

Uncertainty relations with quantum memory for the Wehrl entropy

Giacomo De Palma

Abstract We prove two new fundamental uncertainty relations with quantum memory for the Wehrl entropy. The first relation applies to the bipartite memory scenario. It determines the minimum conditional Wehrl entropy among all the quantum states with a given conditional von Neumann entropy, and proves that this minimum is asymptotically achieved by a suitable sequence of quantum Gaussian states. The second relation applies to the tripartite memory scenario. It determines the minimum of the sum of the Wehrl entropy of a quantum state conditioned on the first memory quantum system with the Wehrl entropy of the same state conditioned on the second memory quantum system, and proves that also this minimum is asymptotically achieved by a suitable sequence of quantum Gaussian states. The Wehrl entropy of a quantum state is the Shannon differential entropy of the outcome of a heterodyne measurement performed on the state. The heterodyne measurement is one of the main measurements in quantum optics, and lies at the basis of one of the most promising protocols for quantum key distribution. These fundamental entropic uncertainty relations will be a valuable tool in quantum information, and will e.g. find application in security proofs of quantum key distribution protocols in the asymptotic regime and in entanglement witnessing in quantum optics.

Keywords entropic uncertainty relations · Wehrl entropy · quantum conditional entropy · quantum Gaussian states

I acknowledge financial support from the European Research Council (ERC Grant Agreements no 337603 and 321029), the Danish Council for Independent Research (Sapere Aude), VILLUM FONDEN via the QMATH Centre of Excellence (Grant No. 10059), and the Marie Skłodowska-Curie Action GENIUS (Grant No. 792557).

Giacomo De Palma
QMATH, Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark
Tel.: +45 35 33 68 04
E-mail: giacomo.depalma@math.ku.dk

Mathematics Subject Classification (2010) 46B28 · 46N50 · 81P45 · 81V80 · 94A15

1 Introduction

Entropic uncertainty relations provide a lower bound to the sum of the entropies of the outcomes of two incompatible measurements performed on the same quantum state. Entropic uncertainty relations are a fundamental tool of quantum information theory, since they are the central ingredient in the security analysis of almost all quantum cryptographic protocols and can be used for entanglement witnessing (see [6] for a review). The quantum information community has recently focused on the scenario with quantum memory [3, 6, 7, 14], where the entropies are conditioned on the knowledge of external observers holding memory quantum systems correlated with the measured system.

The heterodyne measurement [27] is one of the main measurements in quantum optics. It is used for quantum tomography [5], and lies at the basis of one of the most promising quantum key distribution protocols [29, 30]. The Wehrl entropy [31, 32] of a quantum state is the Shannon differential entropy [8] of the outcome of a heterodyne measurement performed on the state. The elements of the POVM that models the heterodyne measurement are the projectors onto the coherent states [1, 16, 19, 20, 28]. Since the coherent states are not orthogonal, the associated projectors do not commute, and nontrivial entropic uncertainty relations are allowed for the heterodyne measurement alone.

The basic uncertainty relation for the Wehrl entropy states that its minimum is achieved by the vacuum state [4, 26]. This relation has been recently improved: it has been proven that thermal quantum Gaussian states minimize the Wehrl entropy among all the quantum states with a given von Neumann entropy [9, 13]. In this paper, we prove two new fundamental uncertainty relations for the Wehrl entropy in the scenario with quantum memory. The first relation (**Theorem 3**) applies to the bipartite scenario with one memory quantum system. It determines the minimum conditional Wehrl entropy among all the quantum states with a given conditional von Neumann entropy, and proves that this minimum is asymptotically achieved by a suitable sequence of quantum Gaussian states (**Theorem 5**). This sequence is built from a two-mode infinitely squeezed pure state shared between the system to be measured and the memory, applying the quantum-limited amplifier to the system to be measured. The second relation (**Theorem 4**) applies to the tripartite scenario with two memory quantum systems. It determines the minimum of the sum of the Wehrl entropy of a quantum state conditioned on the first memory quantum system with the Wehrl entropy of the same quantum state conditioned on the second memory quantum system, and proves that also this minimum is asymptotically achieved by a suitable sequence of quantum Gaussian states (**Theorem 6**). This sequence is the purification of the sequence that saturates

the bipartite memory uncertainty relation, and the purifying system plays the role of the second memory.

The key ingredient of the proof of [Theorem 3](#) is the Entropy Power Inequality with quantum memory [[12, 21](#)]. This fundamental inequality determines the minimum conditional von Neumann entropy of the output of the beam-splitter or of the squeezing among all the input states where the two inputs are conditionally independent given the memory and have given conditional von Neumann entropies. This inequality generalizes the quantum Entropy Power Inequality [[10, 11, 22, 23](#)] to the scenario with quantum memory. The link with the Wehrl entropy is provided by [Theorem 1](#), stating that the heterodyne measurement is asymptotically equivalent to the quantum-limited amplifier in the limit of infinite amplification parameter. The proof of [Theorem 1](#) is based on a new Berezin-Lieb inequality ([Theorem 2](#)) for the scenario with quantum memory.

