the particular qubit and $\vec{a}_i \cdot \vec{r}_i = 0$, $|\vec{a}_i|^2 = 1$. (For example, $A_1 = \vec{a}_1 \cdot \vec{\sigma} \otimes \mathbb{I}_2 \otimes \mathbb{I}_2 \cdots$, $A_2 = \mathbb{I}_2 \otimes \vec{a}_2 \cdot \vec{\sigma} \otimes \mathbb{I}_2 \otimes \cdots$, etc.) If the pure state is completely factorized then the bicorrelation matrices can be decomposed as $\{[t_{ij0\ldots}] = \vec{r}_1 \vec{r}_2^{\mathsf{T}}, \ldots, [t_{\ldots 0ij}] = \vec{r}_{N-1} \vec{r}_N^{\mathsf{T}}\}$. Hence, for genuine product states,

$$M(A_1 : \cdots : A_N) = N - \sqrt{N}. \tag{14}$$

Hence, we state the following proposition.

Proposition 1. For pure N-qubit states with all pairwise correlation tensors of the form $T^{(2)} = \vec{r}_i \vec{r}_j^{\mathsf{T}}$ $(i \neq j)$ and the set of N observables $\{A_i\}$, the mutual uncertainty is $M(A_1 : \cdots : A_N) = N - \sqrt{N}$, where r_i is the Bloch vector of the ith subsystem.

Negation of Proposition 1 for any pure N-qubit state sufficiently tells us that the state contains at least pairwise entanglement. Again, this provides a universal way to detect multiqubit entanglement.

B. Detection of steerability of quantum states

Quantum steering is a nonlocal phenomenon introduced by Schrödinger [24] while reinterpreting the Einstein Podolsky Rosen (EPR) paradox [64]. The presence of entanglement between two subsystems in a bipartite state enables one to control the state of one subsystem by its entangled counterpart [24,26]. Later, it was mathematically formalized in Refs. [65,66]. Let Alice prepare an entangled state ρ_{12} and send one particle to Bob. Her job is to convince Bob that they are sharing nonlocal correlations (entanglement). Bob will believe such a claim if his state cannot be expressed by the local hidden state (LHS) model, i.e., $\tilde{\rho}_1^e = \sum_\mu p(\mu)\mathcal{P}(e|E,\mu)\rho_2^Q(\mu)$, where $F = \{p(\mu), \rho_2^Q(\mu)\}$ is an ensemble prepared by Alice and $\mathcal{P}(e|E,\mu)$ is Alice's stochastic map. Here, $p(\mu)$ is the distribution of hidden variable μ with constraint $\sum_\mu p(\mu) = 1$ and E denotes all possible projective measurements for Alice. Conversely, if Bob cannot find such F and $\mathcal{P}(e|E,\mu)$, then, he must admit that Alice can steer his system. Below, we present a strategy to detect quantum steering using mutual uncertainty.

Strategy. To test whether a multiparticle state exhibits steering, one can devise an inequality based on the quantum properties of one of the particles, and the inequality will be satisfied if the system has a LHS model description. The violation of such inequality will be the signature of the steerability in the system.

Here, we will devise such an inequality based on a simple property of the mutual uncertainty, i.e., $M(A : B) \geqslant 0$. We will employ the method used by Reid in Ref. [26]. If two arbitrary observables A and C have nonzero correlations, i.e., $\mathrm{Cov}(A, C) \neq 0$, then by knowing the measurement outcome of C one can infer the value of A which may reduce the error in the later measurement. Using this simple observation one can derive steering inequalities using different types of uncertainty relations [67–69].

If Alice infers the measurement outcomes of A performed by Bob, then the inferred uncertainty of A is

$$\Delta_{\inf} A = \sqrt{\langle (A - A_{\mathrm{est}}(C)\rangle^2}, \tag{15}$$

where $A_{\mathrm{est}}(C)$ is Alice's estimate using her measurement outcomes of C. In Ref. [68], it has been proved that the following inequality holds if we assume that Bob has LHS description:

$$\begin{gathered}\Delta_{\inf} A + \Delta_{\inf} B \geqslant \Delta(A + B). \\ \text{Hence,} \quad M_{\inf}(A : B) \geqslant 0,\end{gathered} \tag{16}$$

where $M_{\inf}(A : B) = \Delta_{\inf} A + \Delta_{\inf} B - \Delta(A + B)$ might be termed as the "inferred" mutual uncertainty. Equation (16) is another type of steering inequality.

Proposition 2. For any bipartite quantum state and any two observables, A and B, if $M_{\inf}(A : B) < 0$, then the quantum state can demonstrate steering.

To demonstrate the power of the steering criterion in Proposition 2, we consider the following examples.

