



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

ARCHIVIO ISTITUZIONALE
DELLA RICERCA

Alma Mater Studiorum Università di Bologna
Archivio istituzionale della ricerca

The entropy power inequality with quantum conditioning

This is the final peer-reviewed author's accepted manuscript (postprint) of the following publication:

Published Version:

The entropy power inequality with quantum conditioning / De Palma, G. - In: JOURNAL OF PHYSICS. A, MATHEMATICAL AND THEORETICAL. - ISSN 1751-8113. - ELETTRONICO. - 52:8(2019), pp. 08LT03.1-08LT03.12. [10.1088/1751-8121/aaff4]

Availability:

This version is available at: <https://hdl.handle.net/11585/845025> since: 2022-01-12

Published:

DOI: <http://doi.org/10.1088/1751-8121/aaff4>

Terms of use:

Some rights reserved. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

This item was downloaded from IRIS Università di Bologna (<https://cris.unibo.it/>).
When citing, please refer to the published version.

(Article begins on next page)

This is the final peer-reviewed accepted manuscript of:

Giacomo De Palma 2019 *J. Phys. A: Math. Theor.* 52 08LT03

The final published version is available online at: <https://dx.doi.org/10.1088/1751-8121/aaff4>

Rights / License:

The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

This item was downloaded from IRIS Università di Bologna (<https://cris.unibo.it/>)

When citing, please refer to the published version.

The Entropy Power Inequality with quantum conditioning

Giacomo De Palma

QMATH, Department of Mathematical Sciences, University of Copenhagen,
Universitetsparken 5, 2100 Copenhagen, Denmark

Abstract

The conditional Entropy Power Inequality is a fundamental inequality in information theory, stating that the conditional entropy of the sum of two conditionally independent vector-valued random variables each with an assigned conditional entropy is minimum when the random variables are Gaussian. We prove the conditional Entropy Power Inequality in the scenario where the conditioning system is quantum. The proof is based on the heat semigroup and on a generalization of the Stam inequality in the presence of quantum conditioning. The Entropy Power Inequality with quantum conditioning will be a key tool of quantum information, with applications in distributed source coding protocols with the assistance of quantum entanglement.

1 Introduction

The Shannon differential entropy [1] of a random variable X with values in \mathbb{R}^n and probability density function $p(x)$ is

$$S(X) = - \int_{\mathbb{R}^n} p(x) \ln p(x) dx , \quad (1)$$

and quantifies the information got when the value of X is revealed.

A fundamental problem in information theory is the following. Given $a, b \in \mathbb{R}$, let X and Y be independent random variables with values in \mathbb{R}^n

such that $S(X) = a$ and $S(Y) = b$. What is the minimum possible value of $S(X + Y)$? The Entropy Power Inequality [2–4] states that this minimum is achieved when X and Y have a Gaussian probability distribution with proportional covariance matrices, and reads

$$\exp \frac{2S(X + Y)}{n} \geq \exp \frac{2S(X)}{n} + \exp \frac{2S(Y)}{n} . \quad (2)$$

The Entropy Power Inequality is a fundamental tool of information theory [1]. It was introduced by Shannon to provide an upper bound to the information capacity of non-Gaussian channels [4], and was later employed to bound the information capacity region of the Gaussian broadcast channel [5] and the secret information capacity of the Gaussian wiretap channel [6] and to prove the convergence in relative entropy for the central limit theorem [7]. The Entropy Power Inequality was also extended to the Rényi entropies [8] and to the framework of free probability theory [9].

Let the random variable X with values in \mathbb{R}^n be correlated with the random variable M with values in the countable set \mathcal{M} . For any $m \in \mathcal{M}$, let $q(m)$ be the probability that $M = m$, and let $p(x|m)$ be the probability density of X conditioned on $M = m$. The Shannon differential entropy of X conditioned on M is [1]

$$S(X|M) = \sum_{m \in \mathcal{M}} q(m) S(X|M = m) , \quad (3)$$

where for any $m \in \mathcal{M}$

$$S(X|M = m) = - \int_{\mathbb{R}^n} p(x|m) \ln p(x|m) dx \quad (4)$$

is the Shannon differential entropy of X conditioned on $M = m$.

