

Covariance matrices under Bell-like detections

Gaetana Spedalieri, Carlo Ottaviani, and Stefano Pirandola

Department of Computer Science, University of York, York YO10 5GH, United Kingdom

We derive a simple formula for the transformation of an arbitrary covariance matrix of $(n + 2)$ bosonic modes under general Bell-like detections, where the last two modes are combined in an arbitrary beam splitter (i.e., with arbitrary transmissivity) and then homodyned. In particular, we consider the realistic condition of non-unit quantum efficiency for the homodyne detectors. This formula can easily be specialized to describe the standard Bell measurement and the heterodyne detection, which are exploited in many contexts, including protocols of quantum teleportation, entanglement swapping and quantum cryptography. In its general form, our formula can be adopted to study quantum information protocols in the presence of experimental imperfections and asymmetric setups, e.g., deriving from the use of unbalanced beam splitters.

PACS numbers: 03.67.-a, 02.10.Ud, 03.65.Ta

I. INTRODUCTION

Gaussian quantum information is that area of quantum information which deals with continuous variable systems (e.g., bosonic systems) prepared in Gaussian states, evolving by Gaussian unitaries or channels, and finally measured by Gaussian detectors [1]. Gaussian states are easy to generate experimentally and very easy to manipulate theoretically. Their description can be reduced to their first two statistical moments, which are the mean value (or displacement vector) and the covariance matrix (CM). In particular, the CM contains the most relevant information about the Gaussian state, providing its entropy, purity properties and separability properties [1].

One of the most important Gaussian measurements is the Bell detection [1–3] (also known as continuous variable Bell detection). This consists of combining two bosonic modes into a balanced-beam splitter (i.e., with transmissivity $1/2$). The output modes are then measured by two homodyne detectors in such a way that one mode is detected in the position quadrature \hat{q} and the other mode in the momentum quadrature \hat{p} . This measurement is typical of a series of protocols with continuous variable systems, including quantum teleportation [4–10] and entanglement swapping [11–14]. Another important measurement is heterodyne detection, where a single bosonic mode is taken as input of a balanced-beam splitter (with the other input being the vacuum) and the two outputs are homodyned in \hat{q} and \hat{p} , respectively. This is also a fundamental detection in many continuous variable protocols, for instance in coherent-state quantum key distribution [15–18] and two-way quantum cryptography [19].

In this paper, we consider a generalized form of Bell measurement that we call “Bell-like detection”. Here we have two bosonic modes which are combined into a beam splitter of *arbitrary* transmissivity T and then homodyned in the two quadratures (one mode in \hat{q} and the other in \hat{p}). Standard Bell detection and heterodyne detection are specific instances of this more general measurement. In our derivation, we consider the

general scenario where a set of $n + 2$ bosonic modes is given in a Gaussian state with arbitrary CM. By applying the Bell-like detection to the last two modes of the set, we compute the conditional reduced CM of the first n modes surviving the measurement. This is expressed in terms of the input CM and the beam splitter’s transmissivity T adopted in the measurement. We derive this input-output formula both in the ideal case of perfect detection, i.e., unit quantum efficiency for the homodyne detectors, and the realistic case where detection is not necessarily perfect, i.e., the homodyne detectors have arbitrary quantum efficiency $0 < \eta \leq 1$ (a scenario which can be modelled by inserting additional beam splitters in front of the detectors [20]).

Our algebraic derivation is relatively easy starting from the well-known transformation rules for CMs under partial homodyne detections [21, 22], which are here suitably generalized to the case of arbitrary quantum efficiency η . Despite its easy derivation, our main formula for Bell-like detections can be usefully applied in several contexts. For instance, it can be exploited to extend the protocols of quantum teleportation and entanglement swapping to considering unbalanced beam splitters (asymmetric setups). Similarly, it can be used to perturb the ideal model of heterodyne detection which is used in many protocols of quantum key distribution.

The paper is organized as follows. In Sec. II we provide a brief introduction to bosonic Gaussian states and CMs. In Sec. III we review the transformation rules for CMs under homodyne detections, generalizing these well-known rules to the case of arbitrary quantum efficiency. Then, in Sec. IV, we derive the main result of the paper, i.e., the formula for the transformation of CMs under general Bell-like detections, which is first given in the ideal case of unit efficiency and, then, in the general scenario of arbitrary quantum efficiency for the homodyne detectors. Finally, Sec. V is for conclusions, with Appendix A showing specific examples of application of our results to the cases of standard Bell detection and heterodyne detection.

II. BASIC NOTIONS ON BOSONIC GAUSSIAN STATES

A system of n bosonic modes is described by a vector of $2n$ quadrature operators

$$\hat{\mathbf{x}}^T := (\hat{q}_1, \hat{p}_1, \dots, \hat{q}_n, \hat{p}_n), \quad (1)$$

satisfying the commutation relations $[\hat{x}_i, \hat{x}_j] = 2i\Omega_{ij}^{(n)}$, where $\Omega_{ij}^{(n)}$ is the generic element of the n -mode symplectic form

$$\Omega^{(n)} = \bigoplus_{k=1}^n \Omega, \quad \Omega := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (2)$$

By definition, a quantum state ρ of n bosonic modes is said to be ‘‘Gaussian’’ when its phase-space Wigner function is Gaussian [1]. For this reason, a Gaussian state is fully characterized by its first and second-order statistical moments. These are the displacement vector

$$\bar{\mathbf{x}} := \text{Tr}(\hat{\mathbf{x}}\rho), \quad (3)$$

and the CM \mathbf{V} , with generic element

$$V_{ij} = \frac{1}{2} \text{Tr}(\{\hat{x}_i, \hat{x}_j\}\rho) - \bar{x}_i \bar{x}_j.$$

where $\{, \}$ denotes the anticommutator. By definition, the CM is a $2n \times 2n$ real and symmetric matrix. In order to be a quantum CM, it must also satisfy the uncertainty principle [23]

$$\mathbf{V} + i\Omega^{(n)} \geq 0, \quad (4)$$

or an equivalent set of bona-fide conditions (for instance, see Ref. [24] for the case of two-mode CMs). In particular, Eq. (4) implies the positivity definiteness

$$\mathbf{V} > 0. \quad (5)$$

The simplest Gaussian state is the vacuum state, which corresponds to $\bar{\mathbf{x}} = 0$ and $\mathbf{V} = \mathbf{I}$.

