DTU Library

Constructing Local Models for General Measurements on Bosonic Gaussian States

Jabbour, Michael G; Brask, Jonatan Bohr

Published in:
Physical Review Letters

Link to article, DOI:
10.1103/PhysRevLett.131.110202

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

Constructing Local Models for General Measurements on Bosonic Gaussian States

Michael G. Jabbour [*] and Jonatan Bohr Brask [†]
Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark

(Received 2 December 2022; revised 23 May 2023; accepted 22 August 2023; published 12 September 2023)

We derive a simple sufficient criterion for the locality of correlations obtained from given measurements on a Gaussian quantum state. The criterion is based on the construction of a local-hidden-variable model that works by passing part of the inherent Gaussian noise of the state onto the measurements. We illustrate our result in the setting of displaced photodetection on a two-mode squeezed state. Here, our criterion exhibits the existence of a local-hidden-variable model for a range of parameters where the state is still entangled.

DOI: 10.1103/PhysRevLett.131.110202

Introduction.—Quantum mechanics allows for correlations than are impossible classically and which can be exploited in a variety of applications. In particular, entangled quantum states are a key resource for quantum information science, enabling advantages in computing, communication, and sensing [1–4]. Furthermore, as shown by Bell [5], measurements on certain entangled states can lead to observations that violate a so-called Bell inequality and are then incompatible with local causal explanations. This phenomenon, known as nonlocality, demonstrates a profound departure from classical physics and is a cornerstone of modern understanding of quantum physics [6]. Nonlocal correlations also enable advantages for communication [7,8] and information processing at an unprecedented level of security [9–11].

Entanglement and nonlocality, however, are not equivalent. While entanglement is a prerequisite for nonlocality, in general, only carefully chosen measurements on a given entangled state will produce nonlocal observations, and while such measurements can always be found for pure entangled states [12], there exist mixed entangled states that are local for any possible measurements [13,14]. Deciding whether given states can give rise to nonlocality is desirable both for applications and fundamentally. This is, for instance, crucial in the context of device-independent (DI) quantum key distribution (QKD), the strongest form of quantum cryptographic protocols [15,16]. In DIQKD and other DI protocols, security relies on the violation of a Bell inequality and hence requires the use of entangled states that enable nonlocality.

Certifying whether an entangled state exhibits nonlocality is far from trivial. To demonstrate nonlocality, it is sufficient to find a particular set of measurements that leads to violation of a particular Bell inequality. Demonstrating that a state cannot give rise to nonlocality is much harder because there are infinitely many possible measurements and Bell inequalities. It requires the construction of local-hidden-variable (LHV) models that can reproduce the observations for any combination of measurements. Constructing such models is challenging, even for particular classes of measurements. A number of methods for constructing LHV models have nevertheless been developed [13,14,17–22], applicable to a variety of entangled states and measurements. Very often, a clear connection between the introduction of noise and the vanishing of nonlocality can be identified in these models, e.g., in [13,18].

While most previous work is concerned mainly with systems of finite dimension, another relevant class is that of so-called continuous-variables systems [23]. Most particularly, Gaussian bosonic states and transformations are ubiquitous in quantum theory and in experiments in, e.g., optical, superconducting, and mechanical platforms. At the same time, Gaussian systems are relatively easy to model. Their entanglement properties have been extensively studied [24,25] and their nonlocality [26–35] and steering [36] have also been explored. The relation between noise and nonlocality has also been investigated [37,38]. For Gaussian measurements on Gaussian states, the resulting observations are always local, because the positive Wigner function of such states enables the construction of an LHV model for any set of Gaussian measurements (as explained in more detail below). However, little is known about the existence of LHV models for Gaussian states subject to non-Gaussian measurements.

Here, we develop a sufficient criterion for the existence of LHV models for general measurements on Gaussian states. Given a state and a candidate family of measurements, the criterion enables one to certify that they will never lead to nonlocal correlations. The idea behind our result follows the lines of Werner and Wolf's criterion for the separability of Gaussian states [24]. Furthermore, we provide an interesting interpretation in terms of the role of noise for the vanishing of nonlocality, separating the inherent quantum noise resulting from the uncertainty relations from additional classical Gaussian noise. Before presenting our main result, we review some elements of the theory of bosonic systems and nonlocality.

Bosonic systems and Bell nonlocality.—A bosonic system [23] is described by N modes, where each mode is associated with an infinite-dimensional Hilbert space and a pair of bosonic field operators $\hat{a}_k, \hat{a}_k^\dagger$, where $k = 1, \ldots, N$ denotes the mode. The total system Hilbert space is the tensor product over the modes. The field operators satisfy the bosonic commutation relations $[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}$, $[\hat{a}_i, \hat{a}_j] = 0$, $[\hat{a}_i^\dagger, \hat{a}_j^\dagger] = 0$. Alternatively, the system can be described using the quadrature operators $\{\hat{q}_k, \hat{p}_k\}_{k=1}^N$ defined as $\hat{q}_k \coloneqq \hat{a}_k + \hat{a}_k^\dagger$, $\hat{p}_k \coloneqq i(\hat{a}_k^\dagger - \hat{a}_k)$ (we take $\hbar = 2$ throughout), which can also be arranged in the vector $\hat{\boldsymbol{r}} \coloneqq (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_N, \hat{p}_N)^{\mathrm{T}}$. The quadratures satisfy $[\hat{r}_k, \hat{r}_l] = 2i\Omega_{kl}$, where $\boldsymbol{\Omega} \coloneqq \bigoplus_{k=1}^N \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is the symplectic form.

