Supplementary Information: Majorization theory approach to the Gaussian channel minimum entropy conjecture

Raúl García-Patrón,[1,2] Carlos Navarrete-Benlloch,[1,3] Seth Lloyd,[1] Jeffrey H. Shapiro,[1] and Nicolas J. Cerf[1,4]

[1]*Research Laboratory of Electronics, MIT, Cambridge, MA 02139*
[2]*Max-Planck Institut für Quantenoptik, Hans-Kopfermann-Str. 1, D-85748 Garching, Germany*
[3]*Departament d'Òptica, Universitat de València, Dr. Moliner 50, 46100 Burjassot, Spain*
[4]*Quantum Information and Communication, Ecole Polytechnique de Bruxelles, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium*

In what follows, we give a more complete overview of the calculations leading to the main results of this Letter. First, we derive the lower bound used to reduce conjecture **C1** to **C2**. Second, we review the concept of majorization in probability theory, and describe its use in the context of quantum entanglement. Then, we detail the calculation of the output state of a two-mode squeezer for an arbitrary input state expressed as a superposition of Fock states. Finally, we provide a detailed derivation of the chain of majorization relations that are obeyed by a two-mode squeezer with number-state inputs in one port, and present their associated local operation and classical communication (LOCC) protocols.

REDUCTION OF THE MINIMUM ENTROPY CONJECTURE

In what follows we exploit the decomposition $\mathcal{M} = \mathcal{A} \circ \mathcal{L}$ and the concavity of the von Neumann entropy to prove that the minimum output entropy of channel $\mathcal{M}$ is lower-bounded by that of channel $\mathcal{A}$, i.e., $\min_\phi S(\mathcal{M}(\phi)) \geq \min_\psi S(\mathcal{A}(\psi))$.

Let $|\phi\rangle$ be an input pure state of channel $\mathcal{M}$. After passage through the pure-loss channel $\mathcal{L}$, the intermidiate state (between $\mathcal{L}$ and $\mathcal{A}$) is $\tilde{\sigma} = \mathcal{L}(|\phi\rangle\langle\phi|)$. For any decomposition $\{p_i, \psi_i\}$ of $\tilde{\sigma}$ satisfying $\tilde{\sigma} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, we have the following chain of inequalities

$$\begin{aligned} S\left(\mathcal{M}(|\phi\rangle\langle\phi|)\right) &\overset{(1)}{=} S\left(\mathcal{A}(\tilde{\sigma})\right) \overset{(2)}{=} S\left(\sum_i p_i \mathcal{A}(|\psi_i\rangle\langle\psi_i|)\right) \\ &\overset{(3)}{\geq} \sum_i p_i S\left(\mathcal{A}(|\psi_i\rangle\langle\psi_i|)\right) \\ &\overset{(4)}{\geq} \min{}_\psi S(\mathcal{A}(\psi)), \end{aligned} \quad (1)$$

where we have used: the channel decomposition $\mathcal{M} = \mathcal{A} \circ \mathcal{L}$ in (1); the linearity of quantum operations in (2), the sub-additivity of von Neumann entropy in (3); and, finally, the definition of the minimum output entropy of channel $\mathcal{A}$ in (4). The proof concludes by noticing that Eq. (1) holds for every input state of channel $\mathcal{M}$, including the one minimizing the output entropy of $\mathcal{M}$.

MAJORIZATION AND ENTANGLEMENT

Majorization appeared as a way to order probability distributions in terms of their disorder, in an effort to understand when one distribution can be built from another by randomizing the later [1]. Take two probability vectors $\mathbf{p} = (p_1, p_2, ..., p_d)^T$ and $\mathbf{q} = (q_1, q_2, ..., q_d)^T$ of dimension d (which can be infinite as in our case), properly normalized, that is, $\sum_{n=1}^d p_n = \sum_{n=1}^d q_n = 1$. We say that $\mathbf{p}$ majorizes $\mathbf{q}$, and denote it by $\mathbf{p} \succ \mathbf{q}$, if and only if

$$\sum_{n=1}^{m} p_n^\downarrow \geq \sum_{n=1}^{m} q_n^\downarrow \;\; \forall m \leq d, \quad (2)$$

where $\mathbf{p}^\downarrow$ and $\mathbf{q}^\downarrow$ are the original vectors with their components rearranged in decreasing order. This definition is useful from a practical point of view, since it is easy to check numerically if two vectors satisfy these relations. Nevertheless, it can be proven that $\mathbf{p} \succ \mathbf{q}$ is strictly equivalent to two other operational relations:

M1. For every concave function $h(x)$, we have $\sum_{n=1}^d h(p_n) \leq \sum_{n=1}^d h(q_n)$.

M2. $\mathbf{q}$ can be obtained from $\mathbf{p}$ via $\mathbf{q} = D\mathbf{p}$, where D is a column-stochastic matrix.

A square matrix D is column-stochastic if its elements are real and positive, its columns sum to one, and its rows sum to less than one. Most of the literature on the connection between majorization and quantum information studies finite-dimensional systems, in which case it can be shown that column-stochastic matrices are also doubly-stochastic (columns and rows both sum to one). In this work we need the slightly more general definition of column-stochastic to cope with infinite dimensional spaces [3]. Physically, stochastic matrices are equivalent to convex mixtures of permutations of the vector components, and hence, property **M2** shows that $\mathbf{q}$ is more disordered than $\mathbf{p}$.