The fundamental uncertainty relations proven in this paper will be a valuable tool in quantum information and quantum cryptography. Indeed, one of the most promising protocols for quantum key distribution is based on the exchange of Gaussian coherent states and on the heterodyne measurement [[29](#)]. The security of a variant of this protocol has recently been proven [[24, 25](#)]. This variant requires integrating in the protocol a symmetrisation procedure that is difficult to implement. The security of the original protocol without the symmetrisation has not been proven yet. With the uncertainty relations proven in this paper, it will be possible to prove the security of the original protocol in the asymptotic regime of a key of infinite length [[6](#)]. The proof might exploit the techniques of [[15](#)], which proves the security of a quantum key distribution protocol based on the homodyne measurement through an entropic uncertainty relation for the joint measurement of position and momentum. Among the other possible applications of our results, we mention e.g. entanglement witnessing (see [Corollary 1](#)).

The paper is structured as follows. In [section 2](#), we introduce Gaussian quantum systems and the heterodyne measurement. In [section 3](#), we prove the equivalence between heterodyne measurement and quantum-limited amplifier. In [section 4](#) and [section 5](#), we prove the bipartite and tripartite memory entropic uncertainty relations, respectively, and in [section 6](#) we prove their optimality.

2 Gaussian quantum systems

We consider the Hilbert space of M harmonic oscillators, or M modes of the electromagnetic radiation, i.e. the irreducible representation of the canonical commutation relations

$$\left[\hat{a}_i, \hat{a}_j^\dagger \right] = \delta_{ij} \hat{\mathbb{I}}, \quad i, j = 1, \dots, M. \quad (1)$$

The operators $\hat{a}_1^\dagger \hat{a}_1, \dots, \hat{a}_M^\dagger \hat{a}_M$ have integer spectrum and commute. Their joint eigenbasis is the Fock basis $\{|n_1 \dots n_M\rangle\}_{n_1, \dots, n_M \in \mathbb{N}}$. The Hamiltonian

$$\hat{N} = \sum_{i=1}^M \hat{a}_i^\dagger \hat{a}_i \quad (2)$$

counts the number of excitations, or photons. We define the quadratures

$$\hat{Q}_i = \frac{\hat{a}_i + \hat{a}_i^\dagger}{\sqrt{2}}, \quad \hat{P}_i = \frac{\hat{a}_i - \hat{a}_i^\dagger}{i\sqrt{2}}, \quad i = 1, \dots, M. \quad (3)$$

We can collect them in the vector

$$\hat{R}_{2i-1} = \hat{Q}_i, \quad \hat{R}_{2i} = \hat{P}_i, \quad i = 1, \dots, M, \quad (4)$$

and (1) becomes

$$[\hat{R}_i, \hat{R}_j] = i \Delta_{ij} \mathbb{1}, \quad i, j = 1, \dots, 2M, \quad (5)$$

where

$$\Delta = \bigoplus_{i=1}^M \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad (6)$$

is the symplectic form.

2.1 Quantum Gaussian states

A quantum Gaussian state is a density operator proportional to the exponential of a quadratic polynomial in the quadratures:

$$\hat{\gamma} = \frac{\exp\left(-\frac{1}{2} \sum_{i,j=1}^{2M} h_{ij} \hat{R}_i \hat{R}_j\right)}{\text{Tr} \exp\left(-\frac{1}{2} \sum_{i,j=1}^{2M} h_{ij} \hat{R}_i \hat{R}_j\right)}, \quad (7)$$

where h is a positive real $2M \times 2M$ matrix. A quantum Gaussian state is completely identified by its covariance matrix

$$\sigma_{ij} = \frac{1}{2} \text{Tr} \left[\left(\hat{R}_i \hat{R}_j + \hat{R}_j \hat{R}_i \right) \hat{\gamma} \right], \quad i, j = 1, \dots, 2M. \quad (8)$$

The von Neumann entropy of a quantum Gaussian state is

$$S = \sum_{i=1}^M g\left(\nu_i - \frac{1}{2}\right), \quad (9)$$

where

$$g(x) = (x+1) \ln(x+1) - x \ln x, \quad (10)$$

and ν_1, \dots, ν_M are the symplectic eigenvalues of its covariance matrix σ , i.e., the absolute values of the eigenvalues of $\sigma \Delta^{-1}$.

2.2 Coherent states

The classical phase space associated with a M -mode Gaussian quantum system is \mathbb{C}^M , and for any $\mathbf{z} \in \mathbb{C}^M$ we define the coherent state

$$|\mathbf{z}\rangle = e^{-\frac{|\mathbf{z}|^2}{2}} \sum_{n_1, \dots, n_M=0}^{\infty} \frac{z_1^{n_1} \dots z_M^{n_M}}{\sqrt{n_1! \dots n_M!}} |n_1 \dots n_M\rangle. \quad (11)$$

Coherent states satisfy the resolution of the identity [17]

$$\int_{\mathbb{C}^M} |\mathbf{z}\rangle \langle \mathbf{z}| \frac{d^{2M}z}{\pi^M} = \hat{\mathbb{I}}, \quad (12)$$

where the integral converges in the weak topology. The POVM associated with the resolution of the identity (12) is called heterodyne measurement [27].

