Additivity properties of a Gaussian channel

Vittorio Giovannetti[1] and Seth Lloyd[1,2]
[1]*Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA*
[2]*Department of Mechanical Engineering, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA*

(Received 10 March 2004; published 7 June 2004)

The Amosov-Holevo-Werner conjecture implies the additivity of the minimum Rényi entropies at the output of a channel. The conjecture is proven true for all Rényi entropies of integer order greater than two in a class of Gaussian bosonic channel where the input signal is randomly displaced or where it is coupled linearly to an external environment.

DOI: 10.1103/PhysRevA.69.062307 PACS number(s): 03.67.Hk, 03.65.Db, 42.50.−p

One of the most challenging open questions of quantum communication theory is the additivity of the various quantities characterizing the information transmission in a channel [1]. The issue at hand is whether quantum entanglement is able to improve the performance of classical protocols [2,3]. The supposed additivity of the Holevo information [4] is the most important example of this kind of issue. The maximum of this quantity over all possible encoding procedures is known to provide the capacity C_1 in transmitting classical information for a single use of the channel. However, if the sender of the message is allowed to encode messages in entangled states among m successive uses of the communication line, then the resulting capacity per channel use might be higher than C_1 [5]. For this reason to compute the ultimate classical capacity C of the channel it is necessary to introduce a regularization of the Holevo information where a limit $m \to \infty$ has to be performed [1,5]. All this could be avoided if only the Holevo information was shown to be an additive quantity. Up to now no channel has been found for which this regularization is necessary; on the contrary, all the channels for which the value of C has been calculated have additive Holevo information [6–8].

The additivity of the Holevo information has been linked to the additivity of other relevant quantities in Ref. [1]. In particular, it is known that proving the additivity of the Holevo information is equivalent to proving the additivity of the minimum von Neumann entropy $\mathbb{S}$ at the output of the channel. Given a channel described by the completely positive (CP) linear map $\mathcal{M}$ on the input space $\mathcal{H}$, this quantity is defined as

$$\mathbb{S}(\mathcal{M}^{\otimes m}) \equiv \min_{\rho \in \mathcal{H}^{\otimes m}} S(\mathcal{M}^{\otimes m}(\rho)), \tag{1}$$

where the minimization is performed over all the possible input states ρ of m successive uses of the channel, and where $S(\rho) \equiv -\mathrm{Tr}[\rho \ln \rho]$. The additivity hypothesis requires $\mathbb{S}(\mathcal{M}^{\otimes m})$ to be equal to m times the minimum entropy for a single use of the channel $\mathbb{S}(\mathcal{M})$: this conjecture seems simpler to study than the additivity of the Holevo information and some authors have focused their attention to it [8–11]. As a matter of fact the alleged additivity of the $\mathbb{S}$ is just a particular instance of the Amosov-Holevo-Werner conjecture [12] which requires the maximum of the output z norm $\nu_z(\mathcal{M}^{\otimes m})$ of the channel to be multiplicative, i.e., it requires that for m integer

$$\nu_z(\mathcal{M}^{\otimes m}) \equiv \max_{\rho \in \mathcal{H}^{\otimes m}} \|\mathcal{M}^{\otimes m}(\rho)\|_z = [\nu_z(\mathcal{M})]^m, \tag{2}$$

where the maximization is performed again over all the input states of m uses of the channel and where

$$\|A\|_z \equiv (\mathrm{Tr}|A|^z)^{1/z}, \quad z \geqslant 1 \tag{3}$$

is the z norm of the operator A. In other words, the conjecture requires the maximization in the left-hand side of Eq. (2) to be achieved on nonentangled states of $\mathcal{H}^{\otimes m}$. The connection between the property of Eq. (2) and the additivity of the minimal output entropy can be established through the quantum Rényi entropy,

$$S_z(\rho) \equiv -\frac{\ln \mathrm{Tr}[\rho^z]}{z-1}. \tag{4}$$

This quantity is monotonic with respect to the z norm (3) of the state ρ. For $z=2$ the Rényi entropy is a function of the linear entropy $1-\mathrm{Tr}[\rho^2]$ and in the limit $z \to 1$ it tends to the von Neumann entropy [13]. As for the case of S one can define the minimal value

$$\mathbb{S}_z(\mathcal{M}^{\otimes m}) \equiv \min_{\rho \in \mathcal{H}^{\otimes m}} S_z(\mathcal{M}^{\otimes m}(\rho)). \tag{5}$$

If the Amosov-Holevo-Werner conjecture (2) is true then the minimum output z-Rényi entropy is additive and vice versa. Moreover, if such property is verified for values of z arbitrarily close to 1 then the additivity of $\mathbb{S}$ (and hence of the Holevo information) follows [14].

In this paper we will analyze the conjecture (2) for a set of Gaussian channels and prove that it is true for all integer z. The material is organized as follows. In Sec. I we introduce the simple Gaussian channel model $\mathcal{N}_n$ and in Secs. I A and I B we show that the conjecture (2) applies to this channel when z is integer. In Sec. I C we analyze the case of generic

1050-2947/2004/69(6)/062307(9)/$22.50

z giving some bounds for $\nu_z(\mathcal{N}_n^{\otimes m})$. In Sec. II we generalize the results of the first section to a whole class of Gaussian channels.

I. THE CHANNEL MODEL

The channel we analyze here is a bosonic linear channel where the photonic signal from the sender is displaced randomly by the environment. This system is described by the CP map $\mathcal{N}_n$ which transforms the input state of the channel into the output

$$\mathcal{N}_n(\rho) = \int d^2\mu P_n(\mu) D(\mu)\rho D^\dagger(\mu), \tag{6}$$

where for $n \geqslant 0$, $P_n(\mu)$ is the circularly symmetric probability distribution

$$P_n(\mu) = \frac{e^{-|\mu|^2/n}}{\pi n}, \tag{7}$$

and $D(\mu) \equiv \exp(\mu a^\dagger - \mu^* a)$ is the displacement operator of the annihilation a of the input signal. This channel is Gaussian, i.e., it maps the set of input states with Gaussian symmetrically characteristic function into itself [15]. Moreover, the map (6) is unital (i.e., it transforms the identity operator into itself) and it is covariant under displacement or phase transformation [10]. When $\mathcal{N}_n$ acts on a coherent state $\rho_\alpha \equiv |\alpha\rangle\langle\alpha|$ the following transformation takes place:

$$\rho_\alpha \to \mathcal{N}_n(\rho_\alpha) = D(\alpha)\tau(n)D^\dagger(\alpha), \tag{8}$$