Any positive Hermitian operator in state space can equivalently be completely described by its real-valued Wigner function in phase space. If the operator is of unit trace (e.g., the density matrix ρ of a quantum state), its Wigner function integrates to unity. Two quantities of particular interest are the two first statistical moments: the mean of the quadratures $\bar{\boldsymbol{r}} \coloneqq \mathrm{Tr}[\hat{\boldsymbol{r}}\hat{\rho}]$ and the covariance matrix $\boldsymbol{V}$ with $V_{ij} \coloneqq \mathrm{Tr}[\{\Delta\hat{r}_i, \Delta\hat{r}_j\}\hat{\rho}]/2$, where $\Delta\hat{r}_i \coloneqq \hat{r}_i - \bar{r}_i$ and $\{\cdot,\cdot\}$ is the anticommutator. Whenever ρ is a genuine quantum state, the $2N \times 2N$ real, symmetric covariance matrix satisfies the uncertainty principle $\boldsymbol{V} + i\boldsymbol{\Omega} \geq 0$, which also implies $\boldsymbol{V} \geq 0$.

As already mentioned, Gaussian states [39] are ubiquitous in quantum experiments. These are states whose Wigner function is a multivariate Gaussian distribution. As such, they are completely described by their first two statistical moments, and their Wigner function can be written as

$$W(\boldsymbol{r}) = \frac{1}{(2\pi)^N \sqrt{\det \boldsymbol{V}}} e^{-\frac{1}{2}(\boldsymbol{r}-\bar{\boldsymbol{r}})^{\mathrm{T}} \boldsymbol{V}^{-1} (\boldsymbol{r}-\bar{\boldsymbol{r}})}. \tag{1}$$

The entanglement in a Gaussian state is determined by its covariance matrix alone. A bipartite Gaussian state with covariance matrix V_{AB} will be separable if and only if there exist genuine covariance matrices $\boldsymbol{\gamma}_A$ and $\boldsymbol{\gamma}_B$ of parties A and B such that $\boldsymbol{V} \geq \boldsymbol{\gamma}_A \oplus \boldsymbol{\gamma}_B$ [24].

A stronger form of correlations, Bell nonlocality is defined at the level of the observed input-output distribution in an experiment with multiple observers. In particular, a bipartite experiment with observers A and B is characterized by the distribution $p(ab|xy)$, where x, y label the choice of input (measurement setting) of A and B, respectively, and a, b label their outputs (measurement outcomes). The distribution is called nonlocal if it does not admit an LHV model, i.e., if it cannot be written as

$$p(ab|xy) = \int d\lambda q(\lambda) p(a|x,\lambda) p(b|y,\lambda), \tag{2}$$

where the integral is over the (hidden) variable λ, which is distributed according to a probability density $q(\lambda)$ and where $p(a|x,\lambda)$ and $p(b|y,\lambda)$ are local response functions.

Entanglement is necessary but not sufficient for the generation of nonlocal correlations [6]. In a general bipartite quantum experiment, A and B share a state $\hat{\rho}_{AB}$ and each perform a generalized measurement with positive-operator-valued-measure (POVM) elements $Q_{a|x}$ and $R_{b|y}$, respectively. The corresponding probabilities are $p(ab|xy) = \mathrm{Tr}[\hat{\rho}_{AB} Q_{a|x} \otimes R_{b|y}]$. If the quantum state and all the POVM elements have positive Wigner functions, $p(ab|xy)$ is necessarily local. Indeed, if $\hat{\rho}_{AB}$, $Q_{a|x}$, and $R_{b|y}$ have respective Wigner functions W, $\mathcal{Q}_{a|x}$, and $\mathcal{R}_{b|y}$, we have

$$p(ab|xy) = \int d\boldsymbol{r} W(\boldsymbol{r}) \frac{\mathcal{Q}_{a|x}(\boldsymbol{r}_A)}{(4\pi)^{-N_A}} \frac{\mathcal{R}_{b|y}(\boldsymbol{r}_B)}{(4\pi)^{-N_B}}, \tag{3}$$

with $\boldsymbol{r} = (\boldsymbol{r}_A, \boldsymbol{r}_B)$, where $\boldsymbol{r}_A$ and $\boldsymbol{r}_B$ are the phase-space variables and N_A and N_B are the number of modes of party A and B, respectively. This can be understood as an LHV model (2) with $\boldsymbol{r}$ as the hidden variable. W is normalized and is hence a probability density over $\boldsymbol{r}$. Since $\sum_a Q_{a|x} = \mathbb{I}$, with $\mathbb{I}$ the identity operator, the Wigner functions fulfill $\sum_a \mathcal{Q}_{a|x}(\boldsymbol{r}_A) = (4\pi)^{-N_A}$ for all x and $\boldsymbol{r}_A$, because the Wigner function of the identity on N modes is the constant $(4\pi)^{-N}$ in our convention and similarly for $\mathcal{R}_{b|y}$. It follows that the last two terms in (3) are probability distributions over a and b, respectively, and can be interpreted as local response functions. Hence (3) is of the form (2). An immediate consequence is that correlations obtained by Gaussian measurements on a Gaussian state will never be nonlocal.

Constructing the LHV model.—We denote by $\mathcal{G}_{\bar{\boldsymbol{s}},\gamma}$ the multivariate Gaussian distribution with mean $\bar{\boldsymbol{s}}$ and covariance matrix γ, and by $f \circ g$ the convolution of functions f and g, which is defined as

$$(f \circ g)(\boldsymbol{r}) \coloneqq \int d\boldsymbol{r}' f(\boldsymbol{r}') g(\boldsymbol{r} - \boldsymbol{r}'). \tag{4}$$

We also define $\boldsymbol{0} \coloneqq (0, \ldots, 0)^{\mathrm{T}}$. The following statement provides a sufficient criterion for the existence of LHV models for Gaussian states subject to specific measurements.