Once that a state is prepared in a Gaussian states, its evolution can be such to preserve its Gaussian statistics. This is the case of Gaussian unitaries, which are defined as those unitaries transforming Gaussian states into Gaussian states. At the level of the second-order moments, the action of a Gaussian unitary $\rho \rightarrow U\rho U^\dagger$ corresponds to the congruence transformation $\mathbf{V} \rightarrow \mathbf{S}\mathbf{V}\mathbf{S}^T$ where \mathbf{S} is a symplectic matrix, i.e., a matrix preserving the symplectic form $\mathbf{S}\Omega^{(n)}\mathbf{S}^T = \Omega^{(n)}$. A simple example is the beam splitter transformation. This is defined by the single-parameter symplectic matrix

$$\mathbf{K}(T) := \begin{pmatrix} \sqrt{T}\mathbf{I} & \sqrt{1-T}\mathbf{I} \\ -\sqrt{1-T}\mathbf{I} & \sqrt{T}\mathbf{I} \end{pmatrix}, \quad (6)$$

where \mathbf{I} is the 2×2 identity matrix and $0 \leq T \leq 1$ is the transmissivity of the beam splitter. In the Heisenberg

picture, the beam splitter corresponds to the following Bogoliubov transformation of the quadrature operators

$$\begin{pmatrix} \hat{q}_+ \\ \hat{p}_+ \\ \hat{q}_- \\ \hat{p}_- \end{pmatrix} = \mathbf{K}(T) \begin{pmatrix} \hat{q}_1 \\ \hat{p}_1 \\ \hat{q}_2 \\ \hat{p}_2 \end{pmatrix} = \begin{pmatrix} \sqrt{T}\hat{q}_1 + \sqrt{1-T}\hat{q}_2 \\ \sqrt{T}\hat{p}_1 + \sqrt{1-T}\hat{p}_2 \\ -\sqrt{1-T}\hat{q}_1 + \sqrt{T}\hat{q}_2 \\ -\sqrt{1-T}\hat{p}_1 + \sqrt{T}\hat{p}_2 \end{pmatrix}. \quad (7)$$

Finally, Gaussian measurements can be defined as those quantum measurements whose application to Gaussian states provides outcomes which are Gaussian distributed [1]. When a Gaussian measurement is performed on a subset of modes of a bosonic system prepared in a Gaussian state, then the reduced state of the surviving (non-measured) modes is a Gaussian state. At the level of the second-order moments, the CM of the final state is connected to the CM of the initial state. As an example, when we homodyne one mode of a set of n bosonic modes in a Gaussian state, the formula of the final CM has a remarkably easy formula [21, 22]. This is reviewed in the next section.

III. COVARIANCE MATRICES UNDER HOMODYNE DETECTIONS

A. Perfect homodyne detection

Let us consider $n + 1$ bosonic modes in a Gaussian state. This $(n + 1)$ -mode Gaussian state ρ_{in} has a CM that can be written in the blockform

$$\mathbf{V}_{in} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \quad (8)$$

where \mathbf{A} is the CM of the first n modes, \mathbf{B} is the CM of the last mode, and \mathbf{C} is a rectangular ($2n \times 2$) real matrix accounting for the cross correlations.

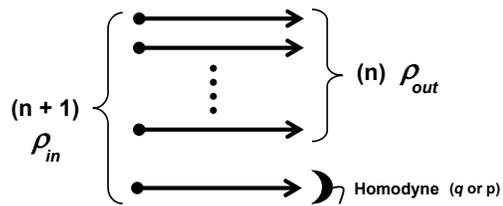


FIG. 1: An input Gaussian state ρ_{in} of $n + 1$ modes is homodyned in its last mode. The resulting output state ρ_{out} of the first n modes is Gaussian. The input and output CMs are related by Eq. (9) for \hat{q} -detection, and by Eq. (12) for \hat{p} -detection.

Now, let us homodyne the $(n + 1)^{\text{th}}$ mode as shown in Fig. 1, performing the detection of the \hat{q} quadrature. The output state ρ_{out} of the remaining n modes is still Gaussian. In particular, this n -mode Gaussian state is described by the following CM [21, 22]

$$\mathbf{V}_{out|q} = \mathbf{A} - \mathbf{C}(\mathbf{I}\mathbf{B}\mathbf{I})^{-1}\mathbf{C}^T, \quad (9)$$

where

$$\mathbf{\Pi} := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \quad (10)$$

If we detect the \hat{p} quadrature, we have to consider the replacement

$$\mathbf{\Pi} \rightarrow \mathbf{\Pi}' := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad (11)$$

so that the conditional output CM is given by

$$\mathbf{V}_{out|p} = \mathbf{A} - \mathbf{C}(\mathbf{\Pi}'\mathbf{B}\mathbf{\Pi}')^{-1}\mathbf{C}^T. \quad (12)$$

It is important to note that, in Eqs. (9) and (12), the matrices $\mathbf{\Pi B \Pi}$ and $\mathbf{\Pi' B \Pi'}$ are singular, so that $(\mathbf{\Pi B \Pi})^{-1}$ and $(\mathbf{\Pi' B \Pi'})^{-1}$ must be interpreted as pseudoinverses. In general, for a singular matrix \mathbf{M} , the pseudoinverse \mathbf{M}^{-1} (also known as Moore-Penrose inverse) is a matrix \mathbf{G} which minimizes the quantity

$$r := \sum_{ij} (\mathbf{H}_{ij})^2 \geq 0,$$

where \mathbf{H}_{ij} are the entries of $\mathbf{H} := \mathbf{M G} - \mathbf{I}$, with \mathbf{I} being the identity matrix.

In the present problem, the pseudoinverses are easy to compute. In fact, let us set

$$\mathbf{B} := \begin{pmatrix} b_1 & b_3 \\ b_3 & b_2 \end{pmatrix}, \quad (13)$$

where $b_1 > 0$ and $b_2 > 0$, since $\mathbf{B} > 0$ (being a reduced CM). Then, we have $\mathbf{\Pi B \Pi} = b_1 \mathbf{\Pi}$, and we can easily compute

$$(\mathbf{\Pi B \Pi})^{-1} = (b_1 \mathbf{\Pi})^{-1} = (b_1)^{-1} \mathbf{\Pi}. \quad (14)$$

This is a consequence of the fact we have $(x \mathbf{\Pi})^{-1} = x^{-1} \mathbf{\Pi}$ for any $x \neq 0$ [25]. Thus, for the \hat{q} -detection, we can write

$$\mathbf{V}_{out|q} = \mathbf{A} - (b_1)^{-1} \mathbf{C} \mathbf{\Pi} \mathbf{C}^T. \quad (15)$$

Similarly, for the detection of the other quadrature, we have $\mathbf{\Pi' B \Pi'} = b_2 \mathbf{\Pi}'$, so that

$$(\mathbf{\Pi' B \Pi'})^{-1} = (b_2)^{-1} \mathbf{\Pi}'. \quad (16)$$

Thus, the formula for the \hat{p} -detection is simply given by

$$\mathbf{V}_{out|p} = \mathbf{A} - (b_2)^{-1} \mathbf{C} \mathbf{\Pi}' \mathbf{C}^T. \quad (17)$$

B. Generalization to arbitrary quantum efficiency

Here we consider the case where the homodyne detector is not necessarily perfect, i.e., it has a quantum efficiency $0 < \eta \leq 1$. This is modelled by considering a beam-splitter with transmissivity η in front of the detector, where one port is accessed by the signal mode (the