Interestingly, majorization theory can also be used to answer the question of whether Alice an Bob can transform a shared bipartite pure state $|\psi\rangle_{AB}$ into $|\varphi\rangle_{AB}$ by using a deterministic protocol involving only local operations and classical communication (LOCC) [2, 4]. Given the probability vectors $\mathbf{p}_\psi$ and $\mathbf{p}_\varphi$ generated with the Schmidt coefficients of these states (the eigenvalues of the reduced density operators), it is possible to prove that the transformation $|\psi\rangle_{AB} \to |\varphi\rangle_{AB}$ is possible if and only if $\mathbf{p}_\varphi \succ \mathbf{p}_\psi$, that is, if the Schmidt coefficients of $|\varphi\rangle_{AB}$ majorize those of $|\psi\rangle_{AB}$, in which case we use the symbolic notation $|\varphi\rangle_{AB} \succ |\psi\rangle_{AB}$. The entanglement of a pure bipartite state $|\psi\rangle_{AB}$ being measured by the von Neumann entropy of the reduced density operator $\rho_A = \mathrm{Tr}_B[|\psi\rangle_{AB}]$, and the von Neumann entropy being a concave function, one gets as an intuitive corollary that $|\psi\rangle_{AB}$ can only be transformed deterministically by an LOCC protocol into states of lower entanglement, i.e.,

$$E[|\psi\rangle_{AB}] \geq E[|\varphi\rangle_{AB}], \tag{3}$$

as follows from property **M1**.

Note that while $|\varphi\rangle_{AB} \succ |\psi\rangle_{AB}$ implies that $\mathbf{p}_\varphi$ can be transformed into $\mathbf{p}_\psi$ by application of a column-stochastic matrix, the transformation goes in the opposite direction for the corresponding states, that is, it is $|\psi\rangle_{AB}$ the state which can be transformed into $|\varphi\rangle_{AB}$ by a deterministic LOCC protocol. In other words, at the level of probability distributions the transformation induces disorder (increases the entropy), while at the level of states the transformation decreases the entanglement, as corresponds to physical deterministic LOCC protocols.

OUTPUT STATES OF A TWO-MODE SQUEEZER

If we inject the vacuum state at the input of a two-mode squeezer $U(r)$, we obtain the two-mode squeezed vacuum state

$$|\Psi^{(0)}\rangle = U(r)|0,0\rangle = \frac{1}{\cosh r}\sum_{n=0}^{\infty} \tanh^n r\, |n,n\rangle, \tag{4}$$

where $|n\rangle$ is a number state, and we use the compact notation $|m\rangle_A \otimes |n\rangle_B = |m,n\rangle$.

Consider now the more general input state

$$|\phi\rangle = |\varphi\rangle \otimes |0\rangle = \sum_{n=0}^{\infty} c_n |n,0\rangle, \tag{5}$$

written in the number state basis, which becomes the state

$$|\phi_{out}\rangle = U(r)|\phi\rangle = \sum_{n=0}^{\infty} c_n |\Psi^{(n)}\rangle, \tag{6}$$

with

$$|\Psi^{(k)}\rangle = U(r)|k,0\rangle, \tag{7}$$

after passing through the two-mode squeezer.

In the reminder of this section, we focus on finding a manageable expression for the states $|\Psi^{(k)}\rangle$, that is, for the output state of the two-mode squeezer when a number state $|k\rangle$ is fed through one of its input ports. We start by noting that $|\Psi^{(k)}\rangle$ can be written in terms of the two-mode squeezed vacuum state $|\Psi^{(0)}\rangle$ as follows

$$|\Psi^{(k)}\rangle = \frac{1}{\sqrt{k!}} U(r) a_A^{\dagger k} |0,0\rangle = \frac{1}{\sqrt{k!}} [U(r) a_A^\dagger U(r)^\dagger]^k |\Psi^{(0)}\rangle, \tag{8}$$

which, using the relation

$$U(r) a_A^\dagger U(r)^\dagger = \cosh r\, a_A^\dagger - \sinh r\, a_B, \tag{9}$$

can be rewritten as

$$|\Psi^{(k)}\rangle = \sum_{j=0}^{k} \frac{(-1)^{k-j}}{\sqrt{k!}} \binom{k}{j} \cosh^j r \sinh^{k-j} r\, a_A^{\dagger j} a_B^{k-j} |\Psi^{(0)}\rangle. \tag{10}$$

Now, an easy calculation shows that

$$\begin{aligned} a_B|\Psi^{(0)}\rangle &= \frac{1}{\cosh r}\sum_{n=1}^{\infty} \sqrt{n} \tanh^n r\, |n, n-1\rangle \qquad (11) \\ &\underset{n\to m+1}{=} \frac{1}{\cosh r}\sum_{m=0}^{\infty} \sqrt{m+1} \tanh^{m+1} r\, |m+1, m\rangle, \end{aligned}$$

leading to the following identity

$$a_B|\Psi^{(0)}\rangle = \tanh r\, a_A^\dagger |\Psi^{(0)}\rangle, \tag{12}$$

which allows us to rewrite (10) as

$$|\Psi^{(k)}\rangle = \frac{\cosh^k r}{\sqrt{k!}} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} \tanh^{2(k-j)} r\, a_A^{\dagger k} |\Psi^{(0)}\rangle. \tag{13}$$