with

$$\tau(n) \equiv \frac{1}{n+1}\left(\frac{n}{n+1}\right)^{a^\dagger a}, \tag{9}$$

the thermal state that gives the output of the channel for a vacuum input [10]. The state $\mathcal{N}_n(\rho_\alpha)$ has z norm (3) equal to

$$\|\mathcal{N}_n(\rho_\alpha)\|_z \equiv \left[\frac{1}{(n+1)^z - n^z}\right]^{1/z}, \tag{10}$$

which does not depend on α since it is invariant under the unitary transformation $D(\alpha)$. In Ref. [11] the right-hand side of Eq. (10) was shown to coincide with the z norm of the single use of the channel $\nu_z(\mathcal{N}_n)$, at least for all $z=k$ integer. In Sec. I A we will generalize this result showing that, for all integer k, the classical channel satisfies the identity,

$$\nu_k(\mathcal{N}_n^{\otimes m}) = \left[\frac{1}{(n+1)^k - n^k}\right]^{m/k}, \tag{11}$$

hence proving the conjecture (2) for integer $z=k$ for the channel $\mathcal{N}_n$. Equations (10) and (11) imply that the maximization implicit in the definition of $\nu_k(\mathcal{N}_n^{\otimes m})$ is achievable with separable input states of the form $|\alpha_1\rangle_1 \otimes \cdots \otimes |\alpha_m\rangle_m$, i.e., by feeding the channel with a coherent state in each of the m successive uses. This result will be proven explicitly in Sec. I B.

A. The proof

In this section we show that Eq. (11) applies for integer z. Clearly, the right-hand side of this equation is a lower bound for the left-hand side: the former is in fact the output z norm associated to the input signal where the m uses of the channel have been prepared in coherent states. To prove the equality in Eq. (11) it is hence sufficient to show that the right-hand side is also an upper bound for $\nu_k(\mathcal{N}_n^{\otimes m})$, i.e., that for all input states $\rho \in \mathcal{H}^{\otimes m}$ the following inequality applies.

$$\mathrm{Tr}\{[\mathcal{N}_n^{\otimes m}(\rho)]^k\} \leqslant \left[\frac{1}{(n+1)^z - n^z}\right]^m. \tag{12}$$

The method to derive this property is similar to the one given in Ref. [11] where an analogous approach was used to calculate the minimum output Rényi entropy (4) of integer order for a single channel use ($m=1$). The only difference is that here we are dealing with an extra tensorial structure associated with $m>1$. For the sake of clarity we divide the proof in two separate parts. First we show that the quantity on the left-hand side of Eq. (12) can be expressed as the expectation value of a Hermitian operator Θ which acts on the Hilbert space $(\mathcal{H}^{\otimes m})^{\otimes k}$: this allows us to derive an upper bound for $\mathrm{Tr}\{[\mathcal{N}_n^{\otimes m}(\rho)]^k\}$ by considering the eigenvalue λ_0 of Θ with maximum absolute value. The second part of the proof is devoted to the analysis of the tensorial structure of Θ and to the proof that λ_0 coincides with the left-hand side of Eq. (12).

1. Part one

Without loss of generality we can assume the initial state of the m uses of the channel to be pure, i.e., $\rho = |\psi\rangle\langle\psi|$. The convexity of the norm (3) guaranties in fact that the maximization in Eq. (2) is achievable with pure input states [12,14]: thus if Eq. (12) holds for all pure states, then it is valid also for all the other channel inputs. In general, $|\psi\rangle$ will be entangled among the various channel uses and the corresponding output state will be

$$\begin{aligned}\mathcal{N}_n^{\otimes m}(\rho) = \int d^2\mu_1 \cdots d^2\mu_m P_n(\mu_1)\cdots P_n(\mu_m)\\ \times D_1(\mu_1)\cdots D_m(\mu_m)\rho D^\dagger(\mu_1)\cdots D_m^\dagger(\mu_m),\end{aligned} \tag{13}$$

where $D_r(\mu) \equiv \exp(\mu a_r^\dagger - \mu^* a_r)$ is the displacement associated with the annihilation operator a_r of the rth use of the channel. Equation (13) can be expressed in a more compact form by introducing a vectorial notation, where $\vec{\mu} \equiv (\mu_1, \ldots, \mu_m)$ is a complex vector in $\mathbb{C}^m$ and $\vec{a} \equiv (a_1, \ldots, a_m)$. The output state becomes thus

$$\mathcal{N}_n^{\otimes m}(\rho) = \int d^2\vec{\mu} P_n(\vec{\mu}) D(\vec{\mu}) \rho D^\dagger(\vec{\mu}), \tag{14}$$

where

$$P_n(\vec{\mu}) \equiv \frac{\exp[-|\vec{\mu}|^2/n]}{(\pi n)^m} \tag{15}$$

and $D(\vec{\mu}) = \exp(\vec{\mu}\cdot\vec{a}^{\,\dagger} - \vec{a}\cdot\vec{\mu}^\dagger)$ is a multimode displacement operator where the input of the rth use of the channel is displaced by μ_r. Consider now for $z=k$ integer the quantity

$$\mathrm{Tr}\{[\mathcal{N}_n^{\otimes m}(\rho)]^k\} = \int d^2\vec{\mu}_1 \cdots d^2\vec{\mu}_k P_n(\vec{\mu}_1) \cdots P_n(\vec{\mu}_k) \times \mathrm{Tr}[D(\vec{\mu}_1)\rho D^\dagger(\mu_1) \cdots D(\vec{\mu}_k)\rho D^\dagger(\mu_k)]. \tag{16}$$

Since $\rho = |\psi\rangle\langle\psi|$, the trace in the integral can be expressed as the expectation value of a Hermitian operator Θ which acts in an extended Hilbert space $(\mathcal{H}^{\otimes m})^{\otimes k}$ made of k copies of the initial one. In fact, from the invariance of the trace under cyclic permutation we have

$$\begin{aligned}
&\mathrm{Tr}[D(\vec{\mu}_1)\rho D^\dagger(\vec{\mu}_1) \cdots D(\vec{\mu}_k)\rho D^\dagger(\vec{\mu}_k)] \\
&\quad = \langle\psi|D^\dagger(\vec{\mu}_1)D(\vec{\mu}_2)|\psi\rangle\langle\psi|D^\dagger(\vec{\mu}_2)D(\vec{\mu}_3)|\psi\rangle \cdots \langle\psi|D^\dagger(\vec{\mu}_k)D(\vec{\mu}_1)|\psi\rangle \\
&\quad = \mathrm{Tr}\{(\rho\otimes\rho\otimes\cdots\otimes\rho)[D_1^\dagger(\vec{\mu}_1)D_1(\vec{\mu}_2)\otimes D_2^\dagger(\vec{\mu}_2)D_2(\vec{\mu}_3)\otimes\cdots\otimes D_k^\dagger(\vec{\mu}_k)D_k(\vec{\mu}_1)]\},
\end{aligned} \tag{17}$$