Theorem 1.—Let $\bar{\boldsymbol{r}}$ be the mean and $\boldsymbol{V}$ the covariance matrix of a Gaussian state $\hat{\rho}_{AB}$ and let $\mathcal{Q}_{a|x}$ and $\mathcal{R}_{b|y}$ be the Wigner functions of the POVM elements $Q_{a|x}$ and $R_{b|y}$. If there exist matrices $\gamma_A \geq 0$ and $\gamma_B \geq 0$ such that

$$\boldsymbol{V} \geq \gamma_A \oplus \gamma_B, \tag{5}$$

and

$$\mathcal{Q}_{a|x} \circ \mathcal{G}_{\boldsymbol{0},\gamma_A} \geq 0 \quad \text{and} \quad \mathcal{R}_{b|y} \circ \mathcal{G}_{\boldsymbol{0},\gamma_B} \geq 0, \tag{6}$$

for all a, x and b, y, then the probabilities $p(ab|xy) = \mathrm{Tr}[\hat{\rho}_{AB} Q_{a|x} \otimes R_{b|y}]$ exhibit an LHV model.

Proof.—Let $\omega = \boldsymbol{V} - \gamma_A \oplus \gamma_B \geq 0$. Since $\gamma_A \geq 0$ and $\gamma_B \geq 0$, one can define genuine Gaussian probability distributions $\mathcal{G}_{\mathbf{0},\gamma_A}$ and $\mathcal{G}_{\mathbf{0},\gamma_B}$, and similarly for $\mathcal{G}_{\bar{\boldsymbol{r}},\omega}$. A useful property of Gaussian distributions is that convolving two such distributions results in a Gaussian distribution, i.e., $\mathcal{G}_{\bar{\boldsymbol{s}}_1,\gamma_1} \circ \mathcal{G}_{\bar{\boldsymbol{s}}_2,\gamma_2} = \mathcal{G}_{\bar{\boldsymbol{s}},\gamma}$, with $\bar{\boldsymbol{s}} = \bar{\boldsymbol{s}}_1 + \bar{\boldsymbol{s}}_2$ and $\gamma = \gamma_1 + \gamma_2$. Exploiting this and the symmetries of Gaussian distributions, we have

$$\begin{aligned} p(ab|xy) &= (4\pi)^N \int d\boldsymbol{r}_A d\boldsymbol{r}_B \mathcal{G}_{\bar{\boldsymbol{r}},\boldsymbol{V}}(\boldsymbol{r}_A, \boldsymbol{r}_B) \mathcal{Q}_{a|x}(\boldsymbol{r}_A) \mathcal{R}_{b|y}(\boldsymbol{r}_B) \\ &= (4\pi)^N \int d\boldsymbol{r}_A d\boldsymbol{r}_B \int d\boldsymbol{r}'_A d\boldsymbol{r}'_B \mathcal{G}_{\bar{\boldsymbol{r}},\omega}(\boldsymbol{r}'_A, \boldsymbol{r}'_B) \mathcal{G}_{\mathbf{0},\gamma_A\oplus\gamma_B}(\boldsymbol{r}_A - \boldsymbol{r}'_A, \boldsymbol{r}_B - \boldsymbol{r}'_B) \mathcal{Q}_{a|x}(\boldsymbol{r}_A) \mathcal{R}_{b|y}(\boldsymbol{r}_B) \\ &= (4\pi)^N \int d\boldsymbol{r}'_A d\boldsymbol{r}'_B \mathcal{G}_{\bar{\boldsymbol{r}},\omega}(\boldsymbol{r}'_A, \boldsymbol{r}'_B) \int d\boldsymbol{r}_A d\boldsymbol{r}_B \mathcal{G}_{\mathbf{0},\gamma_A\oplus\gamma_B}(\boldsymbol{r}'_A - \boldsymbol{r}_A, \boldsymbol{r}'_B - \boldsymbol{r}_B) \mathcal{Q}_{a|x}(\boldsymbol{r}_A) \mathcal{R}_{b|y}(\boldsymbol{r}_B) \\ &= \int d\boldsymbol{r}_A d\boldsymbol{r}_B \mathcal{G}_{\bar{\boldsymbol{r}},\omega}(\boldsymbol{r}_A, \boldsymbol{r}_B) \frac{\tilde{\mathcal{Q}}_{a|x}(\boldsymbol{r}_A)}{(4\pi)^{-N_A}} \frac{\tilde{\mathcal{R}}_{b|y}(\boldsymbol{r}_B)}{(4\pi)^{-N_B}}, \end{aligned} \tag{7}$$

where $\tilde{\mathcal{Q}}_{a|x} \coloneqq \mathcal{Q}_{a|x} \circ \mathcal{G}_{\mathbf{0},\gamma_A} \geq 0$, $\tilde{\mathcal{R}}_{b|y} \coloneqq \mathcal{R}_{b|y} \circ \mathcal{G}_{\mathbf{0},\gamma_B} \geq 0$. Since for the constant distribution $c = (4\pi)^{-N_A}$, it holds that $c \circ \mathcal{G}_{\mathbf{0},\gamma_A} = c$, we also have that $(4\pi)^{N_A} \sum_a \tilde{\mathcal{Q}}_{a|x} = 1$, and similarly for $\tilde{\mathcal{R}}_{b|y}$. Equation (7) can therefore be interpreted as an LHV model. ■

