Driving non-Gaussian to Gaussian states with linear optics

Daniel E. Browne,[1,*] Jens Eisert,[1,2] Stefan Scheel,[1] and Martin B. Plenio[1]
[1]*QOLS, Blackett Laboratory, Imperial College London, Prince Consort Road, London SW7 2BW, United Kingdom*
[2]*Institut für Physik, Universität Potsdam, Am Neuen Palais 10, D-14469 Potsdam, Germany*

(Received 26 November 2002; published 30 June 2003)

We introduce a protocol that maps finite-dimensional pure input states onto approximately Gaussian states in an iterative procedure. This protocol can be used to distill highly entangled bipartite Gaussian states from a supply of weakly entangled pure Gaussian states. The entire procedure requires only the use of passive optical elements and photon detectors, which solely distinguish between the presence and absence of photons.

DOI: 10.1103/PhysRevA.67.062320 PACS number(s): 03.67.−a, 42.50.−p, 03.65.Ud

I. INTRODUCTION

Gaussian entangled states may be prepared quite simply in optical systems: one only has to mix a pure squeezed state with a vacuum state at a beam splitter, both of which are special instances of Gaussian states in systems with canonical coordinates [1,2]. The beam splitter acts as a Gaussian unitary operation that modifies the quantum state, but does not alter the Gaussian character of the state. This state may be used as the resource for protocols in quantum information processing. In fact, teleportation [3], dense coding [4], and cryptographic schemes [5] on the basis of such two-mode squeezed states have been either studied theoretically or already experimentally realized. For the theory of quantum information processing in systems with canonical degrees, Gaussian states play a role closely analogous to that of entangled states of qubits, for which most of the theory of quantum information processing has been developed.

However, there are significant limits to what accuracy highly entangled two-mode squeezed states may be prepared and distributed over large distances. First, the degree of single-mode squeezing which can be achieved limits the degree of two-mode squeezing of the resulting state. Second, decoherence is unavoidable in the transmission of states through fibres, and the original highly entangled state will deteriorate into a very weakly entangled mixed Gaussian state [6]. For finite-dimensional systems, it has been one of the key observations that from weakly entangled states one can obtain highly entangled states by means of local quantum operations supported by classical communication [7] at the price of starting from a large number of weakly entangled systems but ending with a smaller number of more strongly entangled systems. The term entanglement distillation has been coined for such procedures. Importantly, such methods function also as the basis for security proofs of quantum cryptographic schemes [9].

It was generally expected that an analogous procedure should exists for the distillation of Gaussian states by means of local Gaussian operations and classical communication only. Surprisingly however, it was recently proven that this is not the case [10,11]. For example, no matter how the local Gaussian quantum operations are chosen, one cannot map a large number of weakly entangled two-mode squeezed states onto a single highly entangled Gaussian state. Gaussian quantum operations [10–12] correspond in optical systems to the application of optical elements, such as beam splitters, phase shifts, and $\chi^{(2)}$ squeezers, together with homodyne detection. All these operations are, to some degree of accuracy, experimentally accessible. With non-Gaussian quantum operations, in turn, one can distill finite-dimensional states out of a supply of Gaussian states [13], but the resulting states are not Gaussian, and the experimental implementation of the known protocols constitutes a significant challenge.

One may be tempted to think that this observation renders all attempts to increase the degree of entanglement in Gaussian states impossible. In this paper, however, we discuss the possibility of obtaining a Gaussian state with arbitrarily high fidelity from a supply of non-Gaussian states employing only Gaussian operations, namely linear optical elements and projections onto the vacuum. We describe a protocol that prepares approximate Gaussian states from a supply of non-Gaussian states. The non-Gaussian states that we use could, in particular, be obtained from the weak two-mode squeezed vacua by the application of a beam splitter and a photon detector. Together with this step, the proposed procedure offers a complete distillation procedure of Gaussian states to (almost exact) Gaussian states, but via non-Gaussian territory. It is important to note that the protocol introduced below is by no means restricted to a bipartite setting. The bipartite case is the most important one practically, as it allows in effect for distillation of Gaussian states with non-Gaussian operations. But this method can, in particular, also be used in a monopartite setting to approximately obtain a Gaussian state from a supply of unknown non-Gaussian states.

The paper is organized as follows. First, we will describe the protocol that generates Gaussian states from a supply of non-Gaussian states. This protocol requires only passive optical elements and photon detectors which can distinguish between the absence or presence of photons, but do not determine their exact number. We then proceed by discussing the effect of the protocol in more detail. We will discuss the special case of pure states in Schmidt form as well as general pure states. The fixed points of the iteration map will be identified as pure Gaussian states, and a proof of convergence will be given. Finally, we will discuss the feasible

[*] Electronic address: d.browne@ic.ac.uk

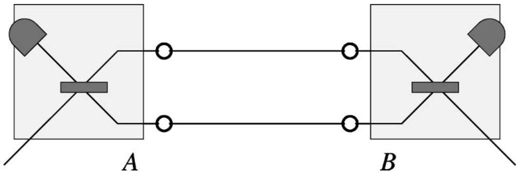

FIG. 1. A single step of the protocol. Two pairs of entangled two-mode states are mixed locally at 50:50 beam splitters, and the absence or presence of photons is detected in one of the output arms on both sides.

preparation of finite-dimensional states from a supply of pure Gaussian states.

II. THE PROTOCOL

The protocol is very simple indeed. We start with a supply of identically prepared bipartite non-Gaussian states. The overall protocol then amounts to an iteration of the following basic steps.

(1) The states will be mixed pairwise locally at 50:50 beam splitters (see Fig. 1).

(2) On one of the outputs of each beam splitter, a photon detector distinguishes between the absence and presence of photons. It should be noted that we do not require photon counters that can discriminate between different photon numbers.

(3) In case of absence of photons at both detectors for a particular pair, one keeps the remaining modes as an input for the next iteration, otherwise the state is discarded.

This is one iteration of the protocol which we will continue until we finally end up with a small number of states that closely resemble Gaussian states. This is clearly a probabilistic protocol. However, the success probability, as we will see later, can be quite high. It should also be noted that the operations in a successful run are indeed Gaussian operations, namely the use of linear optical elements and vacuum projections. Each of these steps can be realized with present-day technology.