The conditional Entropy Power Inequality [10, 11] solves the conditional version of the problem above. Given $a, b \in \mathbb{R}$, let X and Y be random variables with values in \mathbb{R}^n correlated with the random variable M with values in \mathcal{M} such that $S(X|M) = a$ and $S(Y|M) = b$. Let us assume that X and Y are conditionally independent given M , i.e., for any $m \in \mathcal{M}$, X and Y are independent if conditioned on $M = m$ (if \mathcal{M} is trivial, the conditional independence reduces to the standard independence). What is the minimum value of $S(X + Y|M)$? The conditional Entropy Power Inequality [10, 11] states that this minimum is achieved when, for any $m \in \mathcal{M}$,

X and Y conditioned on $M = m$ have a Gaussian probability distribution with proportional covariance matrices, and the proportionality constant does not depend on m . The inequality is identical to the Entropy Power Inequality (2) with the entropies replaced by the conditional entropies:

$$\exp \frac{2S(X + Y|M)}{n} \geq \exp \frac{2S(X|M)}{n} + \exp \frac{2S(Y|M)}{n}. \quad (5)$$

The conditional Entropy Power Inequality is a key tool in information theory. Its main application is in the field of distributed source coding [10], which is a fundamental problem of network information theory concerning the compression of multiple correlated information sources that do not communicate with each other. In this field, the conditional Entropy Power Inequality is necessary to prove the converse theorems for the quadratic Gaussian CEO problem with two terminals [10, 12, 13] and for the Gaussian multi-terminal source coding problem with two sources [10, 14]. In the quadratic Gaussian CEO problem with two terminals there are two encoders, each of which observes a noisy version of the same signal assumed to have a Gaussian distribution. The goal of each encoder is to encode his observation using the minimum number of bits such that the original signal can be recovered from the encodings with a given bound on the average error. In the Gaussian multi-terminal source coding problem with two sources, each encoder observes a perfect copy of a different signal, and the signals observed by the two encoders are correlated.

1.1 Our contribution

We prove the conditional Entropy Power Inequality (5) in the scenario where M is a quantum system, X and Y are conditionally independent given M and $S(X + Y|M)$, $S(X|M)$ and $S(Y|M)$ are the quantum conditional entropies (Theorem 15, see section 2 for the definitions).

A similar result has been proven for the sum of binary random variables [15].

Entropic inequalities with classical conditioning easily follow from the corresponding unconditioned inequalities and from the definition (3) of conditional entropy via Jensen's inequality (see e.g. [11, Appendix A] or [10, Appendix A.5.2]). Since the quantum conditional entropy cannot be defined as in (3) [16], the same method cannot be applied to entropic inequalities with quantum conditioning, whose proof is very challenging.

The Entropy Power Inequality (5) with quantum conditioning complements the conditional Entropy Power Inequality for bosonic quantum systems [11,17] and the conditional Entropy Power Inequality for quantum additive noise channels [18]. In the conditional Entropy Power Inequality for bosonic quantum systems [11,17], the random variables X and Y are replaced by quantum Gaussian systems modeling the electromagnetic radiation and the sum $X+Y$ is replaced by the beam-splitter operation [19,20]. In the conditional Entropy Power Inequality for quantum additive noise channels [18], X is replaced by a quantum Gaussian system and Y is still a random variable representing classical noise added to the quantum state of the radiation.