An important point of Theorem 1 is that γ_A and γ_B need not be covariance matrices of genuine quantum states and only have to be non-negative. It is instructive to have a closer look at the situation when the state $\hat{\rho}_{AB}$ is separable. In that case, there exist covariance matrices γ_A and γ_B of quantum states (i.e., which satisfy the uncertainty principle), such that $\boldsymbol{V} \geq \gamma_A \oplus \gamma_B$ [24], so that

$$\begin{aligned} \tilde{\mathcal{Q}}_{a|x}(\boldsymbol{r}_A) &= \int d\boldsymbol{s}_A \mathcal{Q}_{a|x}(\boldsymbol{s}_A) \mathcal{G}_{\mathbf{0},\gamma_A}(\boldsymbol{r}_A - \boldsymbol{s}_A) \\ &= \int d\boldsymbol{s}_A \mathcal{Q}_{a|x}(\boldsymbol{s}_A) \mathcal{G}_{\boldsymbol{r}_A,\gamma_A}(\boldsymbol{s}_A) \\ &= (4\pi)^{-N_A} \mathrm{Tr}[Q_{a|x} \hat{\sigma}_A], \end{aligned} \tag{8}$$

where $\hat{\sigma}_A$ is the density matrix of the Gaussian state with mean value $\boldsymbol{r}_A$ and covariance matrix γ_A. Since $\hat{\sigma}_A$ is a genuine density matrix, we have that $\tilde{\mathcal{Q}}_{a|x}(\boldsymbol{r}_A) \geq 0$ for all $\boldsymbol{r}_A$. The same reasoning can, of course, be made for party B. We therefore see that, when $\hat{\rho}_{AB}$ is separable, we are always provided with an LHV model whatever the measurements, as should indeed be the case.

In fact, while the Wigner functions $\tilde{\mathcal{Q}}_{a|x}$ and $\tilde{\mathcal{R}}_{b|y}$ will always become positive when subject to enough noise (that is, noise coming from a separable state $\hat{\rho}_{AB}$), one can push the analysis further. Consider the bivariate convolution $\tilde{\mathcal{Q}}^{(t)}_{a|x} \coloneqq \mathcal{Q}_{a|x} \circ \mathcal{G}_{\mathbf{0},\gamma_A}$ with the choice $\gamma_A = t\mathbb{I}_2$, for some $t \geq 0$, where $\mathbb{I}_2$ is the 2×2 identity matrix. It is well known that the function $\tilde{\mathcal{Q}}^{(t)}_{a|x}$ then satisfies the heat (or diffusion) equation [40]

$$\frac{\partial}{\partial t} \tilde{\mathcal{Q}}^{(t)}_{a|x} = \frac{1}{2} \Delta \tilde{\mathcal{Q}}^{(t)}_{a|x}, \tag{9}$$

where Δ is the Laplacian, with initial condition $\tilde{\mathcal{Q}}^{(0)}_{a|x} = \mathcal{Q}_{a|x}$. In the limit of $t \to \infty$, the function $\tilde{\mathcal{Q}}^{(t)}_{a|x}$ approaches a Gaussian, which is necessarily non-negative everywhere. The convolution $\mathcal{Q}_{a|x} \circ \mathcal{G}_{\mathbf{0},\gamma_A}$ actually always makes the quasiprobability distribution $\mathcal{Q}_{a|x}$ "less negative" as the parameter t increases. More precisely, the local minima of $\tilde{\mathcal{Q}}^{(t)}_{a|x}$ have non-negative Laplacian, which implies from the heat equation (9) that their t derivative is non-negative, so that their values never decrease when t increases.

One can give an operational interpretation of Theorem 1 in terms of the effect that added local Gaussian noise has on nonlocality. Consider a bipartite pure Gaussian state $\hat{\rho}_{AB}$ with covariance matrix $\boldsymbol{V}$ and suppose it can be written as $\boldsymbol{V} = \omega + \gamma_A^{\mathrm{q}} \oplus \gamma_B^{\mathrm{q}}$ with $\omega, \gamma_A^{\mathrm{q}}, \gamma_B^{\mathrm{q}} \geq 0$ (where q is for quantum). Suppose further that we apply local noise to $\hat{\rho}_{AB}$ in the form of classical additive Gaussian noise channels [23], i.e., local quantum convolutions in the sense of Ref. [41]. These channels are completely characterized by their action on the covariance matrix, which is of the form $\boldsymbol{V} \mapsto \boldsymbol{V} + \gamma_A^{\mathrm{c}} \oplus \gamma_B^{\mathrm{c}}$ with $\gamma_A^{\mathrm{c}}, \gamma_B^{\mathrm{c}} \geq 0$ (where c is for classical). The resulting mixed Gaussian state $\hat{\rho}'_{AB}$ has covariance matrix $\omega + (\gamma_A^{\mathrm{q}} + \gamma_A^{\mathrm{c}}) \oplus (\gamma_B^{\mathrm{q}} + \gamma_B^{\mathrm{c}})$. Now apply Theorem 1 to $\hat{\rho}'_{AB}$ with the POVM elements $Q_{a|x}$ and $R_{b|y}$. An LHV model will exist if

$$\mathcal{Q}_{a|x} \circ \mathcal{G}_{\mathbf{0},\gamma_A^{\mathrm{q}}+\gamma_A^{\mathrm{c}}} \geq 0 \quad \text{and} \quad \mathcal{R}_{b|y} \circ \mathcal{G}_{\mathbf{0},\gamma_B^{\mathrm{q}}+\gamma_B^{\mathrm{c}}} \geq 0, \tag{10}$$