III. EXAMPLES OF THE PROTOCOL

A. Pure states in Schmidt form

In order to demonstrate the general mechanism, we start by discussing a particularly simple case, namely pure states in Schmidt form. We do not require any prior knowledge of the actual un-normalized state vectors, except that they can be expressed in the following form:

$$|\psi^{(0)}\rangle = \sum_{n=0}^{\infty} \alpha_{n,n}^{(0)} |n,n\rangle, \tag{1}$$

where $\{\alpha_{n,n}^{(0)}\}_{n=0}^{\infty}$ with $\alpha_{n,n}^{(0)} \geqslant 0$ are proportional to the real Schmidt coefficients of the state vector, and $\{|n\rangle : n \in \mathbb{N}\}$ denotes the Fock basis. We only assume $\alpha_{0,0}^{(0)} > 0$ and it is then convenient to consider un-normalized states for which we set $\alpha_{0,0}^{(0)} = 1$. The un-normalized states arising in later steps $i = 1,2, \ldots$ are characterized by coefficients $\{\alpha_{n,n}^{(i)}\}_{n=0}^{\infty}$. These coefficients then become identical to the Schmidt coefficients only after appropriate normalization. Starting from two identical copies of state vectors which have been obtained in the ith step of the protocol, i.e.

$$|\psi^{(i)}\rangle |\psi^{(i)}\rangle, \tag{2}$$

one obtains after application of the 50:50 beam splitters the state vector $(\hat{U}_{12} \otimes \hat{U}_{12}) |\psi^{(i)}\rangle |\psi^{(i)}\rangle$. Here, the beam splitter is described by (see, e.g., Ref. [15])

$$\hat{U}_{12} = T^{\hat{n}_1} e^{-R^* \hat{a}_2^{\dagger} \hat{a}_1} e^{R \hat{a}_2 \hat{a}_1^{\dagger}} T^{-\hat{n}_2}, \tag{3}$$

where $\hat{U}_{12}$ acts on the amplitude operators of the field modes as

$$\hat{U}_{12} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} \hat{U}_{12}^{\dagger} = \begin{pmatrix} T & R \\ -R^* & T^* \end{pmatrix} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix}, \tag{4}$$

where we set $T = R = 1/\sqrt{2}$. The resulting un-normalized state vector, conditional on vacuum outcomes in both detectors, is given by

$$\begin{aligned} |\psi^{(i+1)}\rangle &:= \langle 0,0| (\hat{U}_{12} \otimes \hat{U}_{12}) |\psi\rangle |\psi\rangle \\ &= \sum_{n=0}^{\infty} \left[2^{-n} \sum_{r=0}^{n} \binom{n}{r} \alpha_{r,r}^{(i)} \alpha_{n-r,n-r}^{(i)} \right] |n,n\rangle \\ &= \sum_{n=0}^{\infty} \alpha_{n,n}^{(i+1)} |n,n\rangle, \end{aligned} \tag{5}$$

where

$$\alpha_{n,n}^{(i+1)} := 2^{-n} \sum_{r=0}^{n} \binom{n}{r} \alpha_{r,r}^{(i)} \alpha_{n-r,n-r}^{(i)} \tag{6}$$

for $n = 0,1, \ldots$. The probability of vacuum outcomes being detected in both modes is $\langle \psi^{(i+1)} | \psi^{(i+1)} \rangle / |\langle \psi^{(i)} | \psi^{(i)} \rangle|^2$. The protocol is a Gaussian quantum operation, in the sense that it is a completely positive map that maps all Gaussian states onto Gaussian states. The interesting feature is that by repeated application it also maps non-Gaussian states arbitrarily close to Gaussian states, as will be demonstrated below.

In effect, in each iteration one maps one sequence of coefficients $\alpha^{(i)} = \{\alpha_{n,n}^{(i)}\}_{n=0}^{\infty}$ onto another sequence $\alpha^{(i+1)} = \{\alpha_{n,n}^{(i+1)}\}_{n=0}^{\infty}$, defining the map Φ via

$$\alpha^{(i+1)} =: \Phi(\alpha^{(i)}). \tag{7}$$

In the following, we use the notation $\Phi^{(1)} = \Phi$ and $\Phi^{(i+1)} = \Phi \circ \Phi^{(i)}$ for $i = 0,1, \ldots$. The main observation is that provided $\alpha_{1,1}^{(0)} < \alpha_{0,0}^{(0)}$, the sequence of coefficients $\{\alpha^{(i)}\}_{i=1}^{\infty}$ converges to a distribution corresponding to a Gaussian state, in this special case a two-mode squeezed vacuum.

In other words, although the initial state was not Gaussian, but say, a state corresponding to a finite-dimensional state vector of the form

$$|\psi^{(0)}\rangle = |0,0\rangle + \alpha_{1,1}^{(0)}|1,1\rangle, \tag{8}$$

where $\alpha_{1,1}^{(0)} \in [0,1)$, after a number of steps the resulting state is Gaussian to a high degree of accuracy. We will first show that this convergence is a general feature of this protocol, and we will then discuss the consequences. We start by demonstrating that those distributions associated with the pure Gaussian states are fixed points of the map Φ.

Proposition 1. The distributions $\alpha = \{\alpha_{n,n}\}_{n=0}^{\infty}$ of the form

$$\alpha_{n,n} = \lambda^n \tag{9}$$

$(\lambda \geqslant 0)$, corresponding to two-mode squeezed states, are the only fixed points of the map Φ.

Proof. This can be immediately derived from the definition of Φ. Let us assume that

$$\alpha = \Phi(\alpha) \tag{10}$$

holds. It can be verified by substitution that $\alpha_{n,n} = \lambda^n$ is a solution of this equation. The uniqueness of this solution can be verified by observing that Eq. (10) also implies $\alpha_{0,0} = \alpha_{0,0}^2$, that is, $\alpha_{0,0} = 1$. Then $\alpha_{1,1}$ is a free parameter and once set (i.e., as $\alpha_{1,1} = \lambda$) the remaining coefficients are uniquely determined.

These coefficients, for $\lambda \in [0,1)$, in turn correspond exactly to two-mode pure Gaussian states. If λ lies outside this range, the state is not normalizable. The next proposition states that those distributions associated with Gaussian states are not only fixed points of the map Φ, but provided $\alpha_{0,0}^{(0)} \neq 0$ each sequence of coefficients converges to such a fixed point.

Proposition 2. Let $\alpha^{(0)} = \{\alpha_{n,n}^{(0)}\}_{n=0}^{\infty}$ with $a_{0,0}^{(0)} = 1$ and $0 \leqslant \alpha_{1,1}^{(0)} < 1$. Then

$$\lim_{i\to\infty} \alpha_{n,n}^{(i)} = \alpha_{n,n}^{(\infty)} \tag{11}$$

for all $n = 0,1,\ldots$, where $\alpha^{(\infty)}$ is a distribution of the type of Proposition 1.