Example 1. To demonstrate our criterion in discrete systems, here we will discuss the steerability of the Werner state,

$$\rho_W = p|\Psi^-\rangle\langle\Psi^-| + \frac{1-p}{4}\mathbb{I}_4, \tag{17}$$

where $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ and $\mathbb{I}_4$ is the identity matrix of order 4. The state ρ_W is entangled for $p > \frac{1}{3}$, steerable for $p > \frac{1}{2}$ and Bell nonlocal for $p > \frac{1}{\sqrt{2}}$.

Let us consider two noncommuting observables, $A = \sigma_x/2$ and $B = \sigma_z/2$. In this case, the direct calculation shows that $M_{\inf}(A : B) = \sqrt{1 - p^2} - 1/\sqrt{2}$. Therefore, the Werner state will show steerability if $p > 1/\sqrt{2}$ for two measurement settings. However, there exist two measurement steering inequalities which are violated by the Werner state for $p > 1/\sqrt{2}$ [67,68,70]. Then the question is, What features does our criterion entail? To show the power of our steering inequality, we will consider the following continuous variable systems.

Example 2. We will consider the non-Gaussian state which can be created from a two-mode squeezed vacuum by subtracting a single photon from any of the two modes. The Wigner function of such a state in terms of the conjugate variables (X_1, P_{X_1}), (X_2, P_{X_2}) can be expressed as [71]

$$\begin{aligned}
&W(X_1, P_{X_1}, X_2, P_{X_2}) \\
&\quad = \frac{1}{\pi^2} \exp\Bigg[2\sinh(2\alpha)(X_1X_2 - P_{X_1}P_{X_2}) \\
&\qquad - \cosh(2\alpha)\sum_{i=1}^{2}\left(X_i^2 + P_{X_i}^2\right)\Bigg] \\
&\qquad \times [-\sinh(2\alpha)\{(P_{X_1} - P_{X_2})^2 - (X_1 - X_2)^2\} + \\
&\qquad \times \cosh(2\alpha)\{(P_{X_1} - P_{X_1})^2 + (X_1 - X_2)^2\} - 1],
\end{aligned} \tag{18}$$

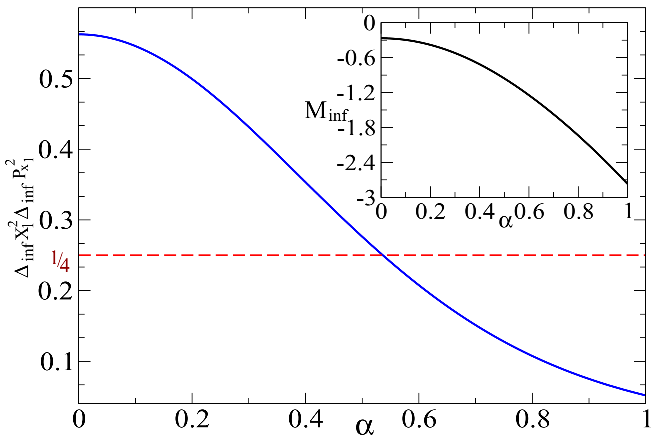

FIG. 1. Steerability of single-photon subtracted squeezed vacuum state. The solid blue curve depicts the plot of the product of inferred uncertainties, $\Delta_{\inf}X_1^2\Delta_{\inf}P_{X_1}^2$, and the red dashed line represents the lower bound of Reid's inequality; the inset graph shows the plot of $M_{\inf}(X_1 : P_{X_1})$ (solid black curve). It is clear that while the criterion based on mutual uncertainty captures the steerability for any value of α, the Reid criterion fails for $\alpha \leqslant \frac{1}{4}\cosh^{-1}(\frac{13}{3}) \approx 0.536$.

where α is a squeezing parameter. Now, Alice will infer the conjugate observables (X_1, P_{X_1}) measured at Bob's by performing the observables (X_2, P_{X_2}) at her side. The inferred uncertainties can directly be calculated and hence the inferred mutual uncertainty is

$$M_{\inf}(X_1 : P_{X_1}) = \frac{\sqrt{3}}{2}\left(\frac{1}{\eta_-} + \frac{1}{\eta_+}\right) - (\eta_+ + \eta_-), \qquad (19)$$

where $\eta_\pm = \sqrt{\cosh(2\alpha) \pm \cosh(\alpha)\sinh(\alpha)}$. If $M_{\inf}(X_1 : P_{X_1}) < 0$, then we can conclude that the state will demonstrate steering. To compare, we consider Reid's criterion for steering, which for our case is $\Delta_{\inf}X_1^2\Delta_{\inf}P_{X_1}^2 \geqslant 1/4$ [26]. For the state considered in Eq. (18), the right-hand side of Reid's inequality comes out to be

$$\Delta_{\inf}X_1^2\Delta_{\inf}P_{X_1}^2 = \frac{9}{2[3\cosh(4\alpha) + 5]}. \qquad (20)$$

Now to draw comparison between the two steering criteria, we plot Eqs. (19) and (20). From Fig. 1, we find that the steerability captured by the criterion based on mutual uncertainty is more than that of Reid's. More precisely, the criterion based on mutual uncertainty captures steerability for the whole range of α while Reid's criterion fails for $\alpha \leqslant \frac{1}{4}\cosh^{-1}(\frac{13}{3}) \approx 0.536$.