2.3 The Gaussian quantum-limited amplifier

The M -mode Gaussian quantum-limited amplifier \mathcal{A}_κ with amplification parameter $\kappa \geq 1$ performs a two-mode squeezing on the input state $\hat{\rho}$ and the vacuum state of an M -mode ancillary Gaussian system E with ladder operators $\hat{e}_1, \dots, \hat{e}_M$:

$$\mathcal{A}_\kappa(\hat{\rho}) = \text{Tr}_E \left[\hat{U}_\kappa (\hat{\rho} \otimes |\mathbf{0}\rangle \langle \mathbf{0}|) \hat{U}_\kappa^\dagger \right]. \quad (13)$$

The squeezing unitary operator

$$\hat{U}_\kappa = \exp \left(\text{arccosh} \sqrt{\kappa} \sum_{i=1}^M (\hat{a}_i^\dagger \hat{e}_i^\dagger - \hat{a}_i \hat{e}_i) \right) \quad (14)$$

acts on the ladder operators as

$$\hat{U}_\kappa^\dagger \hat{a}_i \hat{U}_\kappa = \sqrt{\kappa} \hat{a}_i + \sqrt{\kappa - 1} \hat{e}_i^\dagger, \quad (15a)$$

$$\hat{U}_\kappa^\dagger \hat{e}_i \hat{U}_\kappa = \sqrt{\kappa - 1} \hat{a}_i^\dagger + \sqrt{\kappa} \hat{e}_i, \quad i = 1, \dots, M. \quad (15b)$$

The Gaussian quantum-limited amplifier acts on quantum Gaussian states as follows. Let A and B be Gaussian quantum systems with M_A and M_B modes, respectively. Let $\hat{\gamma}_{AB}$ be the joint quantum Gaussian state on AB with covariance matrix

$$\sigma_{AB} = \frac{1}{2} \begin{pmatrix} X & Z \\ Z^T & Y \end{pmatrix}. \quad (16)$$

Then, $(\mathcal{A}_\kappa \otimes \mathbb{I}_B)(\hat{\gamma}_{AB})$ is the quantum Gaussian state with covariance matrix

$$\sigma'_{AB} = \frac{1}{2} \begin{pmatrix} \kappa X + (\kappa - 1) I_{M_A} & \sqrt{\kappa} Z \\ \sqrt{\kappa} Z^T & Y \end{pmatrix}. \quad (17)$$

3 Asymptotic equivalence between heterodyne measurement and amplifier

In this Section, we extend the asymptotic equivalence between the heterodyne measurement and the quantum-limited amplifier proven in [9] to the scenario with quantum memory.

Theorem 1 (heterodyne measurement - amplifier equivalence) *Let A be an M -mode Gaussian quantum system and B a generic quantum system. For any concave function $f : [0, 1] \rightarrow [0, \infty)$ and for any joint quantum state $\hat{\rho}_{AB}$ on AB ,*

$$\int_{\mathbb{C}^M} \text{Tr}_B f(\langle \mathbf{z} | \hat{\rho}_{AB} | \mathbf{z} \rangle) \geq \limsup_{\kappa \rightarrow \infty} \frac{\text{Tr}_{AB} f(\kappa^M (\mathcal{A}_\kappa \otimes \mathbb{I}_B)(\hat{\rho}_{AB}))}{\kappa^M}. \quad (18)$$

3.1 Proof of Theorem 1

The proof is based on the following generalization of the Berezin-Lieb inequality [2] to the scenario with quantum memory.

Theorem 2 (Berezin-Lieb inequality with quantum memory) *Let A be an M -mode Gaussian quantum system and B a generic quantum system. Then, for any trace-class operator \hat{X} on AB with $0 \leq \hat{X} \leq \hat{\mathbb{I}}_{AB}$ and any concave function $f : [0, 1] \rightarrow [0, \infty)$,*

$$\int_{\mathbb{C}^M} \text{Tr}_B f(\langle \mathbf{z} | \hat{X} | \mathbf{z} \rangle) \frac{d^{2M}z}{\pi^M} \geq \text{Tr}_{AB} f(\hat{X}). \quad (19)$$

Proof Let us diagonalize \hat{X} :

$$\hat{X} = \sum_{k=0}^{\infty} x_k |\psi_k\rangle\langle\psi_k|, \quad \langle\psi_k|\psi_l\rangle = \delta_{kl} \quad \forall k, l \in \mathbb{N}, \quad \sum_{k=0}^{\infty} |\psi_k\rangle\langle\psi_k| = \hat{\mathbb{I}}_{AB}. \quad (20)$$

We have

$$0 \leq x_k \leq 1 \quad \forall k \in \mathbb{N}, \quad \sum_{k=0}^{\infty} x_k < \infty. \quad (21)$$

From the completeness of the $|\psi_k\rangle$ we have for any $\mathbf{z} \in \mathbb{C}^M$

$$\sum_{k=0}^{\infty} \langle \mathbf{z} | \psi_k \rangle \langle \psi_k | \mathbf{z} \rangle = \langle \mathbf{z} | \hat{\mathbb{I}}_{AB} | \mathbf{z} \rangle = \hat{\mathbb{I}}_B. \quad (22)$$

We can then apply Lemma 1 to $|\phi_k\rangle = \langle \mathbf{z} | \psi_k \rangle$ and get

$$\begin{aligned} \text{Tr}_B f(\langle \mathbf{z} | \hat{X} | \mathbf{z} \rangle) &= \text{Tr}_B f\left(\sum_{k=0}^{\infty} x_k \langle \mathbf{z} | \psi_k \rangle \langle \psi_k | \mathbf{z} \rangle\right) \geq \sum_{k=0}^{\infty} \langle \psi_k | \mathbf{z} \rangle \langle \mathbf{z} | \psi_k \rangle f(x_k) \\ &= \text{Tr}_B \langle \mathbf{z} | f(\hat{X}) | \mathbf{z} \rangle. \end{aligned} \quad (23)$$