where k scalar products in the input Hilbert space $\mathcal{H}^{\otimes m}$ in the second line were replaced with a single expectation value in $(\mathcal{H}^{\otimes m})^{\otimes k}$ in the third line. In Eq. (17) the operator $D_s(\vec{\mu})$ represents the multimode displacement that operates on the sth copy of $\mathcal{H}^{\otimes m}$, i.e.,

$$D_s(\vec{\mu}) = \exp(\vec{\mu}\cdot\vec{a}_s^\dagger - \vec{a}_s\cdot\vec{\mu}^\dagger), \tag{18}$$

where for $s=1,\ldots,k$,

$$\vec{a}_s \equiv (a_{s1}, a_{s2}, \ldots, a_{sm}), \tag{19}$$

are the m annihilation operators pertaining to the sth copy of $\mathcal{H}^{\otimes m}$. With this trick Eq. (16) can be written as

$$\mathrm{Tr}\{[\mathcal{N}_n^{\otimes m}(\rho)]^k\} = \mathrm{Tr}[(\rho\otimes\cdots\otimes\rho)\Theta], \tag{20}$$

where each of the k copies of the state ρ is associated to one of the multimode annihilation operator $\vec{a}_s$ and where Θ the Hermitian operator on $(\mathcal{H}^{\otimes m})^{\otimes k}$ is given by

$$\Theta = \int d^2\vec{\mu}_1 \cdots d^2\vec{\mu}_k P_n(\vec{\mu}_1)\cdots P_n(\vec{\mu}_k) \times D_1^\dagger(\vec{\mu}_1)D_1(\vec{\mu}_2)\otimes\cdots\otimes D_k^\dagger(\vec{\mu}_k)D_k(\vec{\mu}_1). \tag{21}$$

Equation (20) allows us to derive an upper bound for the quantity on the left-hand side by considering the eigenvalue λ_0 of Θ with maximum absolute value, i.e.,

$$\mathrm{Tr}\{[\mathcal{N}_n^{\otimes m}(\rho)]^k\} \leqslant |\lambda_0|. \tag{22}$$

2. Part two

To calculate λ_0 it is useful to analyze in details the properties of the operator Θ. As shown in Appendix A 1, this operator has a very simple tensorial form with respect to the index r. In fact Eq. (22) can be decomposed as

$$\Theta = \bigotimes_{r=1}^{m} \Theta_r, \tag{23}$$

where, for $r=1,\ldots,m$, the operator Θ_r acts on the modes associated with the annihilation operators

$$\overleftarrow{a}_r \equiv (a_{1r}, a_{2r}, \ldots, a_{kr}). \tag{24}$$

In vectorial notation Θ_r can be expressed as

$$\Theta_r \equiv \int \frac{d^2\overleftarrow{\mu}_r}{(\pi n)^k} e^{-\overleftarrow{\mu}_r\cdot C\cdot\overleftarrow{\mu}_r^\dagger + \overleftarrow{\mu}_r\cdot G^\dagger\cdot\overleftarrow{a}_r^\dagger - \overleftarrow{a}_r\cdot G\cdot\overleftarrow{\mu}_r^\dagger}, \tag{25}$$

where, as in Eq. (24), $\overleftarrow{\mu}_r \equiv (\mu_{1r}, \mu_{2r}, \ldots, \mu_{kr})$ is a k-element vector, and where G and

$$C \equiv \frac{\mathbb{1}}{n} + \frac{A}{2} \tag{26}$$

are $k\times k$ real matrices ($\mathbb{1}$ is the identity). For $k \geqslant 3$, G and A are

$$G \equiv \begin{bmatrix} -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & -1 & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \\ 0 & 0 & 0 & \cdots & -1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & -1 \end{bmatrix}, \tag{27}$$

$$A \equiv \begin{bmatrix} 0 & -1 & 0 & \cdots & 0 & 1 \\ 1 & 0 & -1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \\ 0 & 0 & 0 & \cdots & 0 & -1 \\ -1 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}. \tag{28}$$

For $k=2$, A is null, while for $k=1$ both G and A are null. The decomposition (23) shows that in the right-hand side of Eq. (20) we have a product of two operators of $(\mathcal{H}^{\otimes m})^{\otimes k}$ which have "orthogonal" tensorial decomposition; the operator $\rho\otimes\cdots\otimes\rho$ factorizes with respect to the index $r=1,\ldots,k$, while Θ factorizes with respect to the index $s=1,\ldots,m$ associated with the successive uses of the channel. This property is common to all memoryless channels where the corresponding CP map acts on each channel use independently. However, the channel model we are considering allows us to further decompose the operator Θ. In fact, G and A of Eqs. (27) and (28) are two circulant matrices [16] which commute and possess a common basis of orthogonal eigenvectors. This means that there exists a $k\times k$ unitary matrix Y for which

$$D \equiv YCY^\dagger = \mathbb{1}/n + YAY^\dagger,$$

$$E \equiv YGY^\dagger \tag{29}$$

are diagonal. Since A is antisymmetric, its eigenvalues $i\xi_j$ are imaginary and the diagonal elements of D (i.e., the quantities $d_j=1/n+i\xi_j$) have positive real part. Using these properties we can rewrite the operator Θ_r of Eq. (25) in factorized form by performing the change of integration variables $\overleftarrow{v}_r \equiv \overleftarrow{\mu}_r\cdot Y^\dagger$ and introducing the new annihilation operators

$$\overleftarrow{b}_r \equiv (b_{1r}, b_{2r}, \ldots, b_{kr}) = \vec{a}_r\cdot Y^\dagger. \tag{30}$$

These operations yield

$$\Theta_r = \overset{k}{\underset{j=1}{\otimes}} \Theta_{jr}, \tag{31}$$

with

$$\Theta_{jr} \equiv \frac{1}{n|e_j|^2}\int \frac{d^2\nu}{\pi}\, e^{-d_j|\nu|^2/|e_j|^2} D_{b_{jr}}(-\nu), \tag{32}$$

where $D_{b_{jr}}(\nu)\equiv\exp(\nu b_{jr}^\dagger - \nu^* b_{jr})$ is the displacement operator associated with b_{jr}, while e_j is the jth diagonal elements of the matrix E (i.e., the jth eigenvalue of G). As demonstrated in Refs. [10,17], this expression can be further simplified, proving that Θ_{jr} is diagonal in the Fock basis of the mode b_{jr} and equal to

$$\Theta_{jr} = \frac{2/n}{2d_j+|e_j|^2}\left(\frac{2d_j-|e_j|^2}{2d_j+|e_j|^2}\right)^{b_{jr}^\dagger b_{jr}} \tag{33}$$

(for the sake of completeness we give an alternative derivation of this result in Appendix A 2).