V. DISCUSSIONS AND CONCLUSIONS

We have introduced several quantities called mutual uncertainty, conditional uncertainty, and conditional variance which may be useful in many ways to develop faithful notions in quantum information theory. In doing so, we have been able to prove many results similar to those of entropic ones such as the chain rule and strong subadditivity relations for uncertainty. We have also shown that conditional variance and mutual uncertainty are useful for witnessing entanglement and quantum steering phenomena. Specifically, for physical applications, we find that using conditional variance, one can detect higher dimensional bipartite entangled states better than with the criteria given in Ref. [25]. Also, we find that the mutual uncertainty for N-qubit product states is exactly equal to $N - \sqrt{N}$, which provides a sufficient criterion to detect entanglement in multiqubit pure states. Moreover, the steering criterion based on mutual uncertainty is able to detect non-Gaussian steering where Reid's criterion [26] fails. In the future, it may be interesting to see if these notions have other implications in quantum information science.

ACKNOWLEDGMENTS

A.K.P. gratefully acknowledges the local hospitality during his visits at IOP, Bhubaneswar, where this work was initiated. We thank Sujit Choudhary for stimulating feedback. We also greatly acknowledge the anonymous referee, whose efforts enriched the presentation as well as the quality of our work.

[1] W. Heisenberg, Z. Phys. **43**, 172 (1927).
[2] E. H. Kennard, Z. Phys. **44**, 326 (1927).
[3] J. A. Wheeler and W. H. Zurek, *Quantum Theory and Measurement*, Princeton Series in Physics (Princeton University, Princeton, NJ, 1983).
[4] H. P. Robertson, Phys. Rev. **34**, 163 (1929).
[5] D. Sen, Curr. Sci. **107**, 203 (2014).
[6] E. Schrödinger, Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-mathematische Klasse **14**, 296 (1930).
[7] L. Maccone and A. K. Pati, Phys. Rev. Lett. **113**, 260401 (2014).
[8] Q.-C. Song and C.-F. Qiao, Phys. Lett. A **380**, 2925 (2016).
[9] K. Wang, X. Zhan, Z. Bian, J. Li, Y. Zhang, and P. Xue, Phys. Rev. A **93**, 052108 (2016).
[10] Y. Xiao and N. Jing, Sci. Rep. **6**, 36616 (2016).
[11] J. Zhang, Y. Zhang, and C.-s. Yu, Quantum Inf. Process. **16**, 131 (2017).
[12] Y. Xiao, N. Jing, X. Li-Jost, and S. M. Fei, Sci. Rep. **6**, 23201 (2016).
[13] T. Li, Y. Xiao, T. Ma, S. M. Fei, N. Jing, X. Li-Jost, and Z.-X. Wang, Sci. Rep. **6**, 35735 (2016).
[14] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
[16] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University, Cambridge, England, 2000).
[17] M. M. Wilde, *Quantum Information Theory* (Cambridge University, Cambridge, England, 2013).
[18] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[19] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Rev. Mod. Phys. **89**, 015002 (2017).
[20] Y. Huang, Phys. Rev. A **86**, 024101 (2012); G. Tóth, arXiv:1701.07461.

[21] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, Rev. Mod. Phys. **84**, 1655 (2012).

[22] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2007).

[23] O. Gühne and G. Tóth, Phys. Rep. **474**, 1 (2009).

[24] E. Schrödinger, Proc. Camb. Phil. Soc. **31**, 555 (1935); Math. Proc. Camb. Phil. Soc. **32**, 446 (1936).

[25] J. I. de Vicente, Quantum Inf. Comput. **7**, 624 (2007).

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

[27] A. K. Pati and P. K. Sahu, Phys. Lett. A **367**, 177 (2007).

[28] No unique multiparticle generalization of quantum mutual information exists. We have considered the relative distance based on one proposed in Ref. [32].

[29] As an illustration of the fact that $\Delta(A|B) < 0$, let us consider a harmonic oscillator Hamiltonian $H = \frac{1}{2}P^2 + \frac{1}{2}X^2$. Let $A = \frac{1}{2}P^2$ and $B = \frac{1}{2}X^2$. With this choice, one can see the quantity $\Delta(A|B)$ can be negative. For example, if $|\psi\rangle$ is an eigenstate of the Hamiltonian then $\Delta(A+B) = 0$ while ΔB is positive, and hence $\Delta(A|B)$ can be negative.