Proof. As before, let us set $\alpha^{(i)} := \Phi^{(i)}(\alpha^{(0)})$ for $i = 1,2,\ldots$. The first step is to see that

$$\frac{\alpha_{1,1}^{(i+1)}}{\alpha_{0,0}^{(i+1)}} = \frac{\alpha_{1,1}^{(i)}}{\alpha_{0,0}^{(i)}} = \alpha_{1,1}^{(0)} \tag{12}$$

for all $i = 0,1,\ldots$. Let us first assume that $\alpha_{1,1}^{(0)} > 0$. Then, as can be seen from the definition of Φ,

$$\alpha_{2,2}^{(i+1)}\alpha_{1,1}^{(i)} = \frac{1}{2}(\alpha_{2,2}^{(i)} + \alpha_{1,1}^{(0)}\alpha_{1,1}^{(i)})\alpha_{1,1}^{(i+1)}. \tag{13}$$

Hence, as $\alpha_{1,1}^{(i)} = \alpha_{1,1}^{(0)} > 0$ for all $i = 0,1,\ldots,$

$$\lim_{i\to\infty} \frac{\alpha_{2,2}^{(i)}}{\alpha_{1,1}^{(i)}} = \alpha_{1,1}^{(0)}. \tag{14}$$

Now let us assume that already $\alpha_{n-1,n-1}^{(i)} > 0$ for all $i = 0,1,\ldots$ and

$$\lim_{i\to\infty} \frac{\alpha_{n,n}^{(i)}}{\alpha_{n-1,n-1}^{(i)}} = \alpha_{1,1}^{(0)} \tag{15}$$

for some $n = 1,2,\ldots$. Then, from

$$\frac{\alpha_{n+1,n+1}^{(i+1)}}{\alpha_{n,n}^{(i+1)}} = \frac{1}{2} \frac{\sum_{r=0}^{n+1} \alpha_{r,r}^{(i)} \alpha_{n-r+1,n-r+1}^{(i)} \binom{n+1}{r}}{\sum_{r=0}^{n} \alpha_{r,r}^{(i)} \alpha_{n-r,n-r}^{(i)} \binom{n}{r}}, \tag{16}$$

it follows after a few steps that $a_{n,n}^{(i)} > 0$ for all $i = 0,1,\ldots,$ and

$$\lim_{i\to\infty} \frac{\alpha_{n+1,n+1}^{(i+1)}}{\alpha_{n,n}^{(i+1)}} = \lim_{i\to\infty} \frac{1}{2^{n+1}} \left[\frac{2\alpha_{n+1,n+1}^{(i)}}{\alpha_{n,n}^{(i)}} + (2^{n+1} - 2)\alpha_{1,1}^{(0)} \right], \tag{17}$$

which means that

$$\lim_{i\to\infty} \frac{\alpha_{n+1,n+1}^{(i+1)}}{\alpha_{n,n}^{(i+1)}} = \alpha_{1,1}^{(0)}. \tag{18}$$

Hence, by induction we find that the ratios of $\alpha_{n+1,n+1}^{(i)}$ and $\alpha_{n,n}^{(i)}$ converge to the ratio of $0 < \alpha_{1,1}^{(0)} < 1$ and $\alpha_{0,0}^{(0)} = 1$ as $i \to \infty$. This means that the coefficients correspond to a Gaussian state as specified in Proposition 1. In case where $\alpha_{1,1}^{(0)} = 0$ an analogous argument can be applied in order to arrive at $\alpha_{0,0}^{(i)} = 1$ for all $i = 0,1,\ldots$ and

$$\lim_{i\to\infty} \alpha_{n,n}^{(i)} = 0 \tag{19}$$

for all $n = 1,2,\ldots$.

This shows formally that the (pointwise) convergence to an effectively Gaussian state is generic [14]. Putting aside the restriction that $\alpha_{0,0}^{(0)} = 1$, three cases shall be discussed in more detail.

(1) If $\alpha_{0,0}^{(0)} > 0$ and $\alpha_{1,1}^{(0)} < \alpha_{0,0}^{(0)}$, then the states converge to a Gaussian state.

(2) A special instance is when $\alpha_{0,0}^{(0)} > 0$, but $\alpha_{1,1}^{(0)} = 0$. Then the states converge to a Gaussian state, but to the product of two vacua.

(3) If $\alpha_{0,0}^{(0)} \leqslant \alpha_{1,1}^{(0)}$, then the sequence does not converge to a sequence of coefficients corresponding to a Gaussian state. In particular, this is always the case when

$$\alpha_{0,0}^{(0)} = 0. \tag{20}$$

This follows immediately from Eq. (6) as $\alpha_{0,0}^{(i)} = 0$ for all i.

In practice, one can actually expect a state that is very close to a Gaussian state already after a very small number of steps, say, three or four steps. As has already been mentioned, the whole scheme is probabilistic. That is, the success probability of actually obtaining the desired state is always less than 1. In Fig. 2, we show the total probability of success, $p_{\text{success}}^{(i)}$, and in Fig. 3 the corresponding fidelity $F^{(i)}$, i.e., the overlap with the Gaussian state to which the protocol

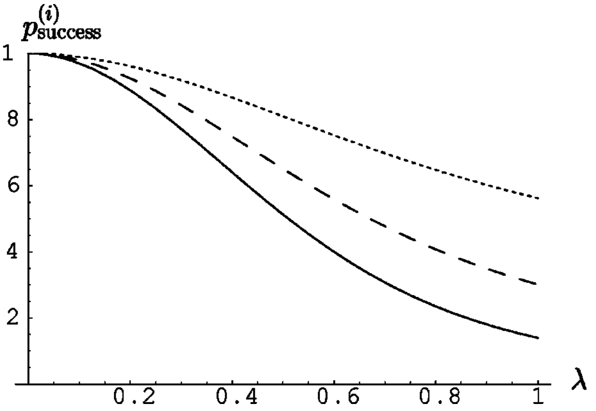

FIG. 2. Success probability $p_{\text{success}}^{(i)}$ after $i=1$ (dotted line), $i=2$ (dashed line), and $i=3$ (solid line) iteration steps, where the initial states were $\propto|0,0\rangle+\lambda|1,1\rangle$.

converges, after $i=1,2,3$ iteration steps. Here, we started with coefficients $\alpha_{0,0}^{(0)}=1$ and $\alpha_{1,1}^{(0)}=\lambda$.