Finally, using the relations

$$\begin{aligned} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} x^{k-j} &= (1-x)^k, \qquad (14a) \\ 1 - \tanh^2 r &= \cosh^{-2} r, \qquad (14b) \end{aligned}$$

we can write the previous expression as

$$\begin{aligned} |\Psi^{(k)}\rangle &= \frac{1}{\sqrt{k!}\cosh^k r} a_A^{\dagger k} |\Psi^{(0)}\rangle \qquad (15) \\ &= \frac{1}{\cosh^{k+1} r} \sum_{n=0}^{\infty} \sqrt{\binom{n+k}{k}} \tanh^n r\, |n+k, n\rangle. \end{aligned}$$

Let us define $\lambda = \tanh r$; from now on we will use the notation

$$|\Psi_\lambda^{(k)}\rangle = \sum_{n=0}^{\infty} \sqrt{p_n^{(k)}(\lambda)} |n+k, n\rangle, \tag{16}$$

with

$$p_n^{(k)}(\lambda) = (1-\lambda^2)^{k+1} \lambda^{2n} \binom{n+k}{n}, \tag{17}$$

to stress the dependence of the state on the squeezing parameter. Note that the states (16) are already written in Schmidt form, and in the following we will use

$$\mathbf{p}^{(k)} = (p_0^{(k)}, p_1^{(k)}, ...)^T, \tag{18}$$

to denote the corresponding probability vectors.

PROOF OF THE MAJORIZATION RELATIONS FOR FOCK STATE INPUTS

In this section we will explain how to derive the column-stochastic matrices needed to prove the majorization relations employed in the Letter.

Proof of $|\Psi_\lambda^{(k)}\rangle \succ |\Psi_\lambda^{(k+1)}\rangle$

Because the states $|\Psi_\lambda^{(k)}\rangle$ are already in Schmidt form as commented previously, we need to prove that there exists a column-stochastic matrix D such that

$$\mathbf{p}^{(k+1)} = D\mathbf{p}^{(k)}. \tag{19}$$

This is actually quite simple if one notices that the Pascal identity

$$\binom{n+k+1}{k+1} = \binom{n+k}{k} + \binom{n+k}{k+1}, \tag{20}$$

implies the following relation (with the convention $p_n^{(k)} = 0$ for $n < 0$):

$$p_n^{(k+1)} = (1-\lambda^2)p_n^{(k)} + \lambda^2 p_{n-1}^{(k+1)}. \tag{21}$$

This recurrence allows us to connect $\mathbf{p}^{(k+1)}$ with $\mathbf{p}^{(k)}$ by means of a lower-triangular matrix

$$\begin{pmatrix} p_0^{(k+1)} \\ p_1^{(k+1)} \\ p_2^{(k+1)} \\ \vdots \end{pmatrix} = (1-\lambda^2)\begin{pmatrix} 1 & 0 & 0 & \dots \\ \lambda^2 & 1 & 0 & \dots \\ \lambda^4 & \lambda^2 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}\begin{pmatrix} p_0^{(k)} \\ p_1^{(k)} \\ p_2^{(k)} \\ \vdots \end{pmatrix}, \tag{22}$$

or in a more compact notation

$$p_n^{(k+1)} = \sum_{m=0}^{n}(1-\lambda^2)\lambda^{2m}p_{n-m}^{(k)}. \tag{23}$$

It is fairly easy to show that the triangular matrix shown above, whose elements are explicitly given by

$$D_{nm} = (1-\lambda^2)\lambda^{2(n-m)}H(n-m), \tag{24}$$

with $H(x)$ being the Heaviside step function defined as $H(x) = 1$ for $x \geq 0$ and $H(x) = 0$ for $x < 0$, is column-stochastic. Hence we conclude that $|\Psi_\lambda^{(k)}\rangle \succ |\Psi_\lambda^{(k+1)}\rangle$ as commented in the Letter.

Proof of $|\Psi_\lambda^{(k)}\rangle \succ |\Psi_\lambda^{(k+\Delta k)}\rangle$ for $\Delta k > 0$

It is clear that $|\Psi_\lambda^{(k)}\rangle \succ |\Psi_\lambda^{(k+1)}\rangle$ implies $|\Psi_\lambda^{(k)}\rangle \succ |\Psi_\lambda^{(k+\Delta k)}\rangle$ for all $\Delta k > 0$ (note that Δk is a positive integer by definition), as majorization is clearly a transitive relation. This shows that when restricted to Fock-state inputs, the output entanglement of a two-mode squeezer increases monotonically with the number of input photons.