for all a, x and b, y. Equation (10) expresses the fact that $\hat{\rho}'_{AB}$ will become local with respect to the POVMs $Q_{a|x}$ and $R_{b|y}$ when the noise provided by the convolutions with the Gaussian distributions $\mathcal{G}_{\mathbf{0},\gamma_A^{\mathrm{q}}+\gamma_A^{\mathrm{c}}}$ and $\mathcal{G}_{\mathbf{0},\gamma_B^{\mathrm{q}}+\gamma_B^{\mathrm{c}}}$ is important enough. There are two contributions to the noise. The first, characterized by γ_A^{q} and γ_B^{q}, is quantum noise; that is, the uncertainty inherent to quantum mechanics coming from the fact that the pure state $\hat{\rho}_{AB}$ is subject to the uncertainty relation. The second, characterized by γ_A^{c} and γ_B^{c}, is classical Gaussian additive noise making the state mixed. An interesting situation arises when either $\gamma_A^{\mathrm{q}}+\gamma_A^{\mathrm{c}}$ or $\gamma_B^{\mathrm{q}}+\gamma_B^{\mathrm{c}}$ is not a genuine covariance matrix, so that $\hat{\rho}'_{AB}$ is still entangled, while the noise is important enough so that there exists an LHV model. We provide an example of this in the following.

An application.—For the sake of illustration, we consider a two-mode squeezed state (TMSS) $\hat{\rho}_{AB}$ with zero mean and covariance matrix

$$\boldsymbol{V} = \begin{pmatrix} \nu\mathbb{I}_2 & \sqrt{\nu^2-1}\boldsymbol{Z} \\ \sqrt{\nu^2-1}\boldsymbol{Z} & \nu\mathbb{I}_2 \end{pmatrix}, \tag{11}$$

where $\nu \geq 1$ and $\boldsymbol{Z} \coloneqq \mathrm{diag}(1,-1)$. It is entangled for $\nu > 1$. We consider a scheme similar to that of Ref. [34] for demonstrating nonlocality with a TMSS (see Fig. 1). First, we take losses into account by applying a local pure-loss channel [23] $\mathcal{E}_\eta$ of parameter $\eta \in [0,1]$ to each mode of the TMSS. The channel $\mathcal{E}_\eta$ acts as

$$\mathcal{E}_\eta[\sigma] \coloneqq \mathrm{Tr}_2[U_\eta(\sigma \otimes |0\rangle\langle 0|)U_\eta^\dagger], \tag{12}$$

where U_η is a beam-splitter unitary and $|0\rangle$ is the vacuum state. Since $\mathcal{E}_\eta$ is Gaussian, the resulting state $\hat{\rho}'_{AB} = (\mathcal{E}_\eta \otimes \mathcal{E}_\eta)[\hat{\rho}_{AB}]$ is also Gaussian with zero mean value and covariance matrix

$$\boldsymbol{V}' = \begin{pmatrix} [1+\eta(\nu-1)]\mathbb{I}_2 & \eta\sqrt{\nu^2-1}\boldsymbol{Z} \\ \eta\sqrt{\nu^2-1}\boldsymbol{Z} & [1+\eta(\nu-1)]\mathbb{I}_2 \end{pmatrix}. \tag{13}$$

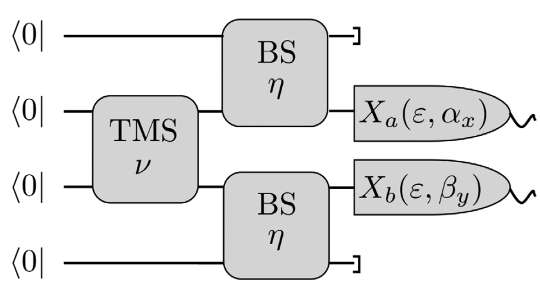

FIG. 1. Sketch of a scheme for demonstrating nonlocality from a TMSS with loss. A TMSS is generated by injecting a couple of vacua into a two-mode squeezer (TMS) of parameter ν, while losses are modeled by the interaction of each output mode of the TMS with a vacuum state through a beam splitter (BS) of transmittance η. The measurements characterized by the POVM elements $X_a(\varepsilon,\alpha_x)$ and $X_b(\varepsilon,\beta_y)$ are then performed on party A and B, respectively.

Furthermore, it can be seen to be entangled for any $\nu > 1$ and $\eta > 0$ by evaluating the partial transpose [25,42,43].

Next, for the measurements we consider displacements followed by non-number-resolving single-photon detection (click or no click). Ideally, this implements a measurement where the no-click outcome corresponds to a projection onto a coherent state. Here, we allow for some noise in the detection by modeling the POVM element corresponding to the no-click outcome as $X_{+1}(\varepsilon,\alpha) \coloneqq D_\alpha[(1-\varepsilon)|0\rangle\langle 0| + \varepsilon|1\rangle\langle 1|]D_\alpha^\dagger$, where D_α is the displacement operator and $|1\rangle$ is the one-photon Fock state. The click outcome corresponds to $X_{-1}(\varepsilon,\alpha) \coloneqq \mathbb{I} - X_{+1}(\varepsilon,\alpha)$. The parameter $\varepsilon \in [0,1]$ can be understood as the probability for an additional excitation to be introduced during measurement.