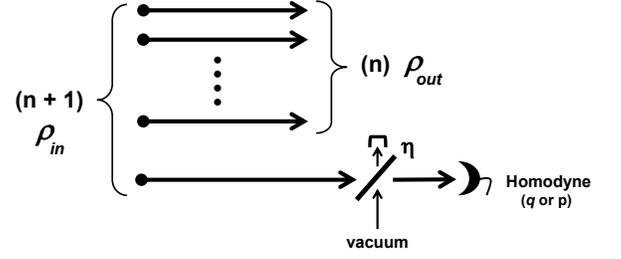


FIG. 2: An input Gaussian state ρ_{in} of $n + 1$ modes is homodyned in its last mode, with quantum efficiency $0 < \eta \leq 1$ (modelled as a beam splitter of transmissivity η which mixes the input signal mode with an environmental vacuum mode). The resulting output state ρ_{out} of the first n modes is Gaussian. The input and output CMs are related by Eq. (21) for \hat{q} -detection, and by Eq. (22) for \hat{p} -detection.

last mode of the bosonic input set) and the other port is accessed by an environmental vacuum mode. This scenario is depicted in Fig. 2

The generalization of the previous formulas is quite easy. The input CM is first dilated to include the vacuum, i.e., $\mathbf{V}_{in} \rightarrow \mathbf{V}' := \mathbf{V}_{in} \oplus \mathbf{I}$. Then, we apply the beam splitter matrix to the last two modes, i.e.,

$$\mathbf{V}' \rightarrow \mathbf{V}'' := [\mathbf{I}^{(n)} \oplus \mathbf{K}] \mathbf{V}' [\mathbf{I}^{(n)} \oplus \mathbf{K}]^T, \quad (18)$$

where $\mathbf{K} = \mathbf{K}(\eta)$ is given in Eq. (6), and

$$\mathbf{I}^{(n)} = \bigoplus_{k=1}^n \mathbf{I} \quad (19)$$

is the n -mode identity matrix ($2n \times 2n$). The next step is to trace out the transmission of the vacuum (i.e., the last output mode), which corresponds to delete the last two rows and columns of the CM \mathbf{V}'' . Thus, we have the following output CM for the $n + 1$ bosonic modes before detection

$$\mathbf{V}''' = \begin{pmatrix} \mathbf{A} & \sqrt{\eta} \mathbf{C} \\ \sqrt{\eta} \mathbf{C}^T & \eta \mathbf{B} + (1 - \eta) \mathbf{I} \end{pmatrix}. \quad (20)$$

Note that the block $\mathbf{B}(\eta) := \eta \mathbf{B} + (1 - \eta) \mathbf{I}$ is positive-definite since it is the reduced CM of the last signal mode after the beam-splitter. By expressing \mathbf{B} in the form of Eq. (13), the diagonal terms of $\mathbf{B}(\eta)$ can be written as $b_1(\eta) := \eta b_1 + 1 - \eta > 0$ and $b_2(\eta) := \eta b_2 + 1 - \eta > 0$.

Now, for \hat{q} -detection, we apply the formula of Eq. (15) to the CM of Eq. (20). This is equivalent to make the replacements $b_1 \rightarrow b_1(\eta)$ and $\mathbf{C} \rightarrow \sqrt{\eta} \mathbf{C}$ in Eq. (15). As a result, we get the final formula

$$\mathbf{V}_{out|q}(\eta) = \mathbf{A} - \left(b_1 + \frac{1 - \eta}{\eta} \right)^{-1} \mathbf{C} \mathbf{\Pi} \mathbf{C}^T, \quad (21)$$

for any quantum efficiency $0 < \eta \leq 1$. On the other hand, if we consider the \hat{p} -detection, we apply the formula of Eq. (17) with $b_2 \rightarrow b_2(\eta)$ and $\mathbf{C} \rightarrow \sqrt{\eta} \mathbf{C}$. Thus, we find

the other general formula

$$\mathbf{V}_{out|p}(\eta) = \mathbf{A} - \left(b_2 + \frac{1-\eta}{\eta} \right)^{-1} \mathbf{C} \mathbf{\Pi}' \mathbf{C}^T, \quad (22)$$

for any quantum efficiency $0 < \eta \leq 1$.

1. Example: Remote state preparation

As a simple example of application, we consider the remote state preparation which is typical in continuous variable quantum cryptography [1]. Alice has an Einstein-Podolsky-Rosen (EPR) state [26], which is a Gaussian state with zero mean and CM equal to

$$\mathbf{V}_{\text{EPR}} = \begin{pmatrix} \mu \mathbf{I} & \sqrt{\mu^2 - 1} \mathbf{Z} \\ \sqrt{\mu^2 - 1} \mathbf{Z} & \mu \mathbf{I} \end{pmatrix}, \quad (23)$$

with parameter $\mu \geq 1$ and

$$\mathbf{Z} := \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}. \quad (24)$$

Suppose that Alice measures the \hat{q} -quadrature of one mode with homodyne efficiency $0 < \eta \leq 1$. Then, the other mode is projected into a Gaussian state with CM

$$\mathbf{V}_{out|q}(\eta) = \mu \mathbf{I} - \frac{\mu^2 - 1}{\mu + \frac{1-\eta}{\eta}} \mathbf{\Pi} = \begin{pmatrix} \frac{\eta + (1-\eta)\mu}{\eta\mu + 1 - \eta} & \\ & \mu \end{pmatrix}. \quad (25)$$

In particular, for $\eta = 1/2$, we have

$$\mathbf{V}_{out|q}(\frac{1}{2}) = \begin{pmatrix} 1 & \\ & \mu \end{pmatrix}, \quad (26)$$

which is an asymmetric Gaussian state, with vacuum fluctuations in the \hat{q} -quadrature and thermal in the \hat{p} -quadrature. In the case of ideal detection $\eta = 1$, we have

$$\mathbf{V}_{out|q}(1) = \begin{pmatrix} \mu^{-1} & \\ & \mu \end{pmatrix}, \quad (27)$$

which is the CM of a position-squeezed pure state.

Similarly, if Alice detects the \hat{p} -quadrature, we have

$$\mathbf{V}_{out|p}(\eta) = \mu \mathbf{I} - \frac{\mu^2 - 1}{\mu + \frac{1-\eta}{\eta}} \mathbf{\Pi}' = \begin{pmatrix} \mu & \\ & \frac{\eta + (1-\eta)\mu}{\eta\mu + 1 - \eta} \end{pmatrix}. \quad (28)$$

For $\eta = 1/2$, Alice remotely prepares the other asymmetric Gaussian state

$$\mathbf{V}_{out|p}(\frac{1}{2}) = \begin{pmatrix} \mu & \\ & 1 \end{pmatrix}, \quad (29)$$

while for ideal detection $\eta = 1$, she remotely prepares a momentum-squeezed pure state

$$\mathbf{V}_{out|p}(1) = \begin{pmatrix} \mu & \\ & \mu^{-1} \end{pmatrix}. \quad (30)$$

IV. COVARIANCE MATRICES UNDER BELL-LIKE DETECTIONS

In this section we derive the transformation rule for the CM under generalized Bell-like detections, first assuming the condition of unit quantum efficiency for the homodyne detectors (Sec. IV A) and, then, the general case of arbitrary quantum efficiencies (Sec. IV B).