Finally, from the completeness relation (12) we have

$$\int_{\mathbb{C}^M} \mathrm{Tr}_B f \left(\langle \mathbf{z} | \hat{X} | \mathbf{z} \rangle \right) \frac{d^{2M}z}{\pi^M} \geq \int_{\mathbb{C}^M} \mathrm{Tr}_B \langle \mathbf{z} | f(\hat{X}) | \mathbf{z} \rangle \frac{d^{2M}z}{\pi^M} = \mathrm{Tr}_{AB} f(\hat{X}) . \quad (24)$$

From [18], Theorem 9, the map $\kappa^M \mathcal{A}_\kappa$ is unital, and

$$0 \leq \kappa^M(\mathcal{A}_\kappa \otimes \mathbb{I}_B)(\hat{\rho}_{AB}) \leq \kappa^M(\mathcal{A}_\kappa \otimes \mathbb{I}_B) \left(\hat{\mathbb{I}}_{AB} \right) = \hat{\mathbb{I}}_{AB} . \quad (25)$$

We can then apply Theorem 2 to $\hat{X} = \kappa^M(\mathcal{A}_\kappa \otimes \mathbb{I}_B)(\hat{\rho}_{AB})$ and get

$$\int_{\mathbb{C}^M} \mathrm{Tr}_B f \left(\kappa^M \langle \mathbf{z} | (\mathcal{A}_\kappa \otimes \mathbb{I}_B)(\hat{\rho}_{AB}) | \mathbf{z} \rangle \right) \frac{d^{2M}z}{\pi^M} \geq \mathrm{Tr}_{AB} f \left(\kappa^M(\mathcal{A}_\kappa \otimes \mathbb{I}_B)(\hat{\rho}_{AB}) \right) . \quad (26)$$

Since for any $\mathbf{z} \in \mathbb{C}^M$

$$\kappa^M \langle \mathbf{z} | (\mathcal{A}_\kappa \otimes \mathbb{I}_B)(\hat{\rho}_{AB}) | \mathbf{z} \rangle = \langle \mathbf{z} / \sqrt{\kappa} | \hat{\rho}_{AB} | \mathbf{z} / \sqrt{\kappa} \rangle \quad (27)$$

([9], Lemma 4), (26) becomes

$$\int_{\mathbb{C}^M} \mathrm{Tr}_B f \left(\langle \mathbf{z} | \hat{\rho}_{AB} | \mathbf{z} \rangle \right) \frac{d^{2M}z}{\pi^M} \geq \frac{1}{\kappa^M} \mathrm{Tr}_{AB} f \left(\kappa^M(\mathcal{A}_\kappa \otimes \mathbb{I}_B)(\hat{\rho}_{AB}) \right) , \quad (28)$$

and the claim follows taking the limit $\kappa \rightarrow \infty$.

4 Bipartite quantum memory uncertainty relation for the Wehrl entropy

Theorem 3 (bipartite quantum memory uncertainty relation for the Wehrl entropy) *Let A be an M -mode Gaussian quantum system and B a generic quantum system. Let $\hat{\rho}_{AB}$ be a joint quantum state on AB such that its marginal $\hat{\rho}_A = \mathrm{Tr}_B \hat{\rho}_{AB}$ has finite average energy, and its marginal $\hat{\rho}_B = \mathrm{Tr}_A \hat{\rho}_{AB}$ has finite von Neumann entropy. Let $\hat{\rho}_{ZB}$ be the probability measure on \mathbb{C}^M taking values in positive operators on B associated with the heterodyne measurement on A :*

$$d\hat{\rho}_{ZB}(\mathbf{z}) = \langle \mathbf{z} | \hat{\rho}_{AB} | \mathbf{z} \rangle \frac{d^{2M}z}{\pi^M} , \quad \mathbf{z} \in \mathbb{C}^M . \quad (29)$$

Then, the following bipartite quantum memory uncertainty relation holds:

$$S(Z|B)_{\hat{\rho}_{ZB}} \geq M \ln \left(\exp \frac{S(A|B)_{\hat{\rho}_{AB}}}{M} + 1 \right) \geq 0 , \quad (30)$$

where

$$S(Z|B)_{\hat{\rho}_{ZB}} = S(\hat{\rho}_{ZB}) - S(\hat{\rho}_B) \quad (31)$$

is the Shannon differential entropy of the outcome Z of the heterodyne measurement performed on A conditioned on the quantum system B , and

$$S(\hat{\rho}_{ZB}) = - \int_{\mathbb{C}^M} \text{Tr}_B [\langle \mathbf{z} | \hat{\rho}_{AB} | \mathbf{z} \rangle \ln \langle \mathbf{z} | \hat{\rho}_{AB} | \mathbf{z} \rangle] \frac{d^{2M}z}{\pi^M} \quad (32)$$

is the joint entropy of Z and B .

Remark 1 If B is the trivial system, (30) becomes

$$S(\hat{\rho}_Z) \geq M \ln \left(\exp \frac{S(\hat{\rho}_A)}{M} + 1 \right) \geq 0. \quad (33)$$

However, the optimal inequality satisfied by the unconditioned Wehrl entropy is [9]

$$S(\hat{\rho}_Z) \geq M \ln \left(g^{-1} \left(\frac{S(\hat{\rho}_A)}{M} \right) + 1 \right) + M \geq M, \quad (34)$$

that is strictly stronger than (33). The presence of the quantum memory then both changes the form of the optimal inequality and reduces the minimum uncertainty: while the minimum Wehrl entropy is M , the minimum conditional Wehrl entropy is 0.