Inputs $x, y \in \{0,1\}$ for A and B correspond to displacements α_x and β_y, respectively, and we label the outputs $a, b \in \{\pm 1\}$, with -1 for click events. We take the noise strength ε to be the same for all measurements. Defining the correlators $\langle a_x b_y\rangle = \sum_{a,b} ab\, p(ab|xy)$, Eq. (2) implies the Clauser-Horne-Shimony-Holt (CHSH) inequality [44]

$$S = \langle a_0 b_0\rangle + \langle a_0 b_1\rangle + \langle a_1 b_0\rangle - \langle a_1 b_1\rangle \leq 2. \tag{14}$$

This inequality can be violated for the quantum probabilities $p(ab|xy) = \mathrm{Tr}[\hat{\rho}'_{AB}(X_a(\varepsilon,\alpha_x) \otimes X_b(\varepsilon,\beta_y))]$. In particular, taking $\beta_y = -\alpha_x$ for $y = x$ and optimizing over real α_x, we find violation for a range of values of the squeezing, loss, and noise, as shown in Fig. 2. To do so, we fix $\varepsilon = 0.02$ as an example, before numerically maximizing the value of S in Eq. (14) over the free parameters $\alpha_0, \alpha_1 \in [-1,1]$, for each value of $\eta \in [0,1]$ and $\nu \in [1, 1.5]$, after a suitable discretization. For instance, if one chooses $\eta = 0.95$ and $\nu = 1.4$, one gets $S \simeq 2.1 > 2$ for $(\alpha_0, \alpha_1) \simeq (0.12, -0.48)$.

On the other hand, we can apply Theorem 1 to show that the correlations must be local for another parameter region. Let $\mathcal{X}_a^{(\varepsilon,\alpha)}$ be the Wigner function of $X_a(\varepsilon,\alpha)$. The quasidistribution $\mathcal{X}_{+1}^{(\varepsilon,\alpha)}$ is non-negative everywhere since $\varepsilon < 1$, while $\mathcal{X}_{-1}^{(\varepsilon,\alpha)}$ admits negative values. According to Theorem 1, the probability $p(ab|xy)$ will satisfy Eq. (2) if there exist non-negative matrices γ_A and γ_B such that $\boldsymbol{V}' \geq \gamma_A \oplus \gamma_B$ and the Wigner functions $\mathcal{X}_a^{(\varepsilon,\alpha_x)} \circ \mathcal{G}_{\mathbf{0},\gamma_A}$ and $\mathcal{X}_b^{(\varepsilon,\beta_y)} \circ \mathcal{G}_{\mathbf{0},\gamma_B}$ are non-negative for all a, b. It is enough to find γ_A and γ_B such that $\mathcal{X}_{-1}^{(\varepsilon,\alpha_x)} \circ \mathcal{G}_{\mathbf{0},\gamma_A} \geq 0$ and $\mathcal{X}_{-1}^{(\varepsilon,\beta_y)} \circ \mathcal{G}_{\mathbf{0},\gamma_B} \geq 0$. Now, consider the choice $\gamma_A = \gamma_B = t\mathbb{I}_2$ with $t \geq 0$. If we are to satisfy $\boldsymbol{V}' \geq \gamma_A \oplus \gamma_B$, we need $t \leq 1 + \eta(\nu - 1 - \sqrt{\nu^2-1})$. From Eq. (9), it follows that if $\mathcal{X}_{-1}^{(\varepsilon,\alpha)} \circ \mathcal{G}_{\mathbf{0},t\mathbb{I}_2}$ becomes non-negative for some value of t, it will remain so for all larger t. Consequently, one can consider the highest acceptable value of t, that is $t = 1 + \eta(\nu - 1 - \sqrt{\nu^2-1})$. Furthermore, by definition of the convolution, the value of t for which $\mathcal{X}_{-1}^{(\varepsilon,\alpha)} \circ \mathcal{G}_{\mathbf{0},t\mathbb{I}_2}$ becomes non-negative does not

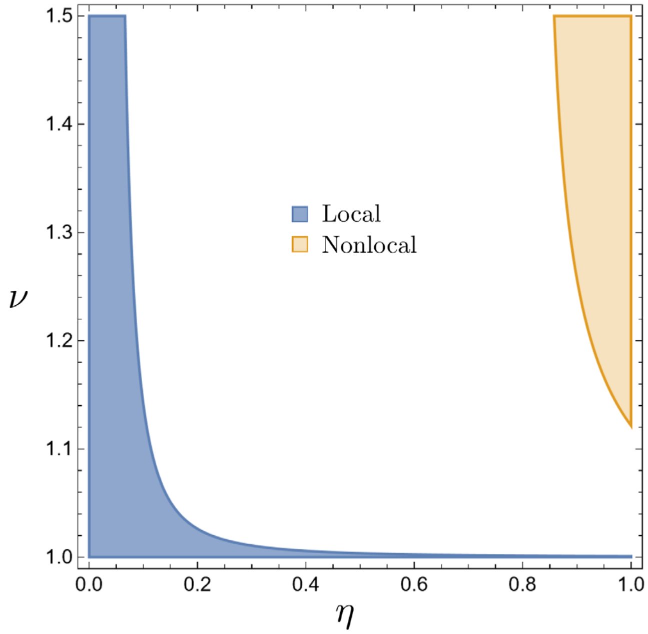

FIG. 2. Comparisons of regions for which the lossy TMSS $\hat{\rho}'_{AB}$ admits an LHV model for the choice of measurements $\{X_{+1}(\varepsilon,\alpha), X_{-1}(\varepsilon,\alpha)\}$ (blue region, left) and for which it violates the CHSH inequality (orange region, right), for the choice $\varepsilon = 0.02$. Note that we limited the figures to values $\nu \in [1, 1.5]$ as this is where a significant violation of the CHSH inequality occurs, but the region of existence of LHV models extends further when increasing the range of values of ν.