A. Ideal Bell-like measurements

As depicted in Fig. 3, let us consider $n + 2$ bosonic modes in a Gaussian state ρ_{in} . Its CM can always be written in the blockform

$$\mathbf{V}_{in} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B}^{(2)} \end{pmatrix}, \quad (31)$$

where \mathbf{A} is the reduced CM of the first n modes,

$$\mathbf{B}^{(2)} = \begin{pmatrix} \mathbf{B}_1 & \mathbf{D} \\ \mathbf{D}^T & \mathbf{B}_2 \end{pmatrix} \quad (32)$$

is the reduced CM of the last two modes (labelled by 1 and 2), and

$$\mathbf{C} = (\mathbf{C}_1 \ \mathbf{C}_2) = \begin{pmatrix} \vdots & \vdots \\ \mathbf{C}_1^k & \mathbf{C}_2^k \\ \vdots & \vdots \end{pmatrix}_{k=1,n} \quad (33)$$

is a rectangular ($2n \times 4$) real matrix, describing the correlations between the first n modes and the last two modes.

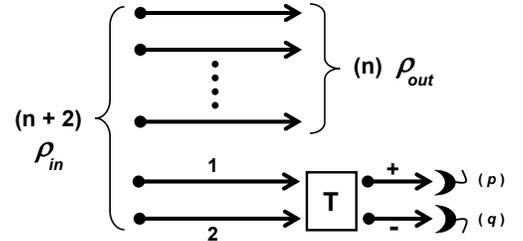


FIG. 3: An input Gaussian state ρ_{in} of $n+2$ modes is subject to an ideal Bell-like detection (with arbitrary transmissivity $0 \leq T \leq 1$) in the last two modes (labelled by 1 and 2). The output state ρ_{out} of the surviving n modes is Gaussian. The output CM \mathbf{V}_{out} is related to the input CM \mathbf{V}_{in} by Eq. (62).

Here, we consider an ideal Bell-like detection applied to the last two modes 1 and 2. This detection consists in applying a beam splitter of transmissivity T , which transforms the input modes 1 and 2 into the output modes “+” and “-”, followed by two conjugate (p - and q -) homodyne detections as shown in Fig. 3. Thus, as a first step, let us apply the beam-splitter symplectic matrix.

The $(n+2)$ -mode Gaussian state $\tilde{\rho}$ at the output of the beam splitter has CM

$$\tilde{\mathbf{V}} = [\mathbf{I}^{(n)} \oplus \mathbf{K}] \mathbf{V}_{in} [\mathbf{I}^{(n)} \oplus \mathbf{K}]^T, \quad (34)$$

where $\mathbf{I}^{(n)}$ is the n -mode identity matrix, and $\mathbf{K} = \mathbf{K}(T)$ is the beam-splitter matrix of Eq. (6) applied to the last two modes. This CM takes the blockform

$$\tilde{\mathbf{V}} = \begin{pmatrix} \mathbf{A} & \tilde{\mathbf{C}} \\ \tilde{\mathbf{C}}^T & \tilde{\mathbf{B}}^{(2)} \end{pmatrix}, \quad (35)$$

where

$$\tilde{\mathbf{C}} = \mathbf{C} \mathbf{K}^T, \quad (36)$$

and

$$\tilde{\mathbf{B}}^{(2)} = \mathbf{K} \mathbf{B}^{(2)} \mathbf{K}^T. \quad (37)$$

More explicitly, the various blocks of the previous CM have the following expressions

$$\tilde{\mathbf{C}} = (\tilde{\mathbf{C}}_1 \quad \tilde{\mathbf{C}}_2) = \begin{pmatrix} \vdots & \vdots \\ \tilde{\mathbf{C}}_1^k & \tilde{\mathbf{C}}_2^k \\ \vdots & \vdots \end{pmatrix}_{k=1,n}, \quad (38)$$

with

$$\tilde{\mathbf{C}}_1 = \sqrt{T} \mathbf{C}_1 + \sqrt{1-T} \mathbf{C}_2, \quad (39)$$

$$\tilde{\mathbf{C}}_2 = -\sqrt{1-T} \mathbf{C}_1 + \sqrt{T} \mathbf{C}_2, \quad (40)$$

and

$$\tilde{\mathbf{B}}^{(2)} = \begin{pmatrix} \tilde{\mathbf{B}}_1 & \tilde{\mathbf{D}} \\ \tilde{\mathbf{D}}^T & \tilde{\mathbf{B}}_2 \end{pmatrix}, \quad (41)$$

with

$$\tilde{\mathbf{B}}_1 = T \mathbf{B}_1 + (1-T) \mathbf{B}_2 + \sqrt{T(1-T)} (\mathbf{D} + \mathbf{D}^T), \quad (42)$$

$$\tilde{\mathbf{B}}_2 = T \mathbf{B}_2 + (1-T) \mathbf{B}_1 - \sqrt{T(1-T)} (\mathbf{D} + \mathbf{D}^T), \quad (43)$$

$$\tilde{\mathbf{D}} = \sqrt{T(1-T)} (\mathbf{B}_2 - \mathbf{B}_1) + T \mathbf{D} - (1-T) \mathbf{D}^T. \quad (44)$$

In terms of the previous blocks, the CM of Eq. (35) takes the more explicit form

$$\tilde{\mathbf{V}} = \begin{pmatrix} \mathbf{A} & \tilde{\mathbf{C}}_1 & \tilde{\mathbf{C}}_2 \\ \tilde{\mathbf{C}}_1^T & \tilde{\mathbf{B}}_1 & \tilde{\mathbf{D}} \\ \tilde{\mathbf{C}}_2^T & \tilde{\mathbf{D}}^T & \tilde{\mathbf{B}}_2 \end{pmatrix}. \quad (45)$$

As already said, this CM describes the Gaussian state after the action of the beam splitter which transforms the last two modes 1 and 2 into the output modes “+” and “-”.