The Entropy Power Inequality proven in this paper is optimal both with and without quantum conditioning. Indeed, if the quantum system M is trivial and X and Y are independent Gaussian random variables with proportional covariance matrices, equality is achieved in (5). On the contrary, the presence of quantum conditioning is fundamental for the optimality of the Entropy Power Inequalities for quantum Gaussian systems of Refs. [11,17,18]. If the quantum system M is not present, quantum Gaussian states do not achieve equality, hence the corresponding unconditioned inequalities are not optimal [21–26]. The optimal inequality that would be saturated by quantum Gaussian states is the longstanding conjecture open since 2007 called Entropy Photon-number Inequality [27], which has so far been proven only in some particular cases [28–35] (see [36,37] for a review). The unconditional Entropy Power Inequality has been explored also for other quantum systems and operations, e.g. the partial swap for qudits [38].

Both in the classical and in the quantum scenarios, the prominent proofs of Entropy Power Inequalities are based on perturbation with the heat semigroup and on some version of the Stam inequality for the Fisher information [3,11,17,18,21,23,24,35]. In this paper we follow the same approach: our proof of the Entropy Power Inequality with quantum conditioning is based on the perturbation with the quantum version of the heat semigroup and on a new Stam inequality for the Fisher information with quantum conditioning (Theorem 12). Other approaches to prove quantum entropic inequalities are majorization theory [28,36,38,39] and Lagrange multipliers [30,32].

The paper is structured as follows. In section 2 we define the conditional entropy and the conditional independence of random variables conditioned on a quantum system. In section 3 we prove the Stam inequality with quantum conditioning (Theorem 12), and in section 4 we prove the Entropy Power Inequality with quantum conditioning (Theorem 15). We conclude in sec-

tion 5.

2 Random variables correlated with a quantum system

2.1 Conditional entropy

A state [40, 41] of the quantum system M is a positive linear operator with unit trace on the Hilbert space associated with M . The von Neumann entropy [40, 41] of the quantum system M in the state ρ is

$$S(M) = -\text{Tr}[\rho \ln \rho] . \quad (6)$$

A classical-quantum state of the classical random variable X with values in \mathbb{R}^n and of the quantum system M is given by a probability density function $p(x)$ for X and a collection of quantum states $\{\rho(x)\}_{x \in \mathbb{R}^n}$ on M , where for any $x \in \mathbb{R}^n$, $\rho(x)$ is the quantum state of M conditioned on $X = x$. In analogy with (3), we define the von Neumann entropy of M conditioned on X as [42, Section III.A.3], [43], [44, Chapter 4.6-4.7]

$$S(M|X) = \int_{\mathbb{R}^n} S(M|X = x) p(x) dx , \quad (7)$$

where for any $x \in \mathbb{R}^n$

$$S(M|X = x) = S(\rho(x)) \quad (8)$$

is the von Neumann entropy of M conditioned on $X = x$. When M is a quantum system, conditioning on the values of M does not have a well-defined meaning [16], hence $S(X|M)$ cannot be defined as in (3).

When M is a classical random variable, the chain rule for the entropy implies

$$S(X|M) = S(M|X) + S(X) - S(M) . \quad (9)$$

Here

$$S(M) = - \sum_{m \in \mathcal{M}} q(m) \ln q(m) \quad (10)$$

is the Shannon entropy [1] of M , where for any $m \in \mathcal{M}$, $q(m)$ is the probability that $M = m$, and $S(M|X)$ is defined by (7) with

$$S(M|X = x) = - \sum_{m \in \mathcal{M}} q(m|x) \ln q(m|x) , \quad (11)$$

where $q(m|x)$ is the probability that $M = m$ conditioned on $X = x$.

All the entropies on the right-hand side of (9) are still well-defined when M is a quantum system, provided they are all finite. We recall that

$$S(M) = S(\rho) , \quad (12)$$

where

$$\rho = \int_{\mathbb{R}^n} \rho(x) p(x) dx \quad (13)$$

is the average state of M . Therefore, we take (9) as definition of the von Neumann entropy of X conditioned on the quantum system M [42, Section III.A.3], [43], [44, Chapter 4.6-4.7].