Equations (23), (31), and (33) show that the eigenvalues of Θ are products of eigenvalues of Θ_{jr}. In particular, λ_0 of Eq. (22) is obtained by taking the eigenvalues of the Θ_{jr} that have maximum absolute value. Since the constants d_j have positive real part, the quantities we are looking for are $2/[n(2d_j+|e_j|^2)]$, i.e., they are the eigenvalues of the operators Θ_{jr} associated with the vacuum state of the mode b_{jr}. This allows us to express the value of λ_0 as

$$\lambda_0 = \prod_{r=1}^{m}\prod_{j=1}^{k}\frac{2/n}{2d_j+|e_j|^2} = \left\{\frac{1/n^k}{\det[C+G^\dagger G/2]}\right\}^m$$

$$= \left[\frac{1}{(n+1)^k-n^k}\right]^m, \tag{34}$$

which, replaced in Eq. (22), proves the thesis (12). [In deriving the second identity we have used the invariance of the determinant under the unitary transformation Y, while the last identity can be obtained from the definitions (27) and (28) by direct calculation of the determinant itself].

B. Optimal inputs

Equations (10) and (11) prove that tensor products of coherent states are optimal since they allow the channel $\mathcal{N}_n$ to achieve the maximal k norm at the output of m successive uses. Here we rederive this result by showing that the state $\rho\otimes\cdots\otimes\rho$ of Eq. (20) with ρ given by a tensor product of coherent states in the input modes $\vec{a}_s$ is an eigenvector of Θ associated with the eigenvalue λ_0 of Eq. (34).

From the analysis of the preceding section we know that the eigenvectors of λ_0 can be written as

$$|\Phi\rangle \equiv \overset{m}{\underset{r=1}{\otimes}} |\Phi_r\rangle_r, \tag{35}$$

where $|\Phi_r\rangle_r$ is an eigenvector of Θ_r of Eq. (31) relative to its eigenvalue with maximum absolute value. For instance, in deriving Eq. (34) we have considered the state where each of the $\overleftarrow{b}_r$ modes is in the vacuum. However, this is not the only possibility. In fact, we notice that for any k the matrices G and A of Eqs. (27) and (28) have a null eigenvalue (say for $j=1$), associated with the common normalized eigenvector $(1,1,\ldots,1)/\sqrt{k}$. On one hand, this means that all the elements in the first row of the matrix Y of Eq. (29) are equal to $1/\sqrt{k}$. On the other hand, this implies also that $e_1=0$, $d_1=1/n$ and, according to Eq. (33),

$$\Theta_{1r} = \mathbb{1}_{1r}. \tag{36}$$

This means that any state of the form

$$|\Phi_r\rangle_r \equiv |\phi_r\rangle_{b_{1r}}\otimes|0\rangle_{b_{2r}}\otimes\cdots\otimes|0\rangle_{b_{kr}}, \tag{37}$$

where the mode b_{1r} is prepared in a generic state $|\phi_r\rangle$ while the other b_{jr} are in the vacuum, is an eigenstate of Θ_r relative to the eigenvalue with maximum absolute value. Consider now the case of $|\phi_r\rangle=|\sqrt{k}\alpha_r\rangle$ coherent. By using the symmetric characteristic function decomposition [18] we can show that, when expressed in terms of the operators $\vec{a}_r$, the state (37) is a tensor product of coherent states $|\alpha_r\rangle$. In fact, defining the complex vector $\overleftarrow{\gamma}\equiv(\sqrt{k}\alpha_r,0,\ldots,0)$ we can express the state $|\Phi_r\rangle_r$ as

$$\begin{aligned}|\Phi_r\rangle_r\langle\Phi_r| &= \int\frac{d^2\overleftarrow{v}}{\pi^k}\exp[-|\overleftarrow{\nu}|^2/2+\overleftarrow{\nu}\cdot(\overleftarrow{b}_r-\overleftarrow{\gamma})^\dagger-(\overleftarrow{b}_r-\overleftarrow{\gamma})\cdot\overleftarrow{v}^{\,\dagger}]\\ &= \int\frac{d^2\overleftarrow{\mu}}{\pi^k}\exp[-|\overleftarrow{\mu}|^2/2+\overleftarrow{\mu}\cdot(\overleftarrow{a}_r^{\,\dagger}-Y^\dagger\cdot\overleftarrow{\gamma})\\ &\quad-(\overleftarrow{a}_r-\overleftarrow{\gamma}\cdot Y)\cdot\overleftarrow{\mu}^\dagger]\\ &= |\alpha_r\rangle_{a_{1r}}\langle\alpha_r|\otimes\cdots\otimes|\alpha_r\rangle_{a_{kr}}\langle\alpha_r|,\end{aligned}\tag{38}$$

where the second identity is obtained by substituting the $\overleftarrow{\nu}$ with $\overleftarrow{\mu}\cdot Y^\dagger$ in the integral, while the third identity derives from the properties of the matrix Y discussed above. The thesis finally follows by replacing this expression in Eq. (35),

$$|\Phi\rangle\langle\Phi| = \bigotimes_{r=1}^{m}(|\alpha_r\rangle_{a_{1r}}\langle\alpha_r|\otimes\cdots\otimes|\alpha_r\rangle_{a_{kr}}\langle\alpha_r|),\tag{39}$$

and observing that this can be represented as $\rho\otimes\cdots\otimes\rho$ of Eq. (20) with $\rho=(\otimes_{r=1}^{m}|\alpha_r\rangle\langle\alpha_r|)^{\otimes k}$.

C. Upper bound

In this section, starting from the values of the $\nu_z(\mathcal{N}_n^{\otimes m})$ for z integer derived in the preceding section, we give some upper bounds for the channel z norm of generic order.