We see that for a large range of values for λ, the fidelity is just below unity and, for λ = 0.5, the probability of success is still above 0.5.

B. General pure states

Suppose now we have a supply of pure states with state vectors of the general form

$$|\psi^{(0)}\rangle=\sum_{m,n=0}^{\infty}\alpha_{m,n}^{(0)}|m,n\rangle, \tag{21}$$

where $\alpha_{m,n}^{(0)}\in\mathbb{C}$ for all n,m. If the procedure described in Sec. II is carried out, using 50:50 beam splitters with appropriate phases such that $T=R=1/\sqrt{2}$, then for a large class of input states, after repeated iterations of the protocol, a state closely approximating a Gaussian state will be obtained. If the identical retained states after i iterations of the procedure are labeled

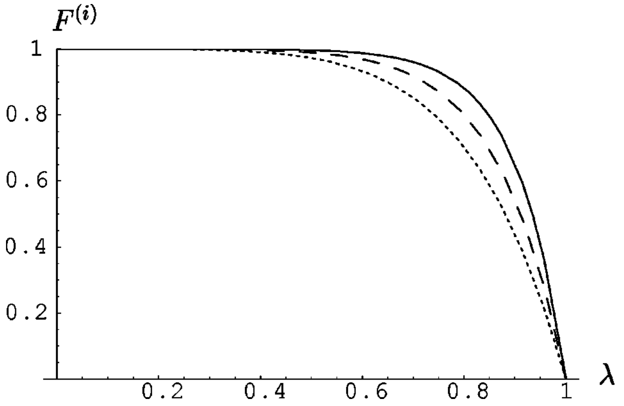

FIG. 3. Fidelity $F^{(i)}$ of the approximately Gaussian state after $i=1$ (dotted line), $i=2$ (dashed line), and $i=3$ (solid line) iterations, where the initial states were $\propto|0,0\rangle+\lambda|1,1\rangle$.

$$|\psi^{(i)}\rangle=\sum_{m,n}\alpha_{m,n}^{(i)}|m,n\rangle, \tag{22}$$

we can describe each iteration in terms of the following recurrence relation:

$$\alpha_{m,n}^{(i)}\mapsto\alpha_{m,n}^{(i+1)}=2^{-(m+n)/2}\sum_{r=0}^{m}\sum_{s=0}^{n}(-1)^{(m+n)-(r+s)}\times\alpha_{r,s}^{(i)}\alpha_{m-r,n-s}^{(i)}\left[\binom{m}{r}\binom{n}{s}\right]^{1/2}, \tag{23}$$

where again

$$\alpha^{(i+1)}=\Phi(\alpha^{(i)}), \tag{24}$$

with $\alpha^{(i)}=\{\alpha_{n,m}^{(i)}\}_{n,m=0}^{\infty}$ for $i=0,1,\ldots$. We will in the following write

$$\alpha_{n,m}^{(\infty)}:=\lim_{i\to\infty}\alpha_{n,m}^{(i)}, \tag{25}$$

whenever this limit exists. The fixed points of Φ, characterized by $\alpha_{m,n}^{(\infty)}\in\mathbb{C}$, correspond to states which are unchanged by one or more iterations of the procedure, and satisfy $\Phi(\alpha^{(\infty)})=\alpha^{(\infty)}$, thus

$$\alpha_{m,n}^{(\infty)}=2^{-(m+n)/2}\sum_{r=0}^{m}\sum_{s=0}^{n}(-1)^{(m+n)-(r+s)}\times\alpha_{r,s}^{(\infty)}\alpha_{m-r,n-s}^{(\infty)}\left[\binom{m}{r}\binom{n}{s}\right]^{1/2} \tag{26}$$

for all n,m. We immediately see that

$$\alpha_{0,0}^{(\infty)}=(\alpha_{0,0}^{(\infty)})^2 \tag{27}$$

and thus $\alpha_{0,0}^{(\infty)}=1$. (The other possibility $\alpha_{0,0}^{(\infty)}=0$ leads to the trivial solution $\alpha_{m,n}^{(\infty)}=0$ for all m,n.) We also find that the coefficients $\alpha_{1,1}^{(\infty)}$, $\alpha_{2,0}^{(\infty)}$, and $\alpha_{0,2}^{(\infty)}$ are the only free parameters. When these values are specified, all other coefficients are determined. The general solution of Eq. (26) is

$$\alpha_{2m,2n+1}^{(\infty)}=\alpha_{2m+1,2n}^{(\infty)}=0, \tag{28}$$

$$\alpha_{2m,2n}^{(\infty)}=\sqrt{(2m)!}\sqrt{(2n)!}\times\sum_{0\leqslant s\leqslant m;s\leqslant n}\left[\frac{\gamma_{12}^{2s}}{(2s)!}\frac{(\gamma_1/2)^{m-s}}{(m-s)!}\frac{(\gamma_2/2)^{n-s}}{(n-s)!}\right], \tag{29}$$

$$\alpha^{(\infty)}_{2m+1,2n+1}=\sqrt{(2m+1)!}\sqrt{(2n+1)!}\times\sum_{0\leqslant s\leqslant m;s\leqslant n}\left[\frac{\gamma_{12}^{2s+1}}{(2s+1)!}\frac{(\gamma_1/2)^{m-s}}{(m-s)!}\frac{(\gamma_2/2)^{n-s}}{(n-s)!}\right], \tag{30}$$

where the coefficients γ_1,γ_2, and γ_{12} are usefully expressed as elements of the symmetric 2×2 matrix

$$\boldsymbol{\Gamma}=\begin{pmatrix}\gamma_1 & \gamma_{12}\\ \gamma_{12} & \gamma_2\end{pmatrix} \tag{31}$$

and are determined uniquely by the free parameters $\alpha^{(\infty)}_{2,0},\alpha^{(\infty)}_{0,2}$, and $\alpha^{(\infty)}_{1,1}$. A specific form for this correspondence is given in Proposition 4. The coefficients $\alpha^{(\infty)}_{mn}$ determine an un-normalized state vector $|\psi(\boldsymbol{\Gamma})\rangle$. In the Fock state representation, this state vector is given by

$$|\psi(\boldsymbol{\Gamma})\rangle=\hat{Q}(\boldsymbol{\Gamma})|0,0\rangle, \tag{32}$$

where the operator $\hat{Q}(\boldsymbol{\Gamma})$ is expressed in terms of $\boldsymbol{\Gamma}$ and the vector $\hat{\boldsymbol{a}}^\dagger=(\hat{a}_1^\dagger,\hat{a}_2^\dagger)^T$ as

$$\hat{Q}(\boldsymbol{\Gamma})=\exp\left[\frac{1}{2}(\hat{\boldsymbol{a}}^\dagger)^T\boldsymbol{\Gamma}(\hat{\boldsymbol{a}}^\dagger)\right]. \tag{33}$$