Now, we apply the \hat{q} -detection on the last mode “-”, and the \hat{p} -detection on the next-to-last mode “+”. The

detection of \hat{q}_- implies the transformation of Eq. (9), which here reads

$$\begin{aligned} \tilde{\mathbf{V}} &\rightarrow \mathbf{V}' \\ &= \begin{pmatrix} \mathbf{A} & \tilde{\mathbf{C}}_1 \\ \tilde{\mathbf{C}}_1^T & \tilde{\mathbf{B}}_1 \end{pmatrix} - \begin{pmatrix} \tilde{\mathbf{C}}_2 \\ \tilde{\mathbf{D}} \end{pmatrix} \mathbf{\Gamma} (\tilde{\mathbf{C}}_2^T \quad \tilde{\mathbf{D}}^T), \end{aligned} \quad (46)$$

where

$$\mathbf{\Gamma} := (\mathbf{\Pi} \tilde{\mathbf{B}}_2 \mathbf{\Pi})^{-1}. \quad (47)$$

In other words, after the detection of “-”, the $(n+1)$ -mode CM describing the first n modes and mode “+” is given by

$$\mathbf{V}' = \begin{pmatrix} \mathbf{A}' & \mathbf{C}' \\ \mathbf{C}'^T & \mathbf{B}' \end{pmatrix}, \quad (48)$$

where

$$\mathbf{A}' = \mathbf{A} - \tilde{\mathbf{C}}_2 \mathbf{\Gamma} \tilde{\mathbf{C}}_2^T, \quad (49)$$

$$\mathbf{B}' = \tilde{\mathbf{B}}_1 - \tilde{\mathbf{D}} \mathbf{\Gamma} \tilde{\mathbf{D}}^T, \quad (50)$$

and

$$\mathbf{C}' = \tilde{\mathbf{C}}_1 - \tilde{\mathbf{C}}_2 \mathbf{\Gamma} \tilde{\mathbf{D}}^T. \quad (51)$$

Now, let us apply the \hat{p} -detection on mode “+”. By using Eq. (12), we get the final CM for the first n modes after the measurement, which is given by

$$\mathbf{V}' \rightarrow \mathbf{V}_{out} = \mathbf{A}' - \mathbf{C}' \mathbf{\Gamma}' \mathbf{C}'^T, \quad (52)$$

where

$$\mathbf{\Gamma}' := (\mathbf{\Pi}' \mathbf{B}' \mathbf{\Pi}')^{-1}. \quad (53)$$

1. Simplification of the input-output formula

Here we simplify the formula for the output CM given in Eq. (52). Let us explicitly write the reduced CM $\mathbf{B}^{(2)}$ of the detected modes by setting

$$\mathbf{B}_1 := \begin{pmatrix} \beta_1 & \beta_3 \\ \beta_3 & \beta_2 \end{pmatrix}, \quad \mathbf{B}_2 := \begin{pmatrix} \beta'_1 & \beta'_3 \\ \beta'_3 & \beta'_2 \end{pmatrix}, \quad (54)$$

$$\mathbf{D} := \begin{pmatrix} \delta_1 & \delta_3 \\ \delta_4 & \delta_2 \end{pmatrix}. \quad (55)$$

From these matrices, we can construct the following real symmetric matrix

$$\boldsymbol{\gamma} := \begin{pmatrix} \gamma_1 & \gamma_3 \\ \gamma_3 & \gamma_2 \end{pmatrix}, \quad (56)$$

where

$$\gamma_1 := (1-T)\beta_1 + T\beta'_1 - 2\sqrt{T(1-T)}\delta_1, \quad (57)$$

$$\gamma_2 := T\beta_2 + (1-T)\beta'_2 + 2\sqrt{T(1-T)}\delta_2, \quad (58)$$

and

$$\gamma_3 := \sqrt{T(1-T)}(\beta'_3 - \beta_3) - (1-T)\delta_3 + T\delta_4. \quad (59)$$

Then, after simple algebra we get

$$\mathbf{\Gamma} = \frac{\mathbf{\Pi}}{\gamma_1}, \quad (60)$$

and

$$\mathbf{\Gamma}' = \frac{\gamma_1}{\det \gamma} \mathbf{\Pi}'. \quad (61)$$

Note that previous Eqs. (60) and (61) are well-defined, since $\gamma_1 > 0$ and $\det \gamma > 0$, i.e., the matrix γ is positive definite. Using Eqs. (60) and (61), we can simplify the previous Eq. (52). After some algebra, we get the first main result of our paper, i.e., the input-output formula for the CM under ideal Bell-like detection

$$\mathbf{V}_{out} = \mathbf{A} - \frac{1}{\det \gamma} \sum_{i,j=1}^2 \mathbf{C}_i \mathbf{K}_{ij} \mathbf{C}_j^T, \quad (62)$$

where

$$\mathbf{K}_{11} = \begin{pmatrix} (1-T)\gamma_2 & \sqrt{T(1-T)}\gamma_3 \\ \sqrt{T(1-T)}\gamma_3 & T\gamma_1 \end{pmatrix}, \quad (63)$$

$$\mathbf{K}_{22} = \begin{pmatrix} T\gamma_2 & -\sqrt{T(1-T)}\gamma_3 \\ -\sqrt{T(1-T)}\gamma_3 & (1-T)\gamma_1 \end{pmatrix}, \quad (64)$$

$$\mathbf{K}_{12} = \mathbf{K}_{21}^T = \begin{pmatrix} -\sqrt{T(1-T)}\gamma_2 & (1-T)\gamma_3 \\ -T\gamma_3 & \sqrt{T(1-T)}\gamma_1 \end{pmatrix}. \quad (65)$$

Thus, the output CM \mathbf{V}_{out} of the surviving n modes after the ideal Bell-like detection is related to the input CM \mathbf{V}_{in} of the initial $n+2$ modes of Eqs. (31)-(33) by means of the input-output relation of Eq. (62), where the matrices \mathbf{K}_{ij} and γ are completely characterized by the reduced CM $\mathbf{B}^{(2)}$ of the detected modes and the transmission $0 \leq T \leq 1$ which is used in the Bell-like detection.

Note that, in Eq. (62), the terms $\mathbf{C}_i \mathbf{K}_{ij} \mathbf{C}_j^T$ generate $2n \times 2n$ matrices, i.e., with the same dimensions of \mathbf{A} . For instance, we have

$$\begin{aligned} \mathbf{C}_1 \mathbf{K}_{11} \mathbf{C}_1^T &= \begin{pmatrix} \vdots \\ \mathbf{C}_1^k \\ \vdots \end{pmatrix} \mathbf{K}_{11} (\cdots (\mathbf{C}_1^k)^T \cdots) \\ &= \begin{pmatrix} \mathbf{C}_1^1 \mathbf{K}_{11} (\mathbf{C}_1^1)^T & \cdots & \mathbf{C}_1^1 \mathbf{K}_{11} (\mathbf{C}_1^n)^T \\ \vdots & \ddots & \vdots \\ \mathbf{C}_1^n \mathbf{K}_{11} (\mathbf{C}_1^1)^T & \cdots & \mathbf{C}_1^n \mathbf{K}_{11} (\mathbf{C}_1^n)^T \end{pmatrix}. \end{aligned} \quad (66)$$

As an exercise, we specify our ideal input-output formula of Eq. (62) to the cases of standard Bell measurement and heterodyne detection in Appendix A.