Corollary 1 (entanglement witnessing) *Under the hypotheses of Theorem 3, if the quantum state $\hat{\rho}_{AB}$ is separable, the following bipartite quantum memory uncertainty relation holds:*

$$S(Z|B)_{\hat{\rho}_{ZB}} \geq M \ln 2. \quad (35)$$

Proof Since $\hat{\rho}_{AB}$ is separable, we have $S(A|B)_{\hat{\rho}_{AB}} \geq 0$. The claim then follows from Theorem 3.

4.1 Proof of Theorem 3

Applying Theorem 1 to $f(x) = -x \ln x$ we get

$$S(\hat{\rho}_{ZB}) \geq \limsup_{\kappa \rightarrow \infty} (S((\mathcal{A}_\kappa \otimes \mathbb{I}_B)(\hat{\rho}_{AB})) - M \ln \kappa). \quad (36)$$

Subtracting $S(\hat{\rho}_B)$ on both sides we get

$$S(Z|B)_{\hat{\rho}_{ZB}} \geq \limsup_{\kappa \rightarrow \infty} (S(A|B)_{(\mathcal{A}_\kappa \otimes \mathbb{I}_B)(\hat{\rho}_{AB})} - M \ln \kappa). \quad (37)$$

From the Entropy Power Inequality with quantum memory [12],

$$S(A|B)_{(\mathcal{A}_\kappa \otimes \mathbb{I}_B)(\hat{\rho}_{AB})} \geq M \ln \left(\kappa \exp \frac{S(A|B)_{\hat{\rho}_{AB}}}{M} + \kappa - 1 \right). \quad (38)$$

We then have

$$\begin{aligned} S(Z|B)_{\hat{\rho}_{ZB}} &\geq M \limsup_{\kappa \rightarrow \infty} \ln \left(\exp \frac{S(A|B)_{\hat{\rho}_{AB}}}{M} + 1 - \frac{1}{\kappa} \right) \\ &= M \ln \left(\exp \frac{S(A|B)_{\hat{\rho}_{AB}}}{M} + 1 \right). \end{aligned} \quad (39)$$

5 Tripartite quantum memory uncertainty relation for the Wehrl entropy

Theorem 4 (tripartite quantum memory uncertainty relation for the Wehrl entropy) *Let A be an M -mode Gaussian quantum system, and let B, C be arbitrary quantum systems. Let $\hat{\rho}_{ABC}$ be a joint quantum state on ABC such that its marginal $\hat{\rho}_A = \text{Tr}_{BC}\hat{\rho}_{ABC}$ has finite average energy, and its marginals $\hat{\rho}_B = \text{Tr}_{AC}\hat{\rho}_{ABC}$ and $\hat{\rho}_C = \text{Tr}_{AB}\hat{\rho}_{ABC}$ have finite von Neumann entropy. Let $\hat{\rho}_{ZBC}$ be the probability measure on \mathbb{C}^M taking values in positive operators on BC associated with the heterodyne measurement on A :*

$$d\hat{\rho}_{ZBC}(\mathbf{z}) = \langle \mathbf{z} | \hat{\rho}_{ABC} | \mathbf{z} \rangle \frac{d^{2M}z}{\pi^M}, \quad \mathbf{z} \in \mathbb{C}^M. \quad (40)$$

Then, the following tripartite quantum memory uncertainty relation holds:

$$S(Z|B)_{\hat{\rho}_{ZB}} + S(Z|C)_{\hat{\rho}_{ZC}} \geq M \ln 4, \quad (41)$$

where $S(Z|B)_{\hat{\rho}_{ZB}}$ and $S(Z|C)_{\hat{\rho}_{ZC}}$ are defined as in (31).

Proof Let us first prove that we can assume $\hat{\rho}_{ABC}$ pure. Let $\hat{\rho}_{ABCR}$ be a purification of $\hat{\rho}_{ABC}$. We have from the data-processing inequality for the quantum conditional entropy

$$S(Z|C)_{\hat{\rho}_{ZC}} \geq S(Z|CR)_{\hat{\rho}_{ZCR}}. \quad (42)$$

Defining $C' = CR$, we have

$$S(Z|B)_{\hat{\rho}_{ZB}} + S(Z|C)_{\hat{\rho}_{ZC}} \geq S(Z|B)_{\hat{\rho}_{ZB}} + S(Z|C')_{\hat{\rho}_{ZC'}}, \quad (43)$$

and we can then assume $\hat{\rho}_{ABC}$ pure.