The Rényi entropy of Eq. (4) is decreasing function of the parameter z. As a matter of fact, it obeys the inequality [13]

$$\frac{z-1}{z}S_z(\rho)\geqslant\frac{z'-1}{z'}S_{z'}(\rho),\tag{40}$$

which applies for any $z\geqslant z'$ and for all ρ. This property and the monotonicity of $S_z(\rho)$ with respect to the norm of Eq. (3) can be used to derive the relation $\|\rho\|_z\leqslant\|\rho\|_{z'}$ which, when applied to the output state of a channel $\mathcal{M}$, implies

$$\nu_z(\mathcal{M}^{\otimes m})\leqslant\nu_{z'}(\mathcal{M}^{\otimes m}),\quad z\geqslant z'\geqslant 1.\tag{41}$$

In the case of the channel $\mathcal{N}_n$, by choosing $z'=k$ integer and using the identity (11) we obtain the upper bound for all $z\geqslant k$, i.e.,

$$\left[\frac{1}{(n+1)^k-n^k}\right]^{m/k}\geqslant\nu_z(\mathcal{N}_n^{\otimes m}).\tag{42}$$

This bound must be compared with the lower bound

$$\left[\frac{1}{(n+1)^z-n^z}\right]^{m/z}\leqslant\nu_z(\mathcal{N}_n^{\otimes m})\tag{43}$$

for arbitrary z that derives by considering as input of the m successive uses of the channel a tensor product of coherent states. These two bounds are plotted in Fig. 1.

II. GENERALIZATION

In this section we show that the results obtained for the channel $\mathcal{N}_n$ apply also to other Gaussian channel models. The first group we analyze is formed by the *classical* channels $\mathcal{G}$ where, as in the case of $\mathcal{N}_n$, the photonic signal from the sender is displaced randomly in phase space according to a Gaussian distribution. The second group is formed by the channels $\mathcal{L}$ where the input signal is linearly coupled to an external environment prepared in a Gaussian state.

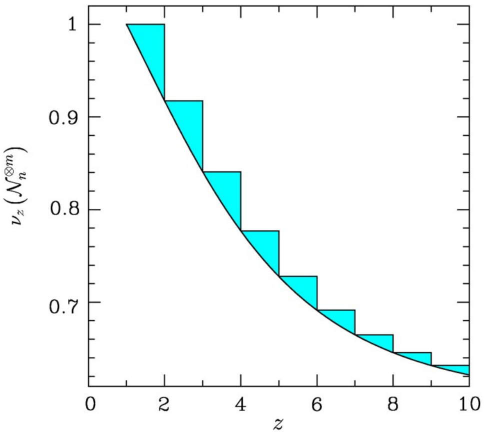

FIG. 1. Plot of the bounds of the z norm $\nu_z(\mathcal{N}_n^{\otimes m})$ of the channel $\mathcal{N}_n$. The function $\nu_z(\mathcal{N}_n^{\otimes m})$ is restricted to the gray area which is limited from above by the upper bound of Eq. (42) and from below by the lower bound of Eq. (43). The two curves meet for the $z=k$ integer. Here $m=2$ and $n=0.3$.

A. Classical channels

Consider CP map $\mathcal{G}$ which transforms the input state ρ into the output state

$$\begin{aligned}\mathcal{G}(\rho)=\int d^2\zeta\,\frac{\exp(-\zeta\Gamma\zeta^\dagger)}{\pi/2(\sqrt{\det[\Gamma]})}&\exp[(a,a^\dagger)\zeta^\dagger]\rho\\ \times\exp[-(a,a^\dagger)\zeta^\dagger],\end{aligned}\tag{44}$$

where $\zeta=(\mu,-\mu^*)$ and

$$\Gamma\equiv\begin{bmatrix}u & v^*\\ v & u\end{bmatrix},\quad u\geqslant|v|,\tag{45}$$

is a 2×2 positive Hermitian matrix [19]. For $\Gamma=\mathbb{1}/(2n)$ the map $\mathcal{G}$ gives $\mathcal{N}_n$ of Sec. I, while for generic Γ the channel (44) is the generalization of $\mathcal{N}_n$ to the case of noncircularly symmetric distribution (7). As shown in Appendix B, the map $\mathcal{G}(\rho)$ can be decomposed according to the relation

$$\mathcal{G}(\rho)=\Sigma^\dagger(\xi)\mathcal{N}_n(\Sigma(\xi)\rho\Sigma^\dagger(\xi))\Sigma(\xi),\tag{46}$$

where

$$n=1/(2\sqrt{u^2-|v|^2}),\tag{47}$$

$$\xi=\frac{v}{|v|}\,\mathrm{arctanh}\left[\left(\frac{u-\sqrt{u^2-|v|^2}}{u+\sqrt{u^2-|v|^2}}\right)^{1/2}\right],\tag{48}$$

and where

$$\Sigma(\xi) \equiv \exp\{[\xi^* a^2 - \xi(a^\dagger)^2]/2\} \tag{49}$$

is the squeezing operator. In other words, for any input state ρ, the output state $\mathcal{G}(\rho)$ can be obtained by applying the squeezing operator $\Sigma(\xi)$ to ρ, then sending it through the channel $\mathcal{N}_n$, and, finally, applying the antisqueezing transformation $\Sigma(\xi)^\dagger$. We can thus consider $\mathcal{N}_n$ as a simplified version of $\mathcal{G}$ where all the squeezing operations have been removed.

An important consequence of Eq. (46) is that the z norms of the channels $\mathcal{G}$ and $\mathcal{N}_n$ are identical. In fact, using the invariance of the norm (3) under the unitary operation $\Sigma^\dagger(\xi)^{\otimes m}$, we can write the z norm of m uses of the channel $\mathcal{G}$ as

$$\begin{aligned}\nu_z(\mathcal{G}^{\otimes m}) &= \max_{\rho\in\mathcal{H}^{\otimes m}} \|\mathcal{N}_n^{\otimes m}(\Sigma(\xi)^{\otimes m}\rho\Sigma^\dagger(\xi)^{\otimes m})\|_z \\ &= \max_{\rho\in\mathcal{H}^{\otimes m}} \|\mathcal{N}_n^{\otimes m}(\rho)\|_z \equiv \nu_z(\mathcal{N}_n^{\otimes m}),\end{aligned} \tag{50}$$

where, in the second identity, the unitary operator $\Sigma(\xi)^{\otimes m}$ has been incorporated in the definition of the input state ρ of the m uses of the channel. In particular, for $m=1$ and $z=k$ integer, Eqs. (50) and (11) give the k norm for the single channel use of $\mathcal{G}$, i.e.,

$$\nu_k(\mathcal{G}) = \left[\frac{(2\sqrt{u^2-|v|^2})^k}{(1+2\sqrt{u^2-|u|^2})^k-1}\right]^{1/k}. \tag{51}$$

According to the decomposition rule of Eq. (46), such a maximum is achieved for the antisqueezed coherent states

$$|\alpha;-\xi\rangle \equiv \Sigma^\dagger(\xi)|\alpha\rangle. \tag{52}$$

In fact, feeding the channel $\mathcal{G}$ with this input is equivalent (apart from an irrelevant unitary transformation) to feeding $\mathcal{N}_n$ with the coherent state $|\alpha\rangle$. Moreover, for generic m Eq. (50) gives

$$\nu_k(\mathcal{G}^{\otimes m}) = \left[\frac{(2\sqrt{u^2-|v|^2})^k}{(1+2\sqrt{u^2-|u|^2})^k-1}\right]^{m/k}, \tag{53}$$

which proves the Amosov-Holevo-Werner conjecture for the channel $\mathcal{G}$, at least for integer $z=k$. As in the case of Eq. (52), the input states that achieve the maximum (53) can be obtained by antisqueezing the states which achieve the maximal output z norm for the channel $\mathcal{N}_n$, i.e., $|\alpha_1;-\xi\rangle_1 \otimes \cdots \otimes |\alpha_m;-\xi\rangle_m$.