The state vectors $|\psi(\boldsymbol{\Gamma})\rangle$ are not normalized, and the requirement that they be normalizable, i.e. $\langle\psi(\boldsymbol{\Gamma})|\psi(\boldsymbol{\Gamma})\rangle$ is finite, places a restriction on $\boldsymbol{\Gamma}$. The following proposition takes its most concise form when we use the spectral norm that is defined as [16]

$$||\boldsymbol{X}||_\infty=\sqrt{\lambda_{\max}}, \tag{34}$$

where $\lambda_{\max}$ is the largest eigenvalue of $\boldsymbol{X}\boldsymbol{X}^\dagger$.

Proposition 3. If and only if $||\boldsymbol{\Gamma}||_\infty<1$, then $|\psi(\boldsymbol{\Gamma})\rangle:=\hat{Q}(\boldsymbol{\Gamma})|0,0\rangle$ is normalizable and represents a pure Gaussian state.

Proof: The matrix $\boldsymbol{\Gamma}$ in Eq. (31) is a complex symmetric 2×2 matrix. Following Takagi's Lemma [16], there exists a unitary matrix $\boldsymbol{U}$ such that

$$\boldsymbol{U}^T\boldsymbol{\Gamma}\boldsymbol{U}=:\boldsymbol{\Delta}, \tag{35}$$

where $\boldsymbol{\Delta}$ is a diagonal matrix the entries of which are the eigenvalues of $\sqrt{\boldsymbol{\Gamma}\boldsymbol{\Gamma}^\dagger}$. With $\hat{\boldsymbol{b}}:=\boldsymbol{U}\hat{\boldsymbol{a}}$, we have

$$|\psi(\boldsymbol{\Gamma})\rangle=\exp\left[\frac{1}{2}(\hat{\boldsymbol{b}}^\dagger)^T\boldsymbol{\Delta}(\hat{\boldsymbol{b}}^\dagger)\right]|0,0\rangle. \tag{36}$$

Because $\hat{b}_1$ and $\hat{b}_2$ commute, this is a tensor product of two single-mode Gaussian states. It is now straightforward to show that the single-mode state vectors are normalizable if and only if both diagonal elements of $\boldsymbol{\Delta}$ are smaller than 1. Then each of the modes is in a single-mode squeezed state [17]. The transformation $\hat{\boldsymbol{a}}\mapsto\boldsymbol{U}\hat{\boldsymbol{a}}$ represents a beam-splitter transformation mapping the original modes $\hat{\boldsymbol{a}}$ onto the modes $\hat{\boldsymbol{b}}$, i.e., it is a passive transformation. Hence, the resulting state vector (32) is also normalizable.

In fact, as can be shown, the state vector $\hat{Q}(\boldsymbol{\Gamma})|0,0\rangle$ is, apart from normalization, equal to the state vector of the two-mode squeezed vacuum state $\hat{S}(\boldsymbol{Z})|0,0\rangle$, where

$$\hat{S}(\boldsymbol{Z})=\exp\left[\frac{1}{2}(\hat{\boldsymbol{a}}^\dagger)^T\boldsymbol{Z}(\hat{\boldsymbol{a}}^\dagger)-\frac{1}{2}(\hat{\boldsymbol{a}})^T\boldsymbol{Z}^\dagger(\hat{\boldsymbol{a}})\right]. \tag{37}$$

$\hat{S}(\boldsymbol{Z})$ is a generalized two-mode squeezing operator [17],

$$\boldsymbol{Z}=-\begin{pmatrix}\zeta_1 & \zeta_{12}\\ \zeta_{12} & \zeta_2\end{pmatrix}, \tag{38}$$

where $\boldsymbol{Z}=\arctan(\boldsymbol{r}_\Gamma)e^{i\boldsymbol{\theta}_\Gamma}$ with the polar decomposition

$$\boldsymbol{\Gamma}=\boldsymbol{r}_\Gamma e^{i\boldsymbol{\theta}_\Gamma}. \tag{39}$$

Proposition 4. Suppose we are given a supply of identical two-mode pure states with state vectors $|\psi^{(0)}\rangle=\Sigma_{m,n}\alpha^{(0)}_{m,n}|m,n\rangle$, and let

$$\boldsymbol{\Gamma}:=\begin{pmatrix}\sqrt{2}\beta_{2,0}-\beta_{1,0}^2 & \beta_{1,1}-\beta_{1,0}\beta_{0,1}\\ \beta_{1,1}-\beta_{1,0}\beta_{0,1} & \sqrt{2}\beta_{0,2}-\beta_{0,1}^2\end{pmatrix}, \tag{40}$$

where $\beta_{m,n}:=\alpha^{(0)}_{m,n}/\alpha^{(0)}_{0,0}$. If $||\boldsymbol{\Gamma}||_\infty<1$ then

$$\lim_{i\to\infty}\alpha^{(i)}_{m,n}=\alpha_{m,n} \tag{41}$$

for all $n,m=0,1,\ldots,$ where

$$\alpha_{m,n}:=\langle m,n|\hat{Q}(\boldsymbol{\Gamma})|0,0\rangle. \tag{42}$$

Proof. To make the proof simpler, we shall use $\alpha^{(0)}_{0,0}=1$ as above. This is merely a change of normalization and does not alter the general validity of the argument. Before proving the convergence of all coefficients $\alpha^{(i)}_{m,n}$ under Φ to the fixed point $\alpha^{(\infty)}_{m,n}$ as $i\to\infty$, let us first show that a certain subset of coefficients actually reaches its final value after a single iteration of Φ.