In order to find the explicit column-stochastic matrix $D^{(\Delta k)}$ satisfying $\mathbf{p}^{(k+\Delta k)} = D^{(\Delta k)}\mathbf{p}^{(k)}$, we use the independence on k of the matrix D which allows us write

$$D^{(\Delta k)} = \underbrace{D \times D \times ... \times D}_{\Delta k \text{ times}}. \tag{25}$$

An explicit form of the elements of this matrix can be inferred for any Δk by evaluating the first matrices:

$$D^{(2)} = (1-\lambda^2)^2\begin{pmatrix} 1 & 0 & 0 & 0 & \dots \\ 2\lambda^2 & 1 & 0 & 0 & \dots \\ 3\lambda^4 & 2\lambda^2 & 1 & 0 & \dots \\ 4\lambda^6 & 3\lambda^2 & 2\lambda^2 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \tag{26a}$$

$$D^{(3)} = (1-\lambda^2)^3\begin{pmatrix} 1 & 0 & 0 & 0 & \dots \\ 3\lambda^2 & 1 & 0 & 0 & \dots \\ 6\lambda^4 & 3\lambda^2 & 1 & 0 & \dots \\ 10\lambda^6 & 6\lambda^2 & 3\lambda^2 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \tag{26b}$$

$$D^{(4)} = (1-\lambda^2)^4\begin{pmatrix} 1 & 0 & 0 & 0 & \dots \\ 4\lambda^2 & 1 & 0 & 0 & \dots \\ 10\lambda^4 & 4\lambda^2 & 1 & 0 & \dots \\ 20\lambda^6 & 10\lambda^2 & 4\lambda^2 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}. \tag{26c}$$

Hence, all $D^{(\Delta k)}$ matrices have a similar structure, except for the $(1-\lambda^2)^{\Delta k}$ prefactor, and the numbers accompanying the powers of λ^2 in the columns, which are given by the Δkth diagonal of the Pascal triangle. It is then fairly simple to prove by induction that the elements of $D^{(\Delta k)}$ are given by

$$D_{nm}^{(\Delta k)} = (1-\lambda^2)^{\Delta k}\binom{m+\Delta k-1}{\Delta k-1}\lambda^{2(n-m)}H(n-m). \tag{27}$$

Note that this general majorization relation implies in particular that $|\Psi_\lambda^{(0)}\rangle \succ |\Psi_\lambda^{(k)}\rangle\ \forall k$, and therefore, among all Fock state inputs, the vacuum state is the one which minimizes the output entanglement of a two-mode squeezer.

Proof of $|\Psi_{\lambda'}^{(0)}\rangle \succ |\Psi_\lambda^{(0)}\rangle$ for $\lambda' < \lambda$

It is well known that the entanglement of the two-mode squeezed vacuum state monotonically increases with the squeezing parameter λ. In what follows we prove a stronger result, that a given two-mode squeezed vacuum state majorizes all the two-mode squeezed vacuum states with stronger squeezing.

We seek for a column-stochastic matrix $R(\lambda,\lambda')$ satisfying

$$\mathbf{p}^{(0)}(\lambda) = R(\lambda,\lambda')\mathbf{p}^{(0)}(\lambda'). \tag{28}$$

Based on the matrices of the previous sections, we make an ansatz in which R is a lower-triangular matrix whose columns are all built from a vector $\mathbf{r}(\lambda,\lambda')$, that is,

$$R = \begin{pmatrix} r_0 & 0 & 0 & 0 & \dots \\ r_1 & r_0 & 0 & 0 & \dots \\ r_2 & r_1 & r_0 & 0 & \dots \\ r_3 & r_2 & r_1 & r_0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}. \tag{29}$$

Introducing this ansatz into equation (28), and recalling that $p_n^{(0)}(x) = (1-x^2)x^{2n}$, we get the following set of linear algebraic equations

$$\begin{aligned} (1-\lambda^2) &= (1-\lambda'^2)r_0, \\ (1-\lambda^2)\lambda^2 &= (1-\lambda'^2)\left(\lambda'^2 r_0 + r_1\right), \\ (1-\lambda^2)\lambda^4 &= (1-\lambda'^2)\left(\lambda'^4 r_0 + \lambda'^2 r_1 + r_2\right), \end{aligned} \tag{30}$$

which can be solved by recursion leading to the solution

$$r_n = \left(\frac{1-\lambda^2}{1-\lambda'^2}\right)\left[\lambda^2 - H(n-1)\lambda'^2\right]\lambda^{2(n-1)}, \tag{31}$$

which can checked, by induction, to be the solution for a general n. Note that $\sum_{n=0}^{\infty} r_n = 1$ as expected.

Proof of $|\Psi_{\lambda'}^{(k)}\rangle \succ |\Psi_{\lambda}^{(k)}\rangle$ for $\lambda' < \lambda$

The same kind of majorization relation can be proved for any $|\Psi_{\lambda}^{(k\neq 0)}\rangle$ state, although the proof is now a little more involved, as we need to find a matrix $R^{(k)}(\lambda,\lambda')$ satisfying

$$\mathbf{p}^{(k)}(\lambda) = R^{(k)}(\lambda,\lambda')\mathbf{p}^{(k)}(\lambda'), \tag{32}$$

which now depends on the value of k. As we now prove, the matrix $R^{(k)}(\lambda,\lambda')$ can still be chosen to be lower-triangular, but now every column is defined by its own vector $\mathbf{r}^{(k,j)}$, that is

$$R^{(k)} = \begin{pmatrix} r_0^{(k,0)} & 0 & 0 & 0 & \dots \\ r_1^{(k,0)} & r_0^{(k,1)} & 0 & 0 & \dots \\ r_2^{(k,0)} & r_1^{(k,1)} & r_0^{(k,2)} & 0 & \dots \\ r_3^{(k,0)} & r_2^{(k,1)} & r_1^{(k,2)} & r_0^{(k,3)} & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}. \tag{33}$$