B. Linear-coupling channels

The linear-coupling channel model represents a communication line where the input photons (described by the annihilation operator a) interact with an external environment (with annihilation operator b) through the beam splitter unitary operator,

$$U = \exp\left[(a^\dagger b - ab^\dagger)\arctan\sqrt{\frac{1-\eta}{\eta}}\right], \tag{54}$$

which transforms the fields according to

$$\begin{aligned} a &\to U^\dagger a U = \sqrt{\eta}\,a + \sqrt{1-\eta}\,b, \\ b &\to U^\dagger b U = \sqrt{\eta}\,b - \sqrt{1-\eta}\,a, \end{aligned} \tag{55}$$

with $\eta \in [0,1]$ being the beam splitter transmissivity. For $\eta=1$, U is the identity and the input signal is decoupled from the environment; for $\eta=0$, instead, U is a swap operator which replaces the input signal with the environment input state. The *CP* map of the linear-coupling channel is obtained by coupling the input state of the signal ρ with the input state of the environment τ_b through U and then by tracing away the mode b. The resulting output state is then

$$\mathcal{L}(\rho) = \mathrm{Tr}_b[U\rho \otimes \rho_b U^\dagger]. \tag{56}$$

If ρ_b is a Gaussian state, the CP map $\mathcal{L}$ is Gaussian. In what follows we will assume ρ_b to be the squeezed thermal state,

$$\rho_b = \Sigma_b^\dagger(\xi)\tau_b(n)\Sigma_b(\xi), \tag{57}$$

where Σ_b and $\tau_b(n)$ are, respectively, the squeezing operator and the thermal state (57) of the b mode. For the channel (56) a decomposition rule analogous to Eq. (46) applies, namely (see Appendix B),

$$\mathcal{L}(\rho) = \Sigma^\dagger(\xi)\mathcal{E}_n(\Sigma(\xi)\rho\Sigma^\dagger(\xi))\Sigma(\xi), \tag{58}$$

with $\mathcal{E}_n(\rho)$ the *CP* map (56) where the environment is in the thermal state $\rho_b=\tau(n)$. The connection between $\mathcal{L}$ and $\mathcal{E}_n$ is thus analogous to the connection between $\mathcal{G}$ and $\mathcal{N}_n$. In particular, we can derive the following identity

$$\nu_z(\mathcal{L}^{\otimes m}) = \nu_z(\mathcal{E}_n^{\otimes m}), \tag{59}$$

which applies for all m integer and for all z. Proving the Amosov-Holevo-Werner conjecture for $\mathcal{E}_n$ is equivalent to proving it for $\mathcal{L}$; moreover, the input states which achieve the maximum output z norm for $\mathcal{L}$ are obtained by antisqueezing the input states which achieve the maximum for $\mathcal{E}_n$.

The channel $\mathcal{E}_n$ has been extensively studied in Ref. [10] where it was shown that it satisfies the relation

$$\mathcal{E}_n(\rho) = (\mathcal{N}_{(1-\eta)n} \circ \mathcal{E}_0)(\rho) \equiv \mathcal{N}_{(1-\eta)n}(\mathcal{E}_0(\rho)), \tag{60}$$

with $\mathcal{E}_0$ being the lossy map, where the input photons interact with the vacuum state of the environment. Equation (60) shows that the output of the channel $\mathcal{E}_n$ can be obtained first applying the lossy map to the input state ρ and then feeding it into the classical channel $\mathcal{N}_n$. This composition rule has two important consequences. On one hand, it implies

$$\nu_z(\mathcal{E}_n^{\otimes m}) = \nu_z((\mathcal{N}_{(1-\eta)n} \circ \mathcal{E}_0)^{\otimes m}) \leqslant \nu_z(\mathcal{N}_{(1-\eta)n}^{\otimes m}). \tag{61}$$

In fact, the maximization implicit in the second term is performed on a set of input states which form a proper subset of the input states which enter in the maximization of the third term. On the other hand, since the lossy channel maps coherent input states into coherent outputs according to the transformation [7],

$$\mathcal{E}_0(|\alpha\rangle\langle\alpha|) = |\sqrt{\eta}\alpha\rangle\langle\sqrt{\eta}\alpha|, \tag{62}$$

Eqs. (60) and (10) show that when $\mathcal{E}_n$ and $\mathcal{N}_{(1-\eta)n}$ act on coherent inputs they produce the same output z norm. This is sufficient to prove that, at least for $z=k$ integer, the inequality in Eq. (61) is replaced by an identity; we have already established in fact that the maximum k norm of the channel $\mathcal{N}_n$ is achieved for a coherent state. Hence we can establish the following identity:

$$\nu_k(\mathcal{E}_n^{\otimes m}) = \left\{ \frac{1}{[(1-\eta)n+1]^k - [(1-\eta)n]^k} \right\}^{m/k}, \tag{63}$$

which, analogously to Eq. (53), shows that the Amosov-Holevo-Werner conjecture applies for the channel $\mathcal{E}_n$ at least for all integer k. Moreover, we know that, as in the case of $\mathcal{N}_n$, tensor products of coherent states are sufficient to achieve the maximum of Eq. (63).

In this paper we have studied various models of Gaussian bosonic channel (i.e., the classical maps $\mathcal{G}$ of Sec. II A and the linear coupling maps $\mathcal{L}$ of Sec. II B) and we have shown that the Amosov-Holevo-Werner conjecture (2) applies to them at least in the case of $z=k$ integer. In particular we have proven that tensor products of squeezed coherent states are the inputs that achieve the maximum output k norm for the m successive uses of these channels. In the case of the circularly symmetric channels $\mathcal{N}_n$ and $\mathcal{E}_n$ the optimal state are just tensor product of coherent states. These properties imply that, for all integer order greater than 2, the Rényi entropies at the output of the channels $\mathcal{G}$ and $\mathcal{L}$ are additive, and suggest that the same behavior should apply also to all the other orders (see Sec. I C). In particular, it seems reasonable to believe that these channel posses an additive Holevo information [15,20].