[30] H. Araki and H. Lieb, Commun. Math. Phys. **18**, 160 (1970).

[31] E. H. Lieb and M. B. Ruskai, J. Math. Phys. **14**, 1938 (1973).

[32] B. Groisman, S. Popescu, and A. Winter, Phys. Rev. A **72**, 032317 (2005).

[33] F. Herbut, J. Phys. A **37**, 3535 (2004).

[34] Sk Sazim and P. Agrawal, arXiv:1607.05155.

[35] B. M. Terhal, M. Horodecki, D. W. Leung, and D. P. DiVincenzo, J. Math. Phys. **43**, 4286 (2002).

[36] S. Bagchi and A. K. Pati, Phys. Rev. A **91**, 042323 (2015).

[37] H. F. Hofmann and S. Takeuchi, Phys. Rev. A **68**, 032103 (2003).

[38] O. Gühne, Phys. Rev. Lett. **92**, 117903 (2004).

[39] C. Qian, J.-L. Li, and C.-F. Qiao, Quantum Inf. Process. **17**, 84 (2018).

[40] O. Gühne, P. Hyllus, O. Gittsovich, and J. Eisert, Phys. Rev. Lett. **99**, 130504 (2007).

[41] J. I. de Vicente, Phys. Rev. A **75**, 052320 (2007); **77**, 039903(E) (2008).

[42] A. R. Usha Devi, R. Prabhu, and A. K. Rajagopal, Phys. Rev. Lett. **98**, 060501 (2007).

[43] S. Beigi, in *Proceedings of Iran Workshop on Communication and Information Theory*, (IEEE, Tehran, Iran, 2014), pp. 1–6.

[44] P. Agrawal, Sk Sazim, I. Chakrabarty, and A. K. Pati, Int. J. Quantum. Inf. **14**, 1640034 (2016).

[45] R. Schwonnek, L. Dammeier, and R. F. Werner, Phys. Rev. Lett. **119**, 170404 (2017).

[46] J.-L. Li and C.-F. Qiao, Sci. Rep. **8**, 1442 (2018).

[47] O. Rudolph, Quantum Inf. Process. **4**, 219 (2005).

[48] K. Chen and L.-A. Wu, Quantum Inf. Comput. **3**, 193 (2003).

[49] H. Barnum, E. Knill, G. Ortiz, R. Somma, and L. Viola, Phys. Rev. Lett. **92**, 107902 (2004)

[50] L. Viola, H. Barnum, E. Knill, G. Ortiz, and R. Somma, arXiv:quant-ph/0403044.

[51] R. Somma, G. Ortiz, H. Barnum, E. Knill, and L. Viola, Phys. Rev. A **70**, 042311 (2004).

[52] S. Boixo, L. Viola, and G. Ortiz, Europhys. Lett. **79**, 40003 (2007).

[53] A. S. M. Hassan and P. S. Joag, Quantum Inf. Comput. **8**, 0773 (2008).

[54] A. S. M. Hassan and P. S. Joag, Phys. Rev. A **77**, 062334 (2008).

[55] A. S. M. Hassan and P. S. Joag, Phys. Rev. A **80**, 042302 (2009).

[56] J. I. de Vicente and M. Huber, Phys. Rev. A **84**, 062306 (2011).

[57] M. Li, J. Wang, S.-M. Fei, and X. Li-Jost, Phys. Rev. A **89**, 022325 (2014).

[58] M. Li, S.-M. Fei, X. Li-Jost, and H. Fan, Phys. Rev. A **92**, 062338 (2015).

[59] R. Bhatia, *Matrix Analysis*, Graduate Texts in Mathematics (Springer, New York, 1997), Vol. 169.

[60] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996); M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[61] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).

[62] The variance is invariant under the substraction of constant diagonal matrix, i.e., for observable $\mathcal{O}$, $\Delta(\mathcal{O} - k\mathbb{I})^2 = \Delta\mathcal{O}^2$ with $k \in \mathcal{R}$ and $\mathbb{I}$ is the identity matrix. Therefore, without loss of generality one can consider traceless Hermitian operators as observables.

[63] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997); W. K. Wootters, *ibid.* **80**, 2245 (1998).

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

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

[66] S. J. Jones, H. M. Wiseman, and A. C. Doherty, Phys. Rev. A **76**, 052116 (2007).

[67] E. G. Cavalcanti and M. D. Reid, J. Mod. Opt. **54**, 2373 (2007).

[68] A. G. Maity, S. Datta, and A. S. Majumdar, Phys. Rev. A **96**, 052326 (2017).

[69] G. Sharma, C. Mukhopadhyay, Sk Sazim, and A. K. Pati, Phys. Rev. A **98**, 032106 (2018).

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

[71] G. S. Agarwal, *Quantum Optics* (Cambridge University, Cambridge, England, 2013).