depend on α, so that one can take $\alpha = 0$. Now, the Wigner functions of the operators $\mathbb{I}$, $|0\rangle\langle 0|$, and $|1\rangle\langle 1|$ are, respectively, given by $W_{\mathbb{I}}(x,p) = 1/(4\pi)$, $W_{|0\rangle\langle 0|}(x,p) = e^{(x^2+p^2)/2}/(2\pi)$, and $W_{|1\rangle\langle 1|}(x,p) = -(1 - x^2 - p^2)e^{(x^2+p^2)/2}/(2\pi)$ [45], while we have $\mathcal{X}_{-1}^{(\varepsilon,\alpha)}(x,p) = W_{\mathbb{I}} - (1-\varepsilon)W_{|0\rangle\langle 0|}(x,p) - \varepsilon W_{|1\rangle\langle 1|}(x,p)$. Using this, we obtain

$$(\mathcal{X}_{-1}^{(\varepsilon,0)} \circ \mathcal{G}_{\mathbf{0},t\mathbb{I}_2})(x,p) = \frac{1}{4\pi} - \frac{(1+t)^2 + \varepsilon[x^2+p^2-2(1+t)]}{2\pi(1+t)^3} e^{\frac{-(x^2+p^2)}{2(1+t)}}. \quad (15)$$

It can easily be shown that, for all $t \geq 0$ and $(x,p) \in \mathbb{R}^2$, the above function achieves its minimum at $(x,p) = 0$, and that this minimum is non-negative for $t \geq \sqrt{1-4\varepsilon}$. From our choice of t, this means that the distribution will be non-negative everywhere for $1 + \eta(\nu - 1 - \sqrt{\nu^2 - 1}) \geq \sqrt{1-4\varepsilon}$. The corresponding region in the (η,ν)-plane is plotted in Fig. 2 for $\varepsilon = 0.02$. In this region, the entangled state $\hat{\rho}'_{AB}$ admits an LHV model for the family of measurements described above.

Conclusion.—In this Letter, we have developed a criterion for the existence of local-hidden-variable models for correlations resulting from general measurements on Gaussian states, by exploiting that measurement-operator Wigner functions can be made positive by passing Gaussian noise from the state to the measurement. We have illustrated the criterion for the case of noisy displacement-based measurements on a two-mode squeezed state subject to loss.

Recently, continuous-variables quantum systems have emerged as a promising platform for the implementation of QKD protocols [46–51]. In particular, Gaussian systems such as coherent states can serve as a resource for security against collective attacks [52,53]. In light of this, we expect the present Letter to also be useful in the context of DIQKD with Gaussian states.

An interesting question is whether the statement of Theorem 1 is also a necessary criterion: if one cannot find two positive semidefinite matrices γ_A and γ_B such that Eq. (6) is satisfied for all POVM elements simultaneously, does this imply nonlocality of the distribution $p(ab|xy) = \mathrm{Tr}[\hat{\rho}_{AB} Q_{a|x} \otimes R_{b|y}]$?

We gratefully acknowledge support from the Carlsberg Foundation CF19-0313, the Independent Research Fund Denmark 7027-00044B, and VILLUM FONDEN Grant No. 40864.

*mgija@dtu.dk
†jonatan.brask@fysik.dtu.dk

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).
[2] Richard Jozsa and Noah Linden, On the role of entanglement in quantum-computational speed-up, Proc. R. Soc. A **459**, 2011 (2003).
[3] Guifré Vidal, Efficient Classical Simulation of Slightly Entangled Quantum Computations, Phys. Rev. Lett. **91**, 147902 (2003).
[4] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone, Quantum Metrology, Phys. Rev. Lett. **96**, 010401 (2006).
[5] J. S. Bell, On the Einstein Podolsky Rosen paradox, Phys. Phys. Fiz. **1**, 195 (1964).
[6] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).
[7] Richard Cleve and Harry Buhrman, Substituting quantum entanglement for communication, Phys. Rev. A **56**, 1201 (1997).
[8] Toby S. Cubitt, Debbie Leung, William Matthews, and Andreas Winter, Zero-error channel capacity and simulation assisted by non-local correlations, IEEE Trans. Inf. Theory **57**, 5509 (2011).
[9] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. Thesis, University of Cambridge, 2009, arXiv:0911.3814.
[10] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).

[11] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[12] N. Gisin, Bell's inequality holds for all non-product states, Phys. Lett. A **154**, 201 (1991).

[13] Reinhard F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, Phys. Rev. A **40**, 4277 (1989).

[14] Jonathan Barrett, Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality, Phys. Rev. A **65**, 042302 (2002).

[15] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[16] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).

[17] Sandu Popescu, Bell's Inequalities Versus Teleportation: What is Nonlocality?, Phys. Rev. Lett. **72**, 797 (1994).

[18] Mafalda L. Almeida, Stefano Pironio, Jonathan Barrett, Géza Tóth, and Antonio Acín, Noise Robustness of the Nonlocality of Entangled Quantum States, Phys. Rev. Lett. **99**, 040403 (2007).

[19] D. Cavalcanti, L. Guerini, R. Rabelo, and P. Skrzypczyk, General Method for Constructing Local Hidden Variable Models for Entangled Quantum States, Phys. Rev. Lett. **117**, 190401 (2016).