Because we have to recover the case $k=0$ (31), we make the following ansatz

$$\begin{aligned} r_m^{(k,n)} &= \lambda^{2(m-1)}\left(\frac{1-\lambda^2}{1-\lambda'^2}\right)^{k+1} \\ &\quad\times\left[B_m^{(k,n)}\lambda^2 - C_m^{(k,n)}H(m-1)\lambda'^2\right], \end{aligned} \tag{34}$$

with $B_m^{(0,n)} = C_m^{(0,n)} = 1$, and where the coefficients $B_m^{(k\neq 0,n)}$ and $C_m^{(k\neq 0,n)}$ may depend on λ and λ'.

Similarly to the previous section, we can find the coefficients $B_m^{(k,n)}$ and $C_m^{(k,n)}$ by introducing this ansatz in (32), and using the explicit form of the probability vectors $p_n^{(k)}(x) = (1-x^2)^{k+1}x^{2n}\binom{n+k}{n}$. Let us show this process step by step.

The system (32) can be rewritten in a compact form as

$$p_n^{(k)}(\lambda) = \sum_{m=0}^{n} r_m^{(k,n-m)}(\lambda,\lambda')p_{n-m}^{(k)}(\lambda'). \tag{35}$$

For $n=0$, this sets

$$B_0^{(k,0)} = 1, \tag{36}$$

while for $n=1$ we get

$$\lambda^2\binom{k+1}{1} = B_0^{(k,1)}\lambda'^2\binom{k+1}{1} + B_1^{(k,0)}\lambda^2 - C_1^{(k,0)}\lambda'^2, \tag{37}$$

of which $B_1^{(k,0)} = \binom{k+1}{k}$ and $C_1^{(k,0)} = B_0^{(k,1)}\binom{k+1}{k}$ are valid solutions. Similarly, for $n=2$ (35) yields

$$\begin{aligned} \lambda^4\binom{k+2}{2} &= B_0^{(k,2)}\lambda'^4\binom{k+2}{2} + B_1^{(k,1)}\lambda^2\lambda'^2\binom{k+1}{1} \\ &-C_1^{(k,1)}\lambda'^4\binom{k+1}{1} + B_2^{(k,0)}\lambda^4 - C_2^{(k,0)}\lambda^2\lambda'^2, \end{aligned} \tag{38}$$

of which $B_2^{(k,2)} = \binom{k+2}{2}$, $C_2^{(k,0)} = B_1^{(k,1)}\binom{k+1}{k}$, and $C_1^{(k,1)} = B_0^{(k,2)}\binom{k+2}{2}/\binom{k+1}{1}$ are now valid solutions.

We observe the pattern of solutions

$$B_m^{(k,0)} = \binom{m+k}{k}, \tag{39a}$$

$$C_m^{(k,n)} = B_{m-1}^{(k,n+1)}\frac{\binom{n+k+1}{k}}{\binom{n+k}{k}}, \tag{39b}$$

so that the components of the vectors $\mathbf{r}^{(k,n)}$ can be rewritten as

$$\begin{aligned} r_m^{(k,n)} &= \binom{n+k}{n}^{-1}\left(\frac{1-\lambda^2}{1-\lambda'^2}\right) \\ &\quad\times\left[L_m^{(k,n)}\lambda^2 - L_{m-1}^{(k,n+1)}\lambda'^2\right]\lambda^{2(m-1)}, \end{aligned} \tag{40}$$

where we have defined the new parameters

$$L_m^{(k,n)} = \binom{n+k}{n}B_m^{(k,n)}, \tag{41}$$

which satisfy $L_m^{(k,0)} = \binom{m+k}{k}$ except for $m<0$, in which case $L_m^{(k,n)} = 0$.

In order to find the coefficients $L_m^{(k,n)}$ we use a further condition: as $R^{(k)}(\lambda,\lambda')$ must be column-stochastic, the vectors $\mathbf{r}^{(k,n)}$ must be normalized. Let us then define the series

$$S^{(k,n)} = \sum_{m=0}^{\infty} L_m^{(k,n)} \lambda'^{2m}, \tag{42}$$

in terms of which the normalization condition $\sum_{m=0}^{\infty} r_m^{(k,n)} = 1$ can be rewritten as

$$\lambda'^2 S^{(k,n+1)} = S^{(k,n)} - \binom{n+k}{k}\left(\frac{1-\lambda'^2}{1-\lambda^2}\right)^{k+1}. \tag{43}$$