APPENDIX A: PROPERTIES OF THE OPERATOR Θ

In this appendix we prove that the operator Θ of Eq. (22) has the tensor product structure of Eq. (23) and we derive the identity (33).

1. Derivation of Eq. (23)

By using the property

$$D_s^\dagger(\vec{\mu})D_s(\vec{\nu}) = D_s(\vec{\nu}-\vec{\mu})\exp[(\vec{\nu}\cdot\vec{\mu}^\dagger - \vec{\mu}\cdot\vec{\nu}^\dagger)/2] \tag{A1}$$

of the multimode displacement operator defined in Eq. (18), the expression (22) of Θ yields

$$\Theta \equiv \int \frac{d^2\overleftrightarrow{\mu}}{(\pi n)^{mk}}\, e^{-\overleftrightarrow{\mu}\cdot\mathbb{C}\cdot\overleftrightarrow{\mu}^\dagger + \overleftrightarrow{\mu}\cdot\mathbb{G}^\dagger\cdot\overleftrightarrow{a}^\dagger - \overleftrightarrow{a}\cdot\mathbb{G}\cdot\overleftrightarrow{\mu}^\dagger}, \tag{A2}$$

where we have introduced the complex linear vector

$$\begin{aligned}\overleftrightarrow{\mu} &\equiv (\vec{\mu}_1;\vec{\mu}_2;\ldots;\vec{\mu}_k)\\ &= (\mu_{11},\ldots,\mu_{1m};\mu_{21},\ldots,\mu_{2m};\mu_{k1},\ldots,\mu_{km}),\end{aligned} \tag{A3}$$

which has km elements, and

$$\overleftrightarrow{a} \equiv (\vec{a}_1;\vec{a}_2;\ldots;\vec{a}_k) = (a_{11},\ldots,a_{1m};a_{21},\ldots,a_{2m};a_{k1},\ldots,a_{km}), \tag{A4}$$

where a_{sr} is the annihilation operator associated with the sth copy of the rth use of the channel. In Eq. (A2), $\mathbb{G}$ and

$$\mathbb{C} \equiv \frac{\mathbb{1}}{n} + \frac{\mathbb{A}}{2} \tag{A5}$$

are now $mk\times mk$ real matrices ($\mathbb{1}$ is the $mk\times mk$ identity), which are obtained, respectively, by tensoring to the mth power the matrices G and C of Eqs. (27) and (26). In particular, for $k\geqslant 3$, $\mathbb{G}$ and $\mathbb{A}$ have the block form

$$\mathbb{G} \equiv G^{\otimes m} = \begin{bmatrix} -\mathbb{1} & \mathbb{1} & 0 & \cdots & 0 & 0 \\ 0 & -\mathbb{1} & \mathbb{1} & \cdots & 0 & 0 \\ 0 & 0 & -\mathbb{1} & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \\ 0 & 0 & 0 & \cdots & -\mathbb{1} & \mathbb{1} \\ \mathbb{1} & 0 & 0 & \cdots & 0 & -\mathbb{1} \end{bmatrix}, \tag{A6}$$

$$\mathbb{A} \equiv A^{\otimes m} = \begin{bmatrix} 0 & -\mathbb{1} & 0 & \cdots & 0 & \mathbb{1} \\ \mathbb{1} & 0 & -\mathbb{1} & \cdots & 0 & 0 \\ 0 & \mathbb{1} & 0 & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \\ 0 & 0 & 0 & \cdots & 0 & -\mathbb{1} \\ -\mathbb{1} & 0 & 0 & \cdots & \mathbb{1} & 0 \end{bmatrix}, \tag{A7}$$

where now $\mathbb{1}$ and 0 are the $m\times m$ identity and null matrix, respectively. On one hand, these equations show that the Gaussian in the integral (A2) couples together all the annihilation operators a_{sr} which have the same index r [i.e., the operators $a_{1r},a_{2r},\ldots$ and $a_{k,r}$ which enter in the definition of the vector $\tilde{a}_r$ of Eq. (24)]. On the other hand, Eqs. (A6) and (A7) show that any two annihilation operators a_{sr} and $a_{s'r'}$ with $r\neq r'$ are not coupled by the integral (A2). We can hence write such an expression as a (tensor) product of m independent Gaussian integrals where only the modes associated with $\tilde{a}_r$ enters; by doing this and using the cyclic symmetry of the matrices $\mathbb{G}$ and $\mathbb{A}$ we finally obtain Eq. (23).

2. Derivation of Eq. (33)

The identity (33) has been derived in Ref. [11] by showing that the operator in the left-hand side of this expression has the same symmetric characteristic function of the operator Θ_{jr} of Eq. (32). Here, instead, we show that these operator coincide by calculating their matrix elements in the Fock basis of the annihilation operator b_{jr}. For the sake of simplicity in the following we will omit the indices j and r.

Given $|p\rangle$ and $|q\rangle$ Fock states of b with $p\geqslant q$, consider the quantity

$$\langle p|\Theta|q\rangle = \int d^2\nu \, \frac{e^{-d|\nu|^2/|e|^2}}{\pi n|e|^2}\langle p|D(-\nu)|q\rangle. \tag{A8}$$

Following the derivation given in Ref. [17] the matrix element in the integral can be expressed in terms of the Laguerre polynomials as

$$\langle p|D(-\nu)|q\rangle = \left(\frac{q!}{p!}\right)^{1/2} e^{-|\lambda|^2/2}\nu^{\,p-q}L_q^{(p-q)}(|\nu|^2). \tag{A9}$$

Replacing this expression in Eq. (A8) and using the identities [21]

$$\int_0^\infty dx\, e^{-\gamma x}L_q^{(0)}(x) = \frac{(\gamma-1)^q}{\gamma^{\,q+1}}, \quad \text{Re } \gamma > 0 \tag{A10}$$

and

$$\int_0^{2\pi} d\varphi \, e^{i\varphi(p-q)} = 2\pi\delta_{pq}, \tag{A11}$$

where δ_{pq} is the Kronecker delta, we finally obtain

$$\langle p|\Theta|q\rangle = \frac{2/n}{2d+|e|^2}\left(\frac{2d-|e|^2}{2d+|e|^2}\right)^p \delta_{pq}, \tag{A12}$$

which proves the thesis.