For any $\mathbf{z} \in \mathbb{C}^M$, the state

$$\hat{\rho}_{BC|Z=\mathbf{z}} = \frac{\langle \mathbf{z} | \hat{\rho}_{ABC} | \mathbf{z} \rangle}{\langle \mathbf{z} | \hat{\rho}_A | \mathbf{z} \rangle} \quad (44)$$

is also pure, hence

$$S(\hat{\rho}_{B|Z=\mathbf{z}}) = S(\hat{\rho}_{C|Z=\mathbf{z}}), \quad (45)$$

and

$$S(B|Z)_{\hat{\rho}_{ZB}} = S(C|Z)_{\hat{\rho}_{ZC}}. \quad (46)$$

We then have

$$\begin{aligned} S(Z|C)_{\hat{\rho}_{ZC}} &= S(C|Z)_{\hat{\rho}_{ZC}} + S(\hat{\rho}_Z) - S(\hat{\rho}_C) = S(B|Z)_{\hat{\rho}_{ZB}} + S(\hat{\rho}_Z) - S(\hat{\rho}_{AB}) \\ &= S(Z|B)_{\hat{\rho}_{ZB}} - S(A|B)_{\hat{\rho}_{AB}}. \end{aligned} \quad (47)$$

Finally, [Theorem 3](#) implies

$$\begin{aligned} S(Z|B)_{\hat{\rho}_{ZB}} + S(Z|C)_{\hat{\rho}_{ZC}} &= 2S(Z|B)_{\hat{\rho}_{ZB}} - S(A|B)_{\hat{\rho}_{AB}} \\ &\geq M \ln \left(2 + 2 \cosh \frac{S(A|B)_{\hat{\rho}_{AB}}}{M} \right) \geq M \ln 4. \end{aligned} \quad (48)$$

6 Optimality of the uncertainty relations

Theorem 5 (optimality of the bipartite memory uncertainty relation) *The uncertainty relation with bipartite memory (30) is optimal and the minimum (30) for $S(Z|B)$ is asymptotically achieved by a suitable sequence of quantum Gaussian states. Indeed, let A and B be M -mode Gaussian quantum systems, and for any $a \geq 1$ let $\hat{\gamma}_{AB}^{(a)}$ be the tensor product of M two-mode squeezed pure quantum Gaussian states, with covariance matrix*

$$\sigma_{AB}^{(a)} = \bigoplus_{i=1}^M \frac{1}{2} \begin{pmatrix} a I_2 & \sqrt{a^2 - 1} \sigma_Z \\ \sqrt{a^2 - 1} \sigma_Z & a I_2 \end{pmatrix}, \quad (49)$$

where

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (50)$$

Let us fix $s \in \mathbb{R}$, and let us define

$$\kappa = \exp \frac{s}{M} + 1. \quad (51)$$

Then, the quantum Gaussian state

$$\hat{\gamma}_{AB}^{(s,a)} = (\mathcal{A}_\kappa \otimes \mathbb{I}_B) \left(\hat{\gamma}_{AB}^{(a)} \right) \quad (52)$$

satisfies

$$\lim_{a \rightarrow \infty} S(A|B)_{\hat{\gamma}_{AB}^{(s,a)}} = s, \quad \lim_{a \rightarrow \infty} S(Z|B)_{\hat{\gamma}_{AB}^{(s,a)}} = M \ln \left(\exp \frac{s}{M} + 1 \right), \quad (53)$$

where $\hat{\gamma}_{ZB}^{(s,a)}$ is the probability measure on \mathbb{C}^M with values in positive operators on B associated to the heterodyne measurement on A , defined as in (29).

Proof The quantum Gaussian state $\hat{\gamma}_{AB}^{(s,a)}$ has covariance matrix

$$\sigma_{AB}^{(s,a)} = \bigoplus_{i=1}^M \frac{1}{2} \begin{pmatrix} (\kappa a + \kappa - 1) I_2 & \sqrt{\kappa(a^2 - 1)} \sigma_Z \\ \sqrt{\kappa(a^2 - 1)} \sigma_Z & a I_2 \end{pmatrix}, \quad (54)$$

whose symplectic eigenvalues are

$$\nu_+ = \frac{\kappa a + \kappa - a}{2}, \quad \nu_- = \frac{1}{2}, \quad (55)$$

each with multiplicity M . We then have

$$S(A|B)_{\hat{\gamma}_{AB}^{(s,a)}} = M g \left(\frac{\kappa a + \kappa - a - 1}{2} \right) - M g \left(\frac{a - 1}{2} \right), \quad (56)$$

and

$$\lim_{a \rightarrow \infty} S(A|B)_{\hat{\gamma}_{AB}^{(s,a)}} = M \ln(\kappa - 1) = s. \quad (57)$$

From [9], Lemma 4, we have for any $\mathbf{z} \in \mathbb{C}^M$

$$\langle \mathbf{z} | \hat{\gamma}_{AB}^{(s,a)} | \mathbf{z} \rangle = \langle \mathbf{z} | (\mathcal{A}_\kappa \otimes \mathbb{I}_B) \left(\hat{\gamma}_{AB}^{(a)} \right) | \mathbf{z} \rangle = \frac{\langle \mathbf{z} / \sqrt{\kappa} | \hat{\gamma}_{AB}^{(a)} | \mathbf{z} / \sqrt{\kappa} \rangle}{\kappa^M}, \quad (58)$$

where $|\mathbf{z}\rangle$ is the coherent state on A . Then, since $\hat{\gamma}_{AB}^{(a)}$ is pure, also $\langle \mathbf{z} | \hat{\gamma}_{AB}^{(s,a)} | \mathbf{z} \rangle$ is pure and

$$S(B|Z)_{\hat{\gamma}_{ZB}^{(s,a)}} = 0. \quad (59)$$

We have from [9], Eq. (70)

$$S\left(\hat{\gamma}_Z^{(s,a)}\right) = M \ln \frac{\kappa(a+1)}{2} + M, \quad (60)$$

hence

$$\begin{aligned} S(Z|B)_{\hat{\gamma}_{ZB}^{(s,a)}} &= S(B|Z)_{\hat{\gamma}_{ZB}^{(s,a)}} + S\left(\hat{\gamma}_Z^{(s,a)}\right) - S\left(\hat{\gamma}_B^{(s,a)}\right) \\ &= M \ln \frac{\kappa(a+1)}{2} + M - M g\left(\frac{a-1}{2}\right). \end{aligned} \quad (61)$$