The coefficients $\alpha^{(1)}_{2m+1,2n}$ and $\alpha^{(1)}_{2m,2n+1}$ reach zero, their fixed point, after a single iteration corresponding to $i=1$, for all m,n. To see this, note that in the following equation:

$$\alpha^{(1)}_{m,n}=2^{-(m+n)/2}\sum_{r=0}^{m}\sum_{s=0}^{n}(-1)^{(m+n)-(r+s)}\times\alpha^{(0)}_{r,s}\alpha^{(0)}_{m-r,n-s}\left[\binom{m}{r}\binom{n}{s}\right]^{1/2}, \tag{43}$$

renaming the summation indices $(r,s)\mapsto(m-r,n-s)$ yields an identical sum except for an overall factor of $(-1)^{m+n}$. Consequently, for odd values of $m+n$ the whole sum must vanish, and coefficients of the form $\alpha^{(1)}_{2m+1,2n}$ and $\alpha^{(1)}_{2m,2n+1}$ vanish after a single iteration step. As a consequence of this, the coefficients $\alpha^{(i)}_{1,1}$, $\alpha^{(i)}_{2,0}$, and $\alpha^{(i)}_{0,2}$ also do not change after one iteration. For example,

$$\alpha^{(i+1)}_{1,1}=\alpha^{(i)}_{1,1}-\alpha^{(i)}_{0,1}\alpha^{(i)}_{1,0} \tag{44}$$

for all $i=0,1,\ldots$. Similarly, $\alpha^{(1)}_{2,0}$ and $\alpha^{(1)}_{0,2}$ also assume their respective fixed points after the first iteration, and thus matrix $\mathbf{\Gamma}$ is determined to be as the one in Eq. (40).

Now let us show that all coefficients $\alpha^{(i)}_{m,n}$ do indeed converge to their respective fixed points $\alpha^{(\infty)}_{m,n}$ as $i\rightarrow\infty$. The recurrence relations in Eq. (23) can be rewritten as

$$\alpha^{(i+1)}_{m,n}=2^{-(m+n)/2}\left[2\alpha^{(i)}_{m,n}+\underbrace{\sum_{r=0}^{m}\sum_{s=0}^{n}}_{(r,s)\neq(0,0)\neq(m,n)}(-1)^{(m+n)-(r+s)}\alpha^{(i)}_{r,s}\alpha^{(i)}_{m-r,n-s}\left[\binom{m}{r}\binom{n}{s}\right]^{1/2}\right]. \tag{45}$$

Let us assume that all coefficients $\alpha^{(i)}_{r,s}$, where $r\leqslant m$, $s\leqslant n$ but $r+s<m+n$, do converge to the fixed points $\alpha^{(\infty)}_{r,s}$ as $i\rightarrow\infty$. Then

$$\lim_{i\rightarrow\infty}\alpha^{(i+1)}_{m,n}=2^{\{1-[(m+n)/2]\}}\lim_{i\rightarrow\infty}\alpha^{(i)}_{m,n}+2^{-(m+n)/2}\underbrace{\sum_{r=0}^{m}\sum_{s=0}^{n}}_{(r,s)\neq(0,0)\neq(m,n)}(-1)^{(m+n)-(r+s)}\alpha^{(\infty)}_{r,s}\alpha^{(\infty)}_{m-r,n-s}\left[\binom{m}{r}\binom{n}{s}\right]^{1/2}. \tag{46}$$

Now let us use the substitution $\delta^{(i)}_{m,n}:=\alpha^{(i)}_{m,n}-\alpha^{(\infty)}_{m,n}$ and we obtain, using Eq. (26),

$$\lim_{i\rightarrow\infty}\delta^{(i+1)}_{m,n}=2^{\{1-[(m+n)/2]\}}\lim_{i\rightarrow\infty}\delta^{(i)}_{m,n}. \tag{47}$$

We see that $\delta^{(i)}_{m,n}$ converges to zero as long as

$$2^{[1-(m+n)/2]}<1, \tag{48}$$

which is the case whenever $m+n>2$. However, since we have already shown that all coefficients $\alpha^{(i)}_{m,n}$, where $m+n\leqslant 2$, (i.e., $\alpha^{(i)}_{0,0}$, $\alpha^{(i)}_{0,1}$, $\alpha^{(i)}_{1,0}$, $\alpha^{(i)}_{1,1}$, $\alpha^{(i)}_{0,2}$, and $\alpha^{(i)}_{2,0}$), converge to a final value after a single iteration, the convergence of all other coefficients follows by induction. Note that whenever $\|\mathbf{\Gamma}\|_{\infty}\geqslant 1$, although the coefficients individually converge to their respective fixed points, the state as a whole does not since $\hat{Q}(\mathbf{\Gamma})|0,0\rangle$ is not a normalizable state vector.

IV. GENERATION OF THE INITIAL STATES FROM GAUSSIAN STATES

So far we did not specify where the supply of initial states should come from. In fact, one could use two (weakly) entangled Gaussian states and feed them into one of the iteration components as shown in Fig. 1. Then, instead of retaining the state in the case of measuring the vacuum, we now retain the state whenever *any* nonzero photon number is obtained. Again, only the detectors that distinguish between the absence or presence of photons are needed. Let us start with a supply of two-mode squeezed vacuum states, the state vectors of which can be written in Schmidt basis as

$$|\psi_q\rangle=\sqrt{1-q^2}\sum_{n=0}^{\infty}q^n|n,n\rangle, \tag{49}$$

with $q\in[0,1)$.

In general, it will be easier to generate two-mode squeezed states with low values of q in an experiment, and using the following simple protocol one can use a supply of such states to generate a supply of non-Gaussian states which, when used as the input of the procedure described in Sec. II, leads to the generation of two-mode squeezed states with much higher q.

Let us feed the two copies of the state of the form as in Eq. (49) with $q\ll 1$ into the device schematically depicted in Fig. 1, and retain those outcomes that correspond to a "click" in both detectors. It does not matter how many photons have been measured, and we do not assume that a different classical signal is associated with different photon numbers. The projection operator [18] describing this process is

$$\hat{P}=(\hat{\mathbb{1}}-|0\rangle\langle 0|)\otimes(\hat{\mathbb{1}}-|0\rangle\langle 0|). \tag{50}$$