B. Bell-like measurements with arbitrary quantum efficiencies

In this subsection, we generalize the previous input-output formula for the CM given in Eq. (62) to realistic detectors. As depicted in Fig. 4, we consider two homodyne detectors with quantum efficiencies $0 < \eta \leq 1$ and $0 < \eta' \leq 1$, modelled by inserting two beam-splitters with transmissivities η and η' , which mix the last two signal modes with environmental vacua.

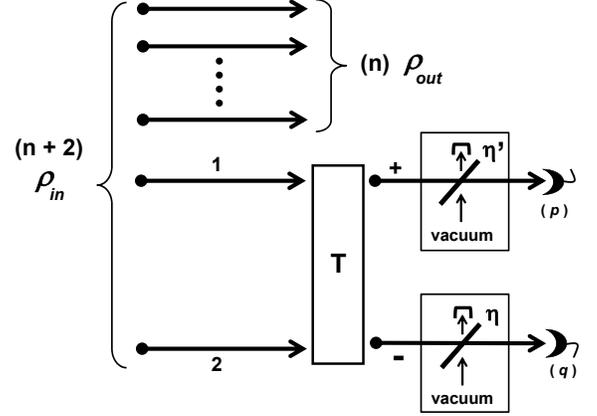


FIG. 4: An input Gaussian state ρ_{in} of $n+2$ modes is subject to a realistic Bell-like detection in its last two modes (labelled by 1 and 2). Homodyne detectors have arbitrary quantum efficiencies $0 < \eta \leq 1$ and $0 < \eta' \leq 1$ (modelled by beam-splitters with transmissivities η and η' , which mix the last two signal modes with two environmental vacua). The output state ρ_{out} of the surviving n modes is Gaussian and its CM is related to the input CM by the formula of Eq. (74).

As before we start from the input CM \mathbf{V}_{in} of Eq. (31), whose blocks are specified in Eqs. (32) and (33), and their parametrization is given in Eqs. (54) and (55). From this parametrization, we construct the γ -matrix of Eq. (56) as before, i.e., using Eqs. (57), (58) and (59). In order to compute the new input-output formula, note that the derivation is the same as before up to Eq. (45), which represents the CM of the state after the action of the Bell's beam-splitter with transmissivity T . The difference is that we now apply an imperfect \hat{q} -detection on the last mode “-” with efficiency η , and an imperfect \hat{p} -detection on the next-to-last mode “+” with efficiency η' . This means that the steps from Eq. (46) to Eq. (53) are still valid, proviso that we suitably replace the two matrices $\mathbf{\Gamma}$ and $\mathbf{\Gamma}'$.

The inefficient \hat{q} -detection on the last mode “-” corresponds to apply the transformation of Eq. (21) to Eq. (45). As a result, we get Eq. (46) with

$$\mathbf{\Gamma} = \frac{\mathbf{\Pi}}{\gamma_1(\eta)}, \quad (67)$$

where

$$\gamma_1(\eta) := \gamma_1 + \frac{1-\eta}{\eta}. \quad (68)$$

This expression clearly coincides with that of Eq. (60) for unit efficiency ($\eta = 1$). Thus, the $(n + 1)$ -mode CM describing the first n modes and mode “+” is now given by Eqs. (48-51) with $\mathbf{\Gamma}$ defined in Eq. (67).

We now apply the inefficient \hat{p} -detection on mode “+”, which corresponds to apply the transformation of Eq. (22) to Eq. (48). As a result we get the final CM \mathbf{V}_{out} for the first n modes after the inefficient Bell-like measurement, which is given by Eq. (52) where the matrix $\mathbf{\Gamma}'$ is now equal to

$$\mathbf{\Gamma}' = \frac{\gamma_1(\eta)}{\det \gamma(\eta, \eta')} \mathbf{\Pi}', \quad (69)$$

where

$$\gamma(\eta, \eta') := \begin{pmatrix} \gamma_1(\eta) & \gamma_3 \\ \gamma_3 & \gamma_2(\eta') \end{pmatrix}, \quad (70)$$

with $\gamma_1(\eta)$ defined in Eq. (68) and

$$\gamma_2(\eta') := \gamma_2 + \frac{1 - \eta'}{\eta'}. \quad (71)$$

In other words, we can write

$$\gamma(\eta, \eta') = \gamma + \mathbf{\Phi}(\eta, \eta'), \quad (72)$$

where

$$\mathbf{\Phi}(\eta, \eta') := \begin{pmatrix} \frac{1-\eta}{\eta} & \\ & \frac{1-\eta'}{\eta'} \end{pmatrix}. \quad (73)$$

The new matrix $\gamma(\eta, \eta')$ is essentially the old matrix γ plus the effect $\mathbf{\Phi}(\eta, \eta')$ of the quantum efficiencies η and η' . Again, for ideal detection ($\eta = \eta' = 1$) we have $\gamma(1, 1) = \gamma$ which means that Eq. (69) becomes identical to the previous Eq. (61).

Using Eqs. (67) and (69) in Eq. (52), we derive the explicit expression of \mathbf{V}_{out} . After some algebra, we get the second main result of our paper, i.e., the general input-output formula for the CM under Bell-like detection with arbitrary quantum efficiencies η and η' . This is given by

$$\mathbf{V}_{out}(\eta, \eta') = \mathbf{A} - \frac{1}{\det \gamma(\eta, \eta')} \sum_{i,j=1}^2 \mathbf{C}_i \mathbf{K}_{ij}(\eta, \eta') \mathbf{C}_j^T, \quad (74)$$

where the matrices $\mathbf{K}_{ij}(\eta, \eta')$ are equal to those given in Eqs. (63-65) up to the replacements

$$\gamma_1 \rightarrow \gamma_1(\eta), \quad \gamma_2 \rightarrow \gamma_2(\eta'). \quad (75)$$

Note that the only difference between the general formula of Eq. (74) and the ideal formula of Eq. (62) is in the replacements of Eq. (75). In other words, to compute the output CM, we perform exactly the same procedure as before for the ideal case, proviso that we now use $\gamma_1(\eta)$ and $\gamma_2(\eta')$ in the γ -matrix and the \mathbf{K} -matrices. As an exercise, we specify our general input-output formula of Eq. (74) to the cases of standard Bell measurement and heterodyne detection in Appendix A.

V. CONCLUSION

In conclusion, we have derived a simple formula for the transformation of CMs under generalized Bell-like detections, where two modes of a bosonic system are subject to an arbitrary beam-splitter transformation, followed by homodyne detections. We have consider first the case of ideal detection and, then, the general case of homodyne detectors with arbitrary quantum efficiencies. Our formula can be applied to study quantum information protocols in various contexts, including protocols of teleportation, entanglement swapping and quantum key distribution. In particular, it can be adopted to generalize the analysis of these protocols to the presence of experimental imperfections and asymmetric setups, for instance, deriving from the use of unbalanced beam splitters.