Finally,

$$\lim_{a \rightarrow \infty} S(Z|B)_{\hat{\gamma}_{ZB}^{(s,a)}} = M \ln \kappa = M \ln \left(\exp \frac{s}{M} + 1 \right). \quad (62)$$

Theorem 6 (optimality of the tripartite memory uncertainty relation) *The uncertainty relation with tripartite memory (41) is optimal and the value $M \ln 4$ for $S(Z|A) + S(Z|B)$ is asymptotically achieved by a suitable sequence of quantum Gaussian states. Indeed, for any $a \geq 1$ let $\hat{\gamma}_{ABC}^{(0,a)}$ be the purification of the quantum Gaussian state $\hat{\gamma}_{AB}^{(0,a)}$ defined in (52). We then have*

$$\lim_{a \rightarrow \infty} \left(S(Z|B)_{\hat{\gamma}_{ZB}^{(0,a)}} + S(Z|C)_{\hat{\gamma}_{ZC}^{(0,a)}} \right) = M \ln 4. \quad (63)$$

Proof From Theorem 5 we have

$$\lim_{a \rightarrow \infty} S(A|B)_{\hat{\gamma}_{AB}^{(0,a)}} = 0, \quad \lim_{a \rightarrow \infty} S(Z|B)_{\hat{\gamma}_{ZB}^{(0,a)}} = M \ln 2. \quad (64)$$

We then have from (48)

$$\begin{aligned} \lim_{a \rightarrow \infty} \left(S(Z|B)_{\hat{\gamma}_{ZB}^{(0,a)}} + S(Z|C)_{\hat{\gamma}_{ZC}^{(0,a)}} \right) &= \lim_{a \rightarrow \infty} \left(2S(Z|B)_{\hat{\gamma}_{ZB}^{(0,a)}} - S(A|B)_{\hat{\gamma}_{AB}^{(0,a)}} \right) \\ &= M \ln 4. \end{aligned} \quad (65)$$

A

Lemma 1 (Jensen's trace inequality) *Let us consider the operator*

$$\hat{A} = \sum_{k=0}^{\infty} a_k |\phi_k\rangle\langle\phi_k|, \quad 0 \leq a_k \leq 1 \quad \forall k \in \mathbb{N}, \quad \sum_{k=0}^{\infty} a_k < \infty, \quad (66)$$

where the vectors $|\phi_k\rangle$ form a resolution of the identity:

$$\sum_{k=0}^{\infty} |\phi_k\rangle\langle\phi_k| = \hat{\mathbb{1}}. \quad (67)$$

Then, for any concave function $f : [0, 1] \rightarrow [0, \infty)$,

$$\text{Tr } f(\hat{A}) \geq \sum_{k=0}^{\infty} f(a_k) \langle\phi_k|\phi_k\rangle. \quad (68)$$

Proof From (67) we get

$$\langle\phi_k|\phi_k\rangle \leq 1 \quad \forall k \in \mathbb{N}. \quad (69)$$

We then have

$$\text{Tr } \hat{A} = \sum_{k=0}^{\infty} a_k \langle\phi_k|\phi_k\rangle \leq \sum_{k=0}^{\infty} a_k < \infty. \quad (70)$$

\hat{A} has then discrete spectrum, and we can diagonalize it:

$$\hat{A} = \sum_{l=0}^{\infty} \lambda_l |v_l\rangle\langle v_l|, \quad \langle v_k|v_l\rangle = \delta_{kl} \quad \forall k, l \in \mathbb{N}, \quad \sum_{l=0}^{\infty} |v_l\rangle\langle v_l| = \hat{\mathbb{1}}. \quad (71)$$

From the completeness of the $|\phi_k\rangle$, for any $l \in \mathbb{N}$

$$\sum_{k=0}^{\infty} |\langle v_l|\phi_k\rangle|^2 = \langle v_l|v_l\rangle = 1, \quad (72)$$

hence $|\langle v_l|\phi_k\rangle|^2$ is a probability distribution on \mathbb{N} . We then have from Jensen's inequality

$$\begin{aligned} \text{Tr } f(\hat{A}) &= \sum_{l=0}^{\infty} f(\lambda_l) = \sum_{l=0}^{\infty} f\left(\sum_{k=0}^{\infty} |\langle v_l|\phi_k\rangle|^2 a_k\right) \geq \sum_{k, l=0}^{\infty} |\langle v_l|\phi_k\rangle|^2 f(a_k) \\ &= \sum_{k=0}^{\infty} \langle\phi_k|\phi_k\rangle f(a_k), \end{aligned} \quad (73)$$

where we have used that for the completeness of the $|v_l\rangle$, for any $k \in \mathbb{N}$

$$\sum_{l=0}^{\infty} |\langle v_l|\phi_k\rangle|^2 = \langle\phi_k|\phi_k\rangle. \quad (74)$$