[20] Flavien Hirsch, Marco Túlio Quintino, Tamás Vértesi, Matthew F. Pusey, and Nicolas Brunner, Algorithmic Construction of Local Hidden Variable Models for Entangled Quantum States, Phys. Rev. Lett. **117**, 190402 (2016).

[21] Joseph Bowles, Jérémie Francfort, Mathieu Fillettaz, Flavien Hirsch, and Nicolas Brunner, Genuinely Multipartite Entangled Quantum States with Fully Local Hidden Variable Models and Hidden Multipartite Nonlocality, Phys. Rev. Lett. **116**, 130401 (2016).

[22] Mathieu Fillettaz, Flavien Hirsch, Sébastien Designolle, and Nicolas Brunner, Algorithmic construction of local models for entangled quantum states: Optimization for two-qubit states, Phys. Rev. A **98**, 022115 (2018).

[23] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[24] R. F. Werner and M. M. Wolf, Bound Entangled Gaussian States, Phys. Rev. Lett. **86**, 3658 (2001).

[25] R. Simon, Peres-Horodecki Separability Criterion for Continuous Variable Systems, Phys. Rev. Lett. **84**, 2726 (2000).

[26] Konrad Banaszek and Krzysztof Wódkiewicz, Nonlocality of the Einstein-Podolsky-Rosen state in the Wigner representation, Phys. Rev. A **58**, 4345 (1998).

[27] Konrad Banaszek and Krzysztof Wódkiewicz, Testing Quantum Nonlocality in Phase Space, Phys. Rev. Lett. **82**, 2009 (1999).

[28] R. García-Patrón, J. Fiurášek, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and Ph. Grangier, Proposal for a Loophole-Free Bell Test Using Homodyne Detection, Phys. Rev. Lett. **93**, 130409 (2004).

[29] M. Revzen, P. A. Mello, A. Mann, and L. M. Johansen, Bell's inequality violation with non-negative Wigner functions, Phys. Rev. A **71**, 022103 (2005).

[30] E. G. Cavalcanti, C. J. Foster, M. D. Reid, and P. D. Drummond, Bell Inequalities for Continuous-Variable Correlations, Phys. Rev. Lett. **99**, 210405 (2007).

[31] Alejo Salles, Daniel Cavalcanti, and Antonio Acín, Quantum Nonlocality and Partial Transposition for Continuous-Variable Systems, Phys. Rev. Lett. **101**, 040404 (2008).

[32] Seung-Woo Lee, Hyunseok Jeong, and Dieter Jaksch, Testing quantum nonlocality by generalized quasiprobability functions, Phys. Rev. A **80**, 022104 (2009).

[33] Q. Y. He, E. G. Cavalcanti, M. D. Reid, and P. D. Drummond, Bell inequalities for continuous-variable measurements, Phys. Rev. A **81**, 062106 (2010).

[34] J. B. Brask and R. Chaves, Robust nonlocality tests with displacement-based measurements, Phys. Rev. A **86**, 010103(R) (2012).

[35] Victor Pozsgay, Flavien Hirsch, Cyril Branciard, and Nicolas Brunner, Covariance Bell inequalities, Phys. Rev. A **96**, 062128 (2017).

[36] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox, Phys. Rev. Lett. **98**, 140402 (2007).

[37] Hyunseok Jeong, Jinhyoung Lee, and M. S. Kim, Dynamics of nonlocality for a two-mode squeezed state in a thermal environment, Phys. Rev. A **61**, 052101 (2000).

[38] Ladislav Mišta, Radim Filip, and Jaromír Fiurášek, Continuous-variable Werner state: Separability, nonlocality, squeezing, and teleportation, Phys. Rev. A **65**, 062315 (2002).

[39] A. Holevo, Some statistical problems for quantum Gaussian states, IEEE Trans. Inf. Theory **21**, 533 (1975).

[40] J. Mathews and R. L. Walker, *Mathematical Methods of Physics*, Addison-Wesley World Student Series (W. A. Benjamin, New York, 1970).

[41] R. Werner, Quantum harmonic analysis on phase space, J. Math. Phys. (N.Y.) **25**, 1404 (1984).

[42] Asher Peres, Separability Criterion for Density Matrices, Phys. Rev. Lett. **77**, 1413 (1996).

[43] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki, Separability of mixed states: Necessary and sufficient conditions, Phys. Lett. A **223**, 1 (1996).

[44] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880 (1969).

[45] Ulf Leonhardt, *Essential Quantum Optics: From Quantum Measurements to Black Holes* (Cambridge University Press, Cambridge, England, 2010), 10.1017/CBO9780511806117.

[46] T. C. Ralph, Security of continuous-variable quantum cryptography, Phys. Rev. A **62**, 062306 (2000).

[47] Frédéric Grosshans and Philippe Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[48] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping

Koy Lam, Quantum Cryptography Without Switching, Phys. Rev. Lett. **93**, 170504 (2004).

[49] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photonics **7**, 378 (2013).

[50] Wei Ye, Hai Zhong, Xiaodong Wu, Liyun Hu, and Ying Guo, Continuous-variable measurement-device-independent quantum key distribution via quantum catalysis, Quantum Inf. Process. **19**, 346 (2020).

[51] Masoud Ghalaii and Stefano Pirandola, Continuous-variable measurement-device-independent quantum key distribution in free-space channels, arXiv:2212.06687.

[52] Frédéric Grosshans, Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution, Phys. Rev. Lett. **94**, 020504 (2005).

[53] R. Renner and J. I. Cirac, de finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography, Phys. Rev. Lett. **102**, 110504 (2009).