Starting from

$$S^{(k,0)} = \sum_{m=0}^{\infty}\binom{m+k}{k}\lambda'^{2m} = (1-\lambda'^2)^{-(k+1)}, \tag{44}$$

these relations allow us to find the rest of $S^{(k,n)}$ recursively, obtaining

$$S^{(k,1)} = \lambda'^{-2}(1-\lambda^2)^{-(k+1)}[1-(1-\lambda'^2)^{k+1}], \tag{45a}$$
$$S^{(k,2)} = \lambda'^{-2}(1-\lambda^2)^{-(k+1)}\Big\{\lambda'^{-2} - \left[\lambda'^{-2} + \binom{k+1}{k}\right](1-\lambda'^2)^{k+1}\Big\}, \tag{45b}$$
$$S^{(k,3)} = \lambda'^{-2}(1-\lambda^2)^{-(k+1)}\Big\{\lambda'^{-4} - \left[\lambda'^{-4} + \lambda'^{-2}\binom{k+1}{k} + \binom{k+2}{k}\right](1-\lambda'^2)^{k+1}\Big\}, \tag{45c}$$
$$\vdots$$

from which one sees the general pattern

$$S^{(k,n)} = \lambda'^{-2n}(1-\lambda^2)^{-(k+1)} \times\left[1-(1-\lambda'^2)^{k+1}\sum_{l=0}^{n-1}\lambda'^{2l}\binom{l+k}{k}\right]. \tag{46}$$

The sum on the right-hand side term can be written in terms of the incomplete beta function

$$B(z;a,b) = \int_0^z dx x^{a-1}(1-x)^{b-1}, \tag{47}$$

as

$$\sum_{l=0}^{n-1}\binom{l+k}{k}\lambda'^{2l} = (1-\lambda'^2)^{-(k+1)} \times\left[1-n\binom{n+k}{k}B(\lambda'^2;n,k+1)\right]. \tag{48}$$

We can therefore rewrite the condition (46) as

$$\sum_{m=0}^{\infty} L_m^{(k,n+1)}\lambda^{2m} = \lambda'^{-2n}(1-\lambda^2)^{-(k+1)} n\binom{n+k}{k}B(\lambda'^2;n,k+1), \tag{49}$$

which, given the result (44), can be satisfied by choosing

$$L_m^{(k,n)} = n\binom{n+k}{k}\binom{m+k}{k}\lambda'^{-2n}B(\lambda'^2;n,k+1). \tag{50}$$

Note that this expression is valid even for $n=0$, as

$$\lim_{a\to 0} aB(x;a,b) = 1, \tag{51}$$

when b is a positive integer. Introducing this expression for the $L_m^{(k,n)}$ coefficients in $\mathbf{r}^{(k,n)}$ (40), and this into (33), we get the column-stochastic matrix $R(\lambda,\lambda')$ given in the Letter. Hence, we have been able to find a stochastic map connecting $\mathbf{p}^{(k)}(\lambda')$ to $\mathbf{p}^{(k)}(\lambda)$, which proves the majorization relation $|\Psi_{\lambda'}^{(k)}\rangle \succ |\Psi_{\lambda}^{(k)}\rangle$ if $\lambda' < \lambda$.

LOCC PROTOCOLS

For completeness, we now give the LOCC protocols corresponding to the previous majorization relations. We believe that these could offer an alternative (more physical) way of attacking the proof of the conjecture for a general input state like (5), and hence find it appropriate to explain how to build such protocols.

Transformation $|\Psi_\lambda^{(k+1)}\rangle \to |\Psi_\lambda^{(k)}\rangle$

Let us assume that Alice and Bob share the bipartite state $|\Psi_\lambda^{(k+1)}\rangle$, and want to convert it into $|\Psi_\lambda^{(k)}\rangle$. Inspired by the recurrence relation (23), we propose the following LOCC protocol. Bob starts by performing a POVM measurement [5] described by the measurement operators

$$B_m = \sum_{l=m}^{\infty}\sqrt{\frac{(1-\lambda^2)\lambda^{2m}p_{l-m}^{(k)}}{p_l^{(k+1)}}}|l-m\rangle\langle l|. \tag{52}$$

Using Eq. (23), it is easy to verify the condition $\sum_{m=0}^{\infty} B_m^\dagger B_m = I$. After Bob has completed his local measurement, depending on the outcome m of the measurement, the joint state "collapses" to

$$(I_A\otimes B_m)\ |\Psi_\lambda^{(k+1)}\rangle \propto \sum_{n=m}^{\infty}\sqrt{p_{n-m}^{(k)}}|n+k+1,n-m\rangle = \sum_{n=0}^{\infty}\sqrt{p_n^{(k)}}|n+k+m+1,n\rangle. \tag{53}$$

Then, after Bob has communicated the outcome m of his measurement to Alice, she performs the local shift operation

$$A_m = \sum_{l=0}^{\infty} |l\rangle\langle l+m+1|, \tag{54}$$

which then yields the desired state $|\Psi_\lambda^{(k)}\rangle$ regardless of m, that is, deterministically. Remark that the shift operator is trace preserving in the subspace spanned by $\{|j+m+1\rangle\}_{j=0,1,..}$, which is the support of $(I_A \otimes B_m)|\Psi_\lambda^{(k+1)}\rangle$ on Alice's side. Notice that one can easily build a shift operation that acts on Alice's full Hilbert space by appending ancillary qubits.