References

1. Bargmann, V.: On a hilbert space of analytic functions and an associated integral transform part i. Communications on pure and applied mathematics **14**(3), 187–214 (1961)
2. Berezin, F.A.: Covariant and contravariant symbols of operators. Izvestiya: Mathematics **6**(5), 1117–1151 (1972)

3. Berta, M., Christandl, M., Colbeck, R., Renes, J.M., Renner, R.: The uncertainty principle in the presence of quantum memory. *Nature Physics* **6**(9), 659–662 (2010)
4. Carlen, E.A.: Some integral identities and inequalities for entire functions and their application to the coherent state transform. *Journal of functional analysis* **97**(1), 231–249 (1991)
5. Carmichael, H.: *Statistical Methods in Quantum Optics 1: Master Equations and Fokker-Planck Equations*. Theoretical and Mathematical Physics. Springer Berlin Heidelberg (2013)
6. Coles, P.J., Berta, M., Tomamichel, M., Wehner, S.: Entropic uncertainty relations and their applications. *Rev. Mod. Phys.* **89**, 015,002 (2017)
7. Coles, P.J., Colbeck, R., Yu, L., Zvolak, M.: Uncertainty relations from simple entropic properties. *Physical Review Letters* **108**(21), 210,405 (2012)
8. Cover, T., Thomas, J.: *Elements of Information Theory*. A Wiley-Interscience publication. Wiley (2006)
9. De Palma, G.: The wehrl entropy has gaussian optimizers. *Letters in Mathematical Physics* **108**(1), 97–116 (2018)
10. De Palma, G., Mari, A., Giovannetti, V.: A generalization of the entropy power inequality to bosonic quantum systems. *Nature Photonics* **8**(12), 958–964 (2014)
11. De Palma, G., Mari, A., Lloyd, S., Giovannetti, V.: Multimode quantum entropy power inequality. *Physical Review A* **91**(3), 032,320 (2015)
12. De Palma, G., Trevisan, D.: The conditional entropy power inequality for bosonic quantum systems. *Communications in Mathematical Physics* pp. 1–24 (2018)
13. De Palma, G., Trevisan, D., Giovannetti, V.: Multimode gaussian optimizers for the wehrl entropy and quantum gaussian channels. arXiv preprint arXiv:1705.00499 (2017)
14. Furrer, F., Berta, M., Tomamichel, M., Scholz, V.B., Christandl, M.: Position-momentum uncertainty relations in the presence of quantum memory. *Journal of Mathematical Physics* **55**(12), 122,205 (2014)
15. Furrer, F., Franz, T., Berta, M., Leverrier, A., Scholz, V.B., Tomamichel, M., Werner, R.F.: Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. *Physical review letters* **109**(10), 100,502 (2012)
16. Glauber, R.J.: Coherent and incoherent states of the radiation field. *Physical Review* **131**(6), 2766 (1963)
17. Holevo, A.S.: Gaussian optimizers and the additivity problem in quantum information theory. *Russian Mathematical Surveys* **70**(2), 331 (2015)
18. Ivan, J.S., Sabapathy, K.K., Simon, R.: Operator-sum representation for bosonic gaussian channels. *Physical Review A* **84**(4), 042,311 (2011)
19. Klauder, J., Sudarshan, E.: *Fundamentals of Quantum Optics*. Dover books on physics. Dover Publications (2006)
20. Klauder, J.R.: The action option and a feynman quantization of spinor fields in terms of ordinary c-numbers. *Annals of Physics* **11**(2), 123–168 (1960)
21. König, R.: The conditional entropy power inequality for gaussian quantum states. *Journal of Mathematical Physics* **56**(2), 022,201 (2015)
22. König, R., Smith, G.: The entropy power inequality for quantum systems. *IEEE Transactions on Information Theory* **60**(3), 1536–1548 (2014)
23. König, R., Smith, G.: Corrections to “the entropy power inequality for quantum systems”. *IEEE Transactions on Information Theory* **62**(7), 4358–4359 (2016)
24. Leverrier, A.: $su(p, q)$ coherent states and a gaussian de finetti theorem. arXiv preprint arXiv:1612.05080 (2016)
25. Leverrier, A.: Security of continuous-variable quantum key distribution via a gaussian de finetti reduction. *Physical Review Letters* **118**(20), 200,501 (2017)
26. Lieb, E.H.: Proof of an entropy conjecture of wehrl. *Communications in Mathematical Physics* **62**(1), 35–41 (1978)
27. Schleich, W.: *Quantum Optics in Phase Space*. Wiley (2015)
28. Schrödinger, E.: Der stetige übergang von der mikro-zur makromechanik. *Naturwissenschaften* **14**(28), 664–666 (1926)
29. Weedbrook, C., Lance, A.M., Bowen, W.P., Symul, T., Ralph, T.C., Lam, P.K.: Quantum cryptography without switching. *Physical review letters* **93**(17), 170,504 (2004)
30. Weedbrook, C., Pirandola, S., Garcia-Patron, R., Cerf, N.J., Ralph, T.C., Shapiro, J.H., Lloyd, S.: Gaussian quantum information. *Reviews of Modern Physics* **84**(2), 621 (2012)

31. Wehrl, A.: General properties of entropy. *Reviews of Modern Physics* **50**(2), 221 (1978)
32. Wehrl, A.: On the relation between classical and quantum-mechanical entropy. *Reports on Mathematical Physics* **16**(3), 353–358 (1979)