VI. ACKNOWLEDGEMENTS

This work has been supported by EPSRC under the research grant HIPERCOM (EP/J00796X/1).

Appendix A: Application of the formulas to specific cases

In this appendix we specify our formulas to the cases of standard Bell detection (balanced beam-splitter) and heterodyne detection (balanced beam-splitter with a vacuum at one of the input ports). First we consider the ideal case of unit quantum efficiencies for the detectors, i.e., we specify the formula of Eq. (62). Then, we extend the results to the case of arbitrary quantum efficiencies, which corresponds to applying the formula of Eq. (74).

1. Standard Bell detection

We achieve the formula for standard Bell detection by setting $T = 1/2$ (balanced beam splitter). In this case, we have

$$\gamma_1 = \frac{1}{2}(\beta_1 + \beta'_1) - \delta_1, \quad \gamma_2 = \frac{1}{2}(\beta_2 + \beta'_2) + \delta_2, \quad (A1)$$

and $\gamma_3 = \frac{1}{2}(\beta'_3 - \beta_3 - \delta_3 + \delta_4)$. Compactly, the γ -matrix takes the form

$$\gamma = \frac{1}{2} (\mathbf{ZB}_1\mathbf{Z} + \mathbf{B}_2 - \mathbf{ZD} - \mathbf{D}^T\mathbf{Z}), \quad (A2)$$

where \mathbf{Z} is given in Eq. (24). The \mathbf{K} -matrices can be simplified too. In fact, we get

$$\mathbf{K}_{11} = \frac{1}{2} \begin{pmatrix} \gamma_2 & \gamma_3 \\ \gamma_3 & \gamma_1 \end{pmatrix} = \frac{1}{2} \mathbf{X}_1^T \boldsymbol{\gamma} \mathbf{X}_1, \quad (\text{A3})$$

$$\mathbf{K}_{22} = \frac{1}{2} \begin{pmatrix} \gamma_2 & -\gamma_3 \\ -\gamma_3 & \gamma_1 \end{pmatrix} = \frac{1}{2} \mathbf{X}_2^T \boldsymbol{\gamma} \mathbf{X}_2 \quad (\text{A4})$$

$$\mathbf{K}_{12} = \mathbf{K}_{21}^T = \frac{1}{2} \begin{pmatrix} -\gamma_2 & \gamma_3 \\ -\gamma_3 & \gamma_1 \end{pmatrix} = \frac{1}{2} \mathbf{X}_1^T \boldsymbol{\gamma} \mathbf{X}_2, \quad (\text{A5})$$

where

$$\mathbf{X}_1 := \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad \mathbf{X}_2 := \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \boldsymbol{\Omega}. \quad (\text{A6})$$

Since $\mathbf{K}_{ij} = \mathbf{X}_i^T \boldsymbol{\gamma} \mathbf{X}_j / 2$, the formula of Eq. (62) becomes

$$\mathbf{V}_{out} = \mathbf{A} - \frac{1}{2 \det \boldsymbol{\gamma}} \sum_{i,j=1}^2 \mathbf{C}_i (\mathbf{X}_i^T \boldsymbol{\gamma} \mathbf{X}_j) \mathbf{C}_j^T, \quad (\text{A7})$$

where the $\boldsymbol{\gamma}$ -matrix is given by Eq. (A2).

It is straightforward to generalize the formula of Eq. (A7) to the case of arbitrary quantum efficiencies η and η' for the homodyne detectors. In fact, it is sufficient to replace

$$\boldsymbol{\gamma} \rightarrow \boldsymbol{\gamma}(\eta, \eta') = \boldsymbol{\gamma} + \boldsymbol{\Phi}(\eta, \eta'), \quad (\text{A8})$$

with $\boldsymbol{\gamma}$ given in Eq. (A2) and $\boldsymbol{\Phi}(\eta, \eta')$ given in Eq. (73).

2. Heterodyne detection

We achieve the heterodyne detection of the $(n+1)^{th}$ mode by setting $T = 1/2$ (balanced beam splitter) and considering the last mode in a vacuum state. As a matter of fact, this is equivalent to a standard Bell detection where the last mode is in a vacuum. Thus, we have

$$\mathbf{B}^{(2)} = \begin{pmatrix} \mathbf{B}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}, \quad \mathbf{C}_2 = \mathbf{0}, \quad (\text{A9})$$

so that the global input CM is equal to

$$\mathbf{V}_{in} = \begin{pmatrix} \mathbf{A} & \mathbf{C}_1 \\ \mathbf{C}_1^T & \mathbf{B}_1 \end{pmatrix} \oplus \mathbf{I}. \quad (\text{A10})$$

By setting $\mathbf{B}_2 = \mathbf{I}$ and $\mathbf{D} = \mathbf{0}$ in Eq. (A2), we derive the expression of the $\boldsymbol{\gamma}$ -matrix, which is given by

$$\boldsymbol{\gamma} = \frac{1}{2} (\mathbf{Z} \mathbf{B}_1 \mathbf{Z} + \mathbf{I}) = \frac{1}{2} \begin{pmatrix} \beta_1 + 1 & -\beta_3 \\ -\beta_3 & \beta_2 + 1 \end{pmatrix}. \quad (\text{A11})$$

This matrix has determinant

$$\det \boldsymbol{\gamma} = \frac{\theta_1}{4}, \quad \theta_1 := \det \mathbf{B}_1 + \text{Tr} \mathbf{B}_1 + 1. \quad (\text{A12})$$

Since $\mathbf{C}_2 = \mathbf{0}$, the sum in Eq. (A7) contains only the term with $i = j = 1$, i.e.,

$$\mathbf{V}_{out} = \mathbf{A} - \frac{1}{2 \det \boldsymbol{\gamma}} \mathbf{C}_1 (\mathbf{X}_1^T \boldsymbol{\gamma} \mathbf{X}_1) \mathbf{C}_1^T. \quad (\text{A13})$$

Now, we can easily check that

$$\begin{aligned} \mathbf{X}_1^T \boldsymbol{\gamma} \mathbf{X}_1 &= \frac{1}{2} \mathbf{X}_1^T (\mathbf{Z} \mathbf{B}_1 \mathbf{Z} + \mathbf{I}) \mathbf{X}_1 \\ &= \frac{1}{2} (\boldsymbol{\Omega}^T \mathbf{B}_1 \boldsymbol{\Omega} + \mathbf{I}) = \frac{1}{2} (\boldsymbol{\Omega} \mathbf{B}_1 \boldsymbol{\Omega}^T + \mathbf{I}). \end{aligned} \quad (\text{A14})$$

By using Eqs. (A12) and (A14) into Eq. (A13), we get

$$\mathbf{V}_{out} = \mathbf{A} - \frac{1}{\theta_1} \mathbf{C}_1 (\boldsymbol{\Omega} \mathbf{B}_1 \boldsymbol{\Omega}^T + \mathbf{I}) \mathbf{C}_1^T. \quad (\text{A15})$$

Similarly, if we heterodyne the $(n+2)^{th}$ mode with the $(n+1)^{th}$ mode being the ancillary vacuum mode, we get

$$\mathbf{V}_{out} = \mathbf{A} - \frac{1}{\theta_2} \mathbf{C}_2 (\boldsymbol{\Omega} \mathbf{B}_2 \boldsymbol{\Omega}^T + \mathbf{I}) \mathbf{C}_2^T, \quad (\text{A16})$$

with

$$\theta_2 := \det \mathbf{B}_2 + \text{Tr} \mathbf{B}_2 + 1. \quad (\text{A17})$$

This formula for the heterodyne detection coincides with that given in Ref. [1] (without an explicit proof).