2.2 Conditional independence

Since conditioning on the values of a quantum system does not have a well-defined meaning, we cannot apply to a quantum conditioning the classical definition of conditional independence. The random variables X and Y are conditionally independent given the random variable M iff the mutual information between X and Y conditioned on M

$$I(X : Y|M) = S(X|M) + S(Y|M) - S(XY|M) \quad (14)$$

vanishes [1]. The right-hand side of (14) is well-defined also when M is a quantum system, hence we take (14) as the definition of the mutual information conditioned on a quantum system [40, 41], and we say that X and Y are conditionally independent given the quantum system M iff

$$I(X : Y|M) = 0 . \quad (15)$$

A characterization theorem for the quantum states of a tripartite finite-dimensional quantum system with vanishing quantum conditional mutual information has been proven in [45]. In particular, the theorem can be applied to a tripartite finite-dimensional classical-classical-quantum system:

Theorem 1. *Let X and Y be classical random variables with values in the finite sets \mathcal{X} and \mathcal{Y} , respectively, and let M be a finite-dimensional quantum system with Hilbert space \mathcal{H} . Let us consider a classical-classical-quantum state on XYM such that X and Y are conditionally independent given M , i.e.,*

$$I(X : Y|M) = 0 . \quad (16)$$

Then, for any $x \in \mathcal{X}$ and any $y \in \mathcal{Y}$ the quantum state $\rho(x, y)$ of M conditioned on $X = x$ and $Y = y$ has the form

$$\rho(x, y) = \bigoplus_{i=1}^N r(i) p(x|i) p(y|i) \rho_i^X(x) \otimes \rho_i^Y(y) \Big/ p(x, y) . \quad (17)$$

Here $r(i)$ is a probability distribution on $\{1, \dots, N\}$ and for any $i = 1, \dots, N$, $p(x|i)$ and $p(y|i)$ are probability distributions on \mathcal{X} and \mathcal{Y} , respectively, such that for any $x \in \mathcal{X}$ and any $y \in \mathcal{Y}$

$$i \sum_{i=1}^N r(i) p(x|i) p(y|i) = p(x, y) , \quad (18)$$

where $p(x, y)$ is the probability that $X = x$ and $Y = y$. Moreover, for any $i = 1, \dots, N$, any $x \in \mathcal{X}$ and any $y \in \mathcal{Y}$, $\rho_i^X(x)$ and $\rho_i^Y(y)$ are quantum states on the Hilbert spaces \mathcal{H}_i^X and \mathcal{H}_i^Y , respectively, such that

$$\mathcal{H} = \bigoplus_{i=1}^N \mathcal{H}_i^X \otimes \mathcal{H}_i^Y . \quad (19)$$

Formally Theorem 1 has not been proven yet in the setup of this paper, where the classical random variables X and Y take continuous values. In this case any classical-classical-quantum state of the form (17) satisfies $I(X : Y|M) = 0$, but it is not known whether any state with $I(X : Y|M) = 0$ has the form (17).

Remark 2. A particularly simple and interesting class of classical-classical-quantum states with vanishing conditional mutual information is the case $N = 1$ in Theorem 1, where the quantum state of M conditioned on $X = x$ and $Y = y$ is

$$\rho(x, y) = \rho_X(x) \otimes \rho_Y(y) , \quad (20)$$

and $\rho_X(x)$ and $\rho_Y(y)$ are quantum states on the Hilbert spaces \mathcal{H}_X and \mathcal{H}_Y , respectively, such that

$$\mathcal{H} = \mathcal{H}_X \otimes \mathcal{H}_Y . \quad (21)$$

3 The de Bruijn identity and the Stam inequality with quantum conditioning

Our proof of the Entropy Power Inequality with quantum conditioning is based on the perturbation with the heat semigroup. Let X be a random

variable with values in \mathbb{R}^n and probability density function $p(x)$. The probability density function $p(x, t)$ of X evolved for time $t \geq 0$ with the heat semigroup is the solution to the heat equation

$$\frac{\partial}{\partial t} p(x, t) = \nabla^2 p(x, t), \quad p(x, 0) = p(x). \quad (22)$$