Although the vacuum projection as well as the identity operation are Gaussian, the difference between them is not and, indeed, we find that when the states used in the protocol have sufficiently small q, then this projection approximates $|1\rangle\langle 1|\otimes|1\rangle\langle 1|$ with high accuracy. Thus, we are not in the situation as in Refs. [10,11]. Acting with Eq. (50) on the two copies of the state (49), after rotating them at the beam splitters, gives the non-Gaussian state with un-normalized state vector

$$|\Psi(q;T_A,R_A;T_B,R_B)\rangle:=\hat{P}[\hat{U}_{12}(T_A,R_A)\otimes\hat{U}_{12}(T_B,R_B)]|\psi_q\rangle^{\otimes 2}, \tag{51}$$

where again

$$\hat{U}_{12}(T,R) = T^{\hat{n}_1} e^{-R^* \hat{a}_2^\dagger \hat{a}_1} e^{R \hat{a}_2 \hat{a}_1^\dagger} T^{-\hat{n}_2} \tag{52}$$

and $T_A, T_B, R_A, R_B \in \mathbb{C}$ with

$$|T_A|^2 + |R_A|^2 = |T_B|^2 + |R_B|^2 = 1. \tag{53}$$

For simplicity of notation, let

$$\omega(q;T_A,R_A;T_B,R_B) := \frac{\mathrm{tr}_M[|\Psi(q;T_A,R_A;T_B,R_B)\rangle\langle\Psi(q;T_A,R_A;T_B,R_B)|]}{\mathrm{tr}[|\Psi(q;T_A,R_A;T_B,R_B)\rangle\langle\Psi(q;T_A,R_A;T_B,R_B)|]} \tag{54}$$

be the normalized state after application of the beam splitters and the two projections, where tr_M is the partial trace over the measured modes. The most appropriate choices for the reflectivities and transmittivities clearly depend on the value of q and on the figure of merit of how one quantifies the quality of the output state. However, when $q \in [0,1)$ is very small, the output state can be made arbitrarily close to a maximally entangled state

$$\rho^+ = \frac{1}{\sqrt{2}}[|0,0\rangle + e^{-i\phi}|1,1\rangle][\langle 0,0| + e^{i\phi}\langle 1,1|] \tag{55}$$

in 2×2 dimensions, where the phase $e^{i\phi}$ depends on the phases of T and R in the beam splitter chosen. More precisely,

$$\lim_{q \to 0} \|\omega(q;t(q),r(q);0,1) - \rho^+\|_1 = 0, \tag{56}$$

where

$$|t(q)| := \left|\frac{1-(1+8q^2)^{1/2}}{4q}\right|, \tag{57}$$

$$|r(q)| := [1-|t(q)|^2]^{1/2}, \tag{58}$$

and $\| \; \|_1$ denotes the trace norm [16]. In other words, in the limit of very small two-mode squeezing the maximally entangled state can be obtained to a high degree of accuracy. So the appropriate choice for the beam splitters on one side does depend on the value of q, whereas the beam splitter on the other side becomes redundant. In a similar manner, one can generate states of the form $|0,0\rangle + \alpha_{1,1}^{(0)}|1,1\rangle$. If one does not care about the phase of $\alpha_{1,1}$, then the correct choices for the above transmittivities and reflectivities are

$$|t(q)| := \left|\frac{|\alpha_{1,1}^{(0)}| - [|\alpha_{1,1}^{(0)}|^2 + 8q^2]^{1/2}}{4q}\right| \tag{59}$$

and $|r(q)| := [1-|t(q)|^2]^{1/2}$. This analysis shows that with the help of passive optical elements and photon detectors, quantum states of the appropriate kind can in fact be prepared. There is, however, a trade-off concerning accuracy of the protocol and success probability. For any finite q, the resulting states are not exactly pure, whereas the probability of success (such that the nonvacuum outcome is obtained in both detectors) is a monotone decreasing function of q.

The resulting states of this protocol can then form the starting point of the generation of Gaussian states via the protocol in Sec. II. In effect, this scheme allows one to generate approximate Gaussian states (in fact, two-mode squeezed vacua) with q higher than the initial supply, which is nothing other than a distillation procedure.

An example of the results of such a distillation protocol, where the initial step is followed by three iterations of the protocol from Sec. II, is illustrated in Fig. 4. The overall probability is far lower than for three steps of the protocol from Sec. II alone (cf. Fig. 2), due to the low success probability of the initial step. This is largely due to the low probability of measuring the presence of photons on the side where no beam splitter is employed, i.e. Alice's side. Since the effect of this measurement is to prepare a single photon

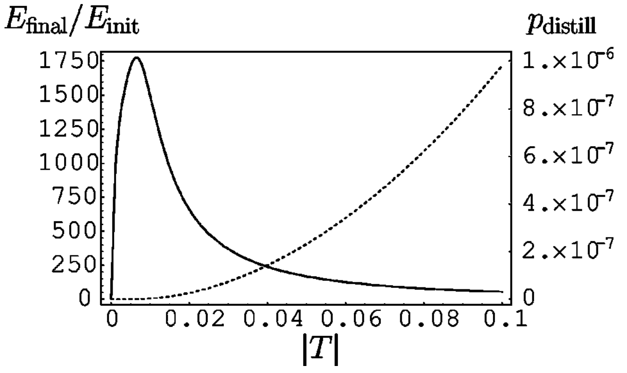

FIG. 4. This figure illustrates a full distillation procedure. Beginning with a supply of two-mode squeezed vacua, with $q = 0.01$, the protocol outlined in Sec. IV is then applied, which maps this state onto a non-Gaussian state of higher entanglement followed by three iterations of the protocol described in Sec. II. The properties of state produced depend on the transmittivity T of the beam splitter employed in the first step. Here, the factor by which the entanglement of the final achieved state E_{final} is greater than the entanglement of the initial supply E_{int} (where the entanglement is calculated as the Von Neumann entropy of the reduced density matrix of a single mode) is plotted as a solid line, and the overall success probability of the entire process, when this initial step is followed by the three iterations of the protocol to generate Gaussian states, is plotted as a dashed line.

on Bob's side, this low probability step could be avoided if a single photon source was available.

In light of the fact that distillation with Gaussian operations alone was shown to be impossible [10,11], it is then significant that this scheme does, in fact, realize pure-state distillation into *approximate* Gaussian states via suitable non-Gaussian operations, here photon detection.

This simple protocol is not suitable when the initial supply consists of two-mode squeezed states with a high q, and another method of generating non-Gaussian states of higher entanglement must be used. A more detailed analysis of optimal preparation protocols that only include passive optical elements and photon detectors will be investigated elsewhere. Here, we concentrate on the proof of principle that Gaussian states can indeed be distilled to approximately Gaussian states.