In this case too, we can easily extend the results to non-unit quantum efficiencies, η and η' , for the homodyne detectors. We need to perform the replacement $\boldsymbol{\gamma} \rightarrow \boldsymbol{\gamma} + \boldsymbol{\Phi}(\eta, \eta')$ in Eq. (A13). First note that

$$\mathbf{X}_1^T (\boldsymbol{\gamma} + \boldsymbol{\Phi}) \mathbf{X}_1 = \frac{1}{2} [\boldsymbol{\Omega} (\mathbf{B}_1 + 2\boldsymbol{\Phi}) \boldsymbol{\Omega}^T + \mathbf{I}]. \quad (\text{A18})$$

Then, for the determinant we can write

$$\det(\boldsymbol{\gamma} + \boldsymbol{\Phi}) = \det \boldsymbol{\gamma} + \det \boldsymbol{\Phi} + \text{Tr} (\boldsymbol{\Omega} \boldsymbol{\Phi} \boldsymbol{\Omega}^T \boldsymbol{\gamma}), \quad (\text{A19})$$

which is an equality valid in general for any symmetric matrix $\boldsymbol{\gamma}$ and diagonal matrix $\boldsymbol{\Phi}$. Now using Eq. (A12) in Eq. (A19), we get

$$\begin{aligned} \det(\boldsymbol{\gamma} + \boldsymbol{\Phi}) &= \frac{\theta_1 + 4 \det \boldsymbol{\Phi} + 2 \text{Tr} \boldsymbol{\Phi} + 2 \text{Tr} (\boldsymbol{\Omega} \boldsymbol{\Phi} \boldsymbol{\Omega}^T \mathbf{B}_1)}{4} \\ &:= \frac{\theta_1(\eta, \eta')}{4}. \end{aligned} \quad (\text{A20})$$

Finally, using Eqs. (A18) and (A20), we get

$$\mathbf{V}_{out}(\eta, \eta') = \mathbf{A} - \frac{1}{\theta_1(\eta, \eta')} \mathbf{C}_1 [\boldsymbol{\Omega} (\mathbf{B}_1 + 2\boldsymbol{\Phi}) \boldsymbol{\Omega}^T + \mathbf{I}] \mathbf{C}_1^T, \quad (\text{A21})$$

which is the generalization of Eq. (A15) to arbitrary quantum efficiencies.

-
- [1] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* **84**, 621 (2012).
- [2] S. L. Braunstein and A. K. Pati, *Quantum Information Theory with Continuous Variables* (Kluwer Academic, Dordrecht, 2003).
- [3] S. L. Braunstein and P. van Loock, *Rev. Mod. Phys.* **77**, 513 (2005).
- [4] A. Furusawa *et al.*, *Science* **282**, 706 (1998).
- [5] S. L. Braunstein, and H. J. Kimble, *Phys. Rev. Lett.* **80**, 869 (1998).
- [6] S. Pirandola, S. Mancini, D. Vitali, and P. Tombesi, *Phys. Rev. A* **68**, 062317 (2003).
- [7] S. D. Bartlett and W. J. Munro, *Phys. Rev. Lett.* **90**, 117901 (2003).
- [8] S. Pirandola and S. Mancini, *Laser Physics* **16**, 1418 (2006).
- [9] J. Sherson, H. Krauter, R. K. Olsson, B. Julsgaard, K. Hammerer, I. Cirac, and E. S. Polzik, *Nature* **443**, 557 (2009).
- [10] P. van Loock, and S. L. Braunstein, *Phys. Rev. Lett.* **84**, 3482 (2000).
- [11] P. van Loock and S. L. Braunstein, *Phys. Rev. A* **61**, 010302(R) (1999).
- [12] N. Takei, H. Yonezawa, T. Aoki, and A. Furusawa, *Phys. Rev. Lett.* **94**, 220502 (2005).
- [13] S. Pirandola, D. Vitali, P. Tombesi, and S. Lloyd, *Phys. Rev. Lett.* **97**, 150403 (2006).
- [14] J. Hoelscher-Obermaier and P. van Loock, *Phys. Rev. A* **83**, 012319 (2010).
- [15] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, *Phys. Rev. Lett.* **93**, 170504 (2004).
- [16] C. Weedbrook, C., A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, *Phys. Rev. A* **73**, 022316 (2006).
- [17] S. Pirandola, S. L. Braunstein, and S. Lloyd, *Phys. Rev. Lett.* **101**, 200504 (2008).
- [18] C. Weedbrook, S. Pirandola, S. Lloyd, T. C. Ralph, *Phys. Rev. Lett.* **105**, 110501 (2010).
- [19] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, *Nature Physics* **4**, 726 (2008).
- [20] U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, Cambridge, 1997).
- [21] J. Eisert, and M.B. Plenio, *Int. J. Quant. Inf.* **1**, 479 (2003).
- [22] J. Eisert, S. Scheel, and M.B. Plenio, *Phys. Rev. Lett.* **89**, 137903 (2002).
- [23] R. Simon, N. Mukunda, and B. Dutta, *Phys. Rev. A* **49**, 1567 (1994).
- [24] S. Pirandola, A. Serafini, and S. Lloyd, *Phys. Rev. A* **79**, 052327 (2009).
- [25] Proof is trivial. Set $\mathbf{M} = x\mathbf{\Pi}$ and $\mathbf{G} = \begin{pmatrix} a & c \\ d & b \end{pmatrix}$. Then, $\mathbf{H} = \begin{pmatrix} ax - 1 & cx \\ 0 & -1 \end{pmatrix}$ and $r = (ax - 1)^2 + c^2x^2 + 1$. The gradient of r is given by $\frac{\partial r}{\partial c} = 2x^2c$ and $\frac{\partial r}{\partial a} = 2x(ax - 1)$ which is zero for $c = 0$ and $a = x^{-1}$ (since $x \neq 0$). Finally, we can freely choose $b = d = 0$, so that $\mathbf{G} = x^{-1}\mathbf{\Pi}$.
- [26] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).