The fundamental property of the heat semigroup states that $p(x, t)$ coincides with the probability density function of the random variable $X + \sqrt{t} Z$, where Z is a normal Gaussian random variable with values in \mathbb{R}^n independent of X . In the following, we will employ this representation of the heat semigroup. The semigroup property implies

Lemma 3 (semigroup property). *Let X be a random variable with values in \mathbb{R}^n , and let Z_1, Z_2 and Z be normal Gaussian random variables with values in \mathbb{R}^n such that X, Z_1, Z_2 and Z are all independent. Then, for any $t_1, t_2 \geq 0$, $X + \sqrt{t_1} Z_1 + \sqrt{t_2} Z_2$ has the same probability distribution as $X + \sqrt{t_1 + t_2} Z$.*

Definition 4 (Fisher information with quantum conditioning [18, Definition 8]). Let X be a random variable on \mathbb{R}^n correlated with the quantum system M such that $\|X\|^2$ has finite average and the function $x \mapsto \rho(x)$ is continuous in the trace norm, where for any $x \in \mathbb{R}^n$, $\rho(x)$ is the quantum state of M conditioned on $X = x$. The Fisher information of X conditioned on M is

$$J(X|M) = \lim_{t \rightarrow 0^+} \frac{I(X + \sqrt{t} Z : Z | M)}{t}, \quad (23)$$

where Z is a normal Gaussian random variable on \mathbb{R}^n independent on both X and M .

Remark 5. The conditional mutual information in (23) is computed on the classical-classical-quantum state of $X' = X + \sqrt{t} Z$, Z and M . This state is determined by the joint probability density of X' and Z and by the collection of quantum states $\{\rho'(x', z)\}_{x', z \in \mathbb{R}^n}$ of M conditioned on $X' = x'$ and $Z = z$. We recall that

$$\rho'(x', z) = \rho(x' - \sqrt{t} z), \quad (24)$$

where for any $x \in \mathbb{R}^n$, $\rho(x)$ is the quantum state of M conditioned on $X = x$.

Remark 6. The limit (23) always exists, finite or infinite, from Lemma 7 below.

Lemma 7 ([18, Theorem 2]). *The function*

$$t \mapsto I \left(X + \sqrt{t} Z : Z \middle| M \right) = S \left(X + \sqrt{t} Z \middle| M \right) - S(X|M) \quad (25)$$

is concave for any $t \geq 0$.

Remark 8. If the quantum system M is trivial, the Fisher information with quantum conditioning coincides with the trace of the Fisher information matrix

$$J_{ij}(X) = \int_{\mathbb{R}^n} \frac{\partial \ln p(x)}{\partial x^i} \frac{\partial \ln p(x)}{\partial x^j} p(x) dx, \quad i, j = 1, \dots, n, \quad (26)$$

where p is the probability density function of X .

The de Bruijn identity provides the link between the Fisher information and the growth rate of the entropy under the heat semigroup.

Proposition 9 (de Bruijn identity with quantum conditioning [18, Proposition 1]). *Let X be a random variable on \mathbb{R}^n correlated with the quantum system M such that $\|X\|^2$ has finite average and the function $x \mapsto \rho(x)$ is continuous in the trace norm, where for any $x \in \mathbb{R}^n$, $\rho(x)$ is the quantum state of M conditioned on $X = x$. Then,*

$$J(X|M) = \left. \frac{d}{dt} S \left(X + \sqrt{t} Z \middle| M \right) \right|_{t=0}, \quad (27)$$

where Z is a normal Gaussian random variable on \mathbb{R}^n independent on both X and M .

Remark 10. If the quantum system M is trivial, the de Bruijn identity with quantum conditioning (27) becomes the de Bruijn identity

$$J(X) = \left. \frac{d}{