Transformation $|\Psi_\lambda^{(k+\Delta k)}\rangle \to |\Psi_\lambda^{(k)}\rangle$ for $\Delta k > 0$

Similarly as before but exploiting now (27), we engineer the following POVM on Bob's side

$$B_m = \sum_{l=m}^{\infty} \sqrt{\frac{(1-\lambda^2)^{\Delta k}\binom{m+\Delta k-1}{\Delta k-1}\lambda^{2m} p_{l-m}^{(k)}}{p_l^{(k+\Delta k)}}} |l-m\rangle\langle l|, \tag{55}$$

which, combined with the conditional shift in Alice's side

$$A_m = \sum_{l=0}^{\infty} |l\rangle\langle l+m+\Delta k|, \tag{56}$$

deterministically transforms the state $|\Psi_\lambda^{(k+\Delta k)}\rangle$ into $|\Psi_\lambda^{(k)}\rangle$. Whenever $k=0$, we obtain the two-mode vacuum squeezed state $|\Psi_\lambda^{(0)}\rangle$, which is thus at the end of the majorization chain, and its entanglement is minimum when compared to all other states $|\Psi_\lambda^{(k)}\rangle$.

Transformation $|\Psi_\lambda^{(0)}\rangle \to |\Psi_{\lambda'}^{(0)}\rangle$ for $\lambda' < \lambda$

Constructing an LOCC protocol from the stochastic matrix $R(\lambda,\lambda')$ (29) which connects $\mathbf{p}^{(0)}(\lambda')$ with $\mathbf{p}^{(0)}(\lambda)$ is not an easy task. Interestingly, we found a simpler deterministic protocol achieving the same result. Let us first give a probabilistic scheme performing the transformation, which we later make deterministic.

As shown in Figure 1, Bob mixes his mode B with an ancillary mode C on a beam-splitter of transmissivity T. The initial state is

$$|\psi\rangle_{ABC} = |\Psi_\lambda^{(0)}\rangle \otimes |0\rangle = \mathcal{N}(\lambda)\sum_{n=0}^{\infty}\lambda^n |n,n,0\rangle, \tag{57}$$

where $\mathcal{N}(\lambda) = (1-\lambda^2)^{1/2}$ a normalization factor. After passage through the beam-splitter, the joint state becomes

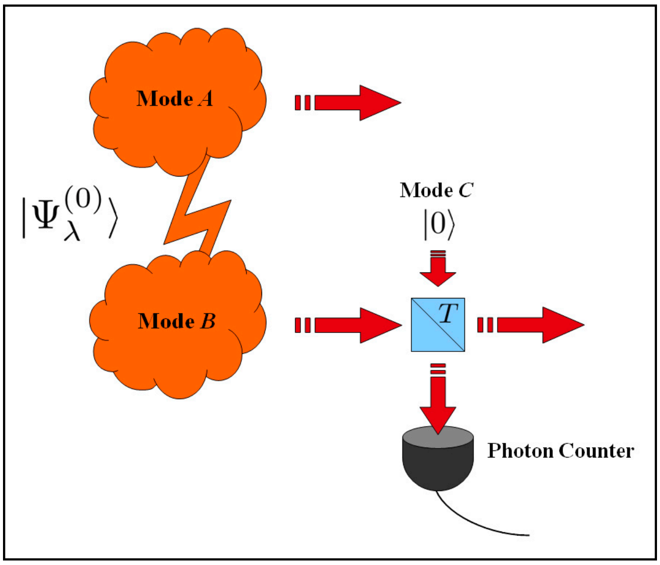

FIG. 1: Probabilistic LOCC protocol achieving the transformation $|\Psi_\lambda^{(0)}\rangle \to |\Psi_{\lambda'}^{(0)}\rangle$ for $\lambda' < \lambda$. Initially, Alice and Bob share the entangled state $|\Psi_\lambda^{(0)}\rangle_{AB}$. The first step of the protocol consists in Bob mixing his mode B with a vacuum ancillary mode C into a beam-splitter of transmissivity T, and measuring the number of photons at the output of mode C with a photon counter. Conditioned to the measurement of zero reflected photons, the desired transformation is achieved with $\lambda' = \sqrt{T}\lambda$.

$$|\psi'\rangle_{ABC} = \mathcal{N}(\lambda) \sum_{n,m=0}^{\infty} (T\lambda^2)^{n/2}\left(\frac{1-T}{T}\right)^{m/2} \times \binom{n}{m}^{1/2} |n, n-m, m\rangle. \tag{58}$$

Finally, Bob measures the number of photons reflected by the beam-splitter. The outcome of the measurement will be zero with probability $\mathcal{P} = \mathcal{N}^2(\sqrt{T}\lambda)/\mathcal{N}^2(\lambda)$, after which the state will collapse according to

$$\begin{aligned}\sqrt{\mathcal{P}}|\psi''\rangle_{AB} &= {}_C\langle 0|\psi'\rangle_{ABC} = \mathcal{N}(\lambda)\sum_{n=0}^{\infty} T^{n/2}\lambda^n |n,n\rangle \\ &= \sqrt{\mathcal{P}}|\Psi_{\sqrt{T}\lambda}^{(0)}\rangle_{AB}.\end{aligned} \tag{59}$$

Then, by choosing the transmissivity of the beam-splitter to satisfy $\lambda' = \sqrt{T}\lambda$ we obtain the target state. Note that there always exists a valid transmissivity T, as $\lambda' < \lambda$. The input state $|\Psi_\lambda^{(0)}\rangle_{AB} \otimes |0\rangle_C$ being a Gaussian state and the projection into vacuum being a Gaussian operation, there must exist a deterministic LOCC protocol generating the same outcome [6]. Such a protocol consists of replacing Bob's projection onto vacuum by heterodyne detection followed by local displacements on Alice and Bob sides that are proportional to the outcome of Bob's heterodyne measurement.