APPENDIX B: DECOMPOSION OF THE MAPS $\mathcal{G}$ AND $\mathcal{L}$

In this section we derive the decomposition rule of Eqs. (46) and (58) which allows to express the map $\mathcal{G}$ of Eq. (44) in terms of $\mathcal{N}_n$ and the map $\mathcal{L}$ of Eq. (56) in terms of $\mathcal{E}_n$, respectively.

1. Derivation of Eq. (46)

Consider the Hermitian matrix

$$B \equiv \begin{bmatrix} \alpha & \beta^* \\ \beta & \alpha \end{bmatrix}, \tag{B1}$$

with

$$\alpha = \left(\frac{u+\sqrt{u^2-|v|^2}}{2\sqrt{u^2-|v|^2}}\right)^{1/2},$$

$$\beta = \frac{v}{|v|}\left(\frac{u-\sqrt{u^2-|v|^2}}{2\sqrt{u^2-|v|^2}}\right)^{1/2}, \tag{B2}$$

where u and v are the elements of Γ defined in Eq. (7). The matrix B has determinant equal to 1 and inverse

$$B^{-1} \equiv \begin{bmatrix} \alpha & -\beta^* \\ -\beta & \alpha \end{bmatrix}, \tag{B3}$$

which diagonalizes Γ through the relation

$$B^{-1}\Gamma B^{-1} = \begin{bmatrix} \sqrt{u^2-|v|^2} & 0 \\ 0 & \sqrt{u^2-|v|^2} \end{bmatrix}. \tag{B4}$$

Moreover, when applied to $(a,a^\dagger)$ this matrix produces the Bogoliubov transformation

$$(c,c^\dagger) \equiv (a,a^\dagger)B^{-1} = \Sigma^\dagger(\xi)(a,a^\dagger)\Sigma(\xi), \tag{B5}$$

where $\Sigma(\xi)$ is the squeezing operator defined in Eq. (49). Using these properties we can obtain Eq. (46) from Eq. (44) by performing a change of integration variables. In fact, for $\zeta \to \zeta B$ we have

$$\begin{aligned}\mathcal{G}(\rho) &= \int d^2\zeta \, \frac{\exp[-\zeta(B^{-1}\Gamma B^{-1})\zeta^\dagger]}{\pi/(2\sqrt{\det[\Gamma]})}\exp[(c,c^\dagger)\zeta^\dagger]\rho \\ &\quad \times \exp[-(c,c^\dagger)\zeta^\dagger] \\ &= \int d^2\mu \frac{\exp[-2\sqrt{u^2-|v|^2}|\mu|^2]}{\pi/(2\sqrt{u^2-|v|^2})} \\ &\quad \times \Sigma^\dagger(\xi)D(\mu)\Sigma(\xi)\rho\Sigma^\dagger(\xi)D^\dagger(\mu)\Sigma(\xi),\end{aligned} \tag{B6}$$

which, according to Eqs. (7) and (47) coincide with the left-hand side of Eq. (44).

2. Derivation of Eq. (58)

For the sake of clarity, in what follows the operators which acts only on the environment will have the subscript b while the operators which act only on the input state will have the subscript a. Using the relations (55) it is easy to show that the coupling operator U transforms a^2+b^2 into itself, i.e., it commutes with the operator $\Sigma_a(\xi)\Sigma_b(\xi)$ which squeezes both the signal mode a and the environment mode b by the same quantity ξ. Inserting the identity decomposition $\Sigma_a^\dagger(\xi)\Sigma_a(\xi)=\mathbb{1}$ in Eq. (56) and using the invariance of the trace under cyclic permutation, the above property allows us to write Eq. (56) as

$$\begin{aligned}\mathcal{L}(\rho) &= \Sigma_a^\dagger(\xi)\text{Tr}_b\{U[\Sigma_a(\xi)\rho\Sigma_a^\dagger(\xi)\otimes \tau_b(n)]U^\dagger\}\Sigma_a(\xi) \\ &= \Sigma_a^\dagger(\xi)\mathcal{E}_n(\Sigma_a(\xi)\rho\Sigma_a^\dagger(\xi))\Sigma_a(\xi),\end{aligned} \tag{B7}$$

which proves the thesis (58).

[1] P. W. Shor, e-print quant-ph/0305035; A. S. Holevo, e-print quant-ph/0306196.

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

[3] C. H. Bennet and P. W. Shor, IEEE Trans. Inf. Theory **44**, 2724 (1998).

[4] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).

[5] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998); P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and

W. K. Wootters, Phys. Rev. A **54**, 1869 (1996); B. Schumacher and M. D. Westmoreland, *ibid.* **56**, 131 (1989).

[6] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, Phys. Rev. Lett. **78**, 3217 (1997).

[7] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, Phys. Rev. Lett. **92**, 027902 (2004).

[8] C. King, IEEE Trans. Inf. Theory **49**, 221 (2003).

[9] C. King and M. B. Ruskai, IEEE Trans. Inf. Theory **47**, 192 (2001).

[10] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, and J. H. Shapiro, e-print quant-ph/0404005.

[11] V. Giovannetti, S. Lloyd, L. Maccone, J. H. Shapiro, and B. J. Yen, e-print quant-ph/0404037.

[12] G. G. Amosov, A. S. Holevo, and R. F. Werner, Probl. Inf. Transm. **36**, 305 (2000); e-print math-ph/0003002.

[13] K. Życzkowski, Open Syst. Inf. Dyn. **10**, 297 (2003); C. Beck and F. Schlögl, *Thermodynamics of Chaotic Systems* (Cambridge University Press, Cambridge, 1993).

[14] G. G. Amosov and A. S. Holevo, Theor. Probab. Appl. **47**, 123 (2001).

[15] A. S. Holevo, M. Sohma, and O. Hirota, Phys. Rev. A **59**, 1820 (1999); M. Sohma and O. Hirota, Recent Res. Dev. Opt. **1**, 146 (2000); A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001); M. Sohma and O. Hirota, *ibid.* **65**, 022319 (2002).

[16] U. Grenander and G. Szegö, *Toeplitz Forms and Their Applications* (University of California Press, Berkley, 1958).

[17] C. Caves, http://info.phys.unm.edu/caves/reports/cvteleportation.pdF

[18] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer-Verlag, Berlin, 1994).

[19] In Eq. (46) the differential form $d^2\zeta$ stands for $d^2\mu \equiv d\mathrm{Re}(\mu)d\mathrm{Im}(\mu)$.

[20] V. Giovannetti, S. Lloyd, L. Maccone, and J. H. Shapiro (unpublished).

[21] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products* (Academic Press, San Diego, 2000), Chap. 7 , p. 416.