V. DISCUSSION AND CONCLUSIONS

We have shown that, using passive optical elements and photon detectors which do not distinguish different photon numbers, one can distill pure Gaussian states to arbitrarily high precision, in spite of the impossibility of distilling Gaussian states with Gaussian operations [10,11]. It should be noted that in our discussion we have assumed the photon detectors to have unit efficiency in order to show that how one can, in principle, generate Gaussian states from a non-Gaussian supply. Needless to say, in any experimental realization, one would have to deal with detector efficiencies significantly less than 1. Such detectors can, e.g., be modeled by employing perfect detectors, together with an appropriate beam splitter with an empty input port [19]. If the detector efficiency is still close to 1, one would expect—after a small number of iterations of the procedure—the resulting states to be still close to those presented in this idealized protocol. The convergence properties will, in general, be different from the ideal situation. Dark counts of the detector, in turn, do not affect the performance of the protocol, except that the success probability is decreased. These matters will be discussed in more detail elsewhere.

In several practical applications of the procedure, one can actually assume the initial state to be known. This is the case, for example, if one uses the above protocol in order to purify a state in a quantum privacy amplification procedure [9].

In this paper, we have restricted our analysis to pure states. In practical implementations, it would clearly also be useful to be able to distill highly entangled Gaussian states from a mixed initial supply. However, the full treatment of these protocols for general mixed states is lengthy and will be presented elsewhere. To summarize, we have identified a procedure that asymptotically produces Gaussian states from a supply of non-Gaussian, finite-dimensional states by means of Gaussian operations. In fact, the limiting Gaussian state for a pure given input can be found analytically. We have seen that even after a very small number of iteration steps, the degree of overlap between the resulting state and the theoretical limit state is close to unity. Moreover, the probability of obtaining this approximate state is of the order of 0.1. In that respect, the whole protocol is experimentally feasible with the present-day technology. This result should contribute to the search for strategies to distribute continuous-variable entanglement over large distances.

ACKNOWLEDGMENTS

We would like to thank I. Walmsley and J. I. Cirac for fruitful discussions, and K. Audenaert, A. Lund, and W.J. Munro for very helpful remarks on the manuscript. This work was partially funded by the Alexander von Humboldt Foundation, Hewlett-Packard Ltd., the EPSRC, and the European Commission (EQUIP).

[1] R.E. Slusher, L.W. Hollberg, B. Yurke, J.C. Mertz, and J.F. Valley, Phys. Rev. Lett. **55**, 2409 (1985); L.A. Wu, H.J. Kimble, J.L. Hall, and H. Wu, *ibid.* **57**, 2520 (1986); M.D. Reid and D.F. Walls, Phys. Rev. A **34**, 1260 (1986); Ch. Silberhorn, P.K. Lam, O. Weiss, F. König, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **86**, 4267 (2001); C. Schori, J.L. Sǿrensen, and E.S. Polzik, Phys. Rev. A **66**, 033802 (2002); M.M. Wolf, J. Eisert, and M.B. Plenio, Phys. Rev. Lett. **90**, 047904 (2003).

[2] Gaussian states of systems with canonical degrees of freedom are those states with a Gaussian Wigner function (or equivalently, a Gaussian characteristic function [15]).

[3] L. Vaidman, Phys. Rev. A **49**, 1473 (1994); S.L. Braunstein and H.J. Kimble, Phys. Rev. Lett. **80**, 869 (1998); G.J. Milburn and S.L. Braunstein, Phys. Rev. A **60**, 937 (1999).

[4] S.L. Braunstein and H.J. Kimble, Phys. Rev. A **61**, 042302 (2000).

[5] T.C. Ralph and P.K. Lam, Phys. Rev. Lett. **81**, 5668 (1998); M. Hillery, Phys. Rev. A **61**, 022309 (2000); D. Gottesman and J. Preskill, *ibid.* **63**, 022309 (2001); F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002); P. Navez, Eur. Phys. J. D **18**, 219 (2002); Ch. Silberhorn, T.C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[6] S.J. van Enk, J.I. Cirac, and P. Zoller, Science **279**, 205 (1998); S. Scheel and D.-G. Welsch, Phys. Rev. A **64**, 063811 (2001); e-print quant-ph/0207114.

[7] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996), see also Refs. [8].

[8] J.-W. Pan, C. Simon, C. Brukner, and A. Zeilinger, Nature (London) **410**, 1067 (2001); X.B. Wang, e-print quant-ph/0208166.

[9] H. Aschauer and H.J. Briegel, Phys. Rev. Lett. **88**, 047902 (2002); H. Aschauer and H.J. Briegel, Phys. Rev. A **66**, 032302 (2002).

[10] J. Eisert, S. Scheel, and M.B. Plenio, Phys. Rev. Lett. **89**, 137903 (2002).

[11] J. Fiurášek, Phys. Rev. Lett. **89**, 137904 (2002); G. Giedke and J.I. Cirac, Phys. Rev. A **66**, 032316 (2002).

[12] B. Demoen, P. Vanheuverzwijn, and A. Verbeure, Lett. Math.

Phys. **2**, 161 (1977); B. Demoen, P. Vanheuverzwijn, and A. Verbeure, Rep. Math. Phys. **15**, 27 (1979); J. Eisert and M.B. Plenio, Phys. Rev. Lett. **89**, 097901 (2002); J. Fiuráŝek, Phys. Rev. A **66**, 012304 (2002).

[13] L.-M. Duan, G. Giedke, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000); T. Opatrný, G. Kurizki, and D.-G. Welsch, Phys. Rev. A **61**, 032302 (2000); L.-M. Duan, G. Giedke, J.I. Cirac, and P. Zoller, *ibid.* **62**, 032304 (2000); G. Giedke, L.-M. Duan, J.I. Cirac, and P. Zoller, Quantum Inf. Comput. **1**, 79 (2001); P.T. Cochrane, T.C. Ralph, and G.J. Milburn, Phys. Rev. A **65**, 062306 (2002).

[14] Note that this convergence is pointwise convergence for the coefficients specifying the state vector.

[15] W. Vogel, D.-G. Welsch, and S. Wallentowitz, *Quantum Optics, An Introduction* (Wiley-VCH, Weinheim, 2001).

[16] R.A. Horn and C.R. Johnson, *Matrix Analyis* (Cambridge University Press, Cambridge, 1987).

[17] X. Ma and W. Rhodes, Phys. Rev. A **41**, 4625 (1990).

[18] S.D. Bartlett and B.C. Sanders, Phys. Rev. A **65**, 042304 (2002).

[19] K. Nemoto and S.L. Braunstein, Phys. Rev. A **66**, 032306 (2002).