Transformation $|\Psi_\lambda^{(k)}\rangle \to |\Psi_{\lambda'}^{(k)}\rangle$ for $\lambda' < \lambda$

Similarly to the case $k=0$, constructing an LOCC protocol from the stochastic matrix $R^{(k)}(\lambda,\lambda')$ (33) which connects $\mathbf{p}^{(k)}(\lambda')$ with $\mathbf{p}^{(k)}(\lambda)$ is not an easy task. Instead, we give a simpler deterministic protocol achieving the same result.

Just as in the previous protocol, Bob starts by mixing mode B with an ancillary mode C on a beam-splitter of transmissivity T. The joint initial state is

$$\begin{aligned} |\psi\rangle_{ABC} &= |\Psi_\lambda^{(k)}\rangle \otimes |0\rangle \\ &= \mathcal{N}(k,\lambda)\sum_{n=0}^{\infty}\lambda^n \binom{n+k}{k}^{1/2} |n+k,n,0\rangle, \end{aligned} \tag{60}$$

with $\mathcal{N}(k,\lambda) = (1-\lambda^2)^{(k+1)/2}$, which becomes

$$\begin{aligned} |\psi'\rangle_{ABC} &= \mathcal{N}(k,\lambda)\sum_{n,m=0}^{\infty}(T\lambda^2)^{n/2}\left(\frac{1-T}{T}\right)^{m/2} \\ &\times \binom{n+k}{k}^{1/2}\binom{n}{m}^{1/2}|n+k,n-m,m\rangle, \end{aligned} \tag{61}$$

after passing through the beam-splitter.

Second, Bob measures the number of photons reflected by the beam-splitter. With probability

$$\mathcal{P}(l) = (1-T)^l\lambda^{2l}\binom{k+l}{l}\frac{\mathcal{N}^2(k,\lambda)}{\mathcal{N}^2(k+l,\sqrt{T}\lambda)}, \tag{62}$$

the outcome of the measurement will be l photons, and the state of modes A and B will collapse in that case to

$$\begin{aligned} \sqrt{\mathcal{P}(l)}\;|\psi''\rangle_{AB} &= {}_C\langle l|\psi'\rangle_{ABC} \\ &= \mathcal{N}(k,\lambda)\left(\frac{1-T}{T}\right)^{l/2} \\ \times\quad & \sum_{n=l}^{\infty}(T\lambda^2)^{n/2}\binom{n+k}{k}^{1/2}\binom{n}{l}^{1/2}|n+k,n-l\rangle. \end{aligned} \tag{63}$$

Now, making the variable change $n-l\to n$ in the sum, and using the relation

$$\binom{n+l+k}{k}\binom{n+l}{l} = \binom{n+k+l}{n}\binom{k+l}{l}, \tag{64}$$

this state can be rewritten as

$$\begin{aligned} \sqrt{\mathcal{P}(l)}|\psi''\rangle_{AB} &= \mathcal{N}(k,\lambda)(1-T)^{l/2}\lambda^l\binom{k+l}{l}^{1/2} \\ &\times \sum_{n=0}^{\infty}(T\lambda^2)^{n/2}\binom{n+k+l}{n}^{1/2}|n+k+l,n\rangle \\ &= \sqrt{\mathcal{P}(l)}|\Psi_{\sqrt{T}\lambda}^{(k+l)}\rangle. \end{aligned} \tag{65}$$

Notice that by properly choosing the transmissivity of the beam-splitter so that $\lambda' = \sqrt{T}\lambda$, the final state is $|\Psi_{\lambda'}^{(k+l)}\rangle$. Therefore, the last step of the protocol consists of applying the transformation $|\Psi_{\lambda'}^{(k+l)}\rangle \to |\Psi_{\lambda'}^{(k)}\rangle$ described above in order to finalize the map $|\Psi_\lambda^{(k)}\rangle \to |\Psi_{\lambda'}^{(k)}\rangle$. It is important to remark that our protocol is fully deterministic. Despite the randomness of the photon-counter outcome, the determinism is recovered by choosing a different transformation $|\Psi_{\lambda'}^{(k+l)}\rangle \to |\Psi_{\lambda'}^{(k)}\rangle$ for each l, such that the protocol always ends up in the final state $|\Psi_{\lambda'}^{(k)}\rangle$.

[1] B. C. Arnold, *Majorization and the Lorenz Order*, Springer-Verlag Lecture Notes in Statistics **43** (1987).

[2] M. A. Nielsen and G. Vidal, Quant. Inf. Comp. **1,** 76 (2001).

[3] V. Kaftal and G. Weiss, "An infinite dimensional Schur-Horn Theorem and majorization theory", J. Funct. Anal. (2010), doi:10.1016/j.jfa.2010.08.018

[4] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2002).

[6] J. Fiurasek, Phys. Rev. Lett. **89**, 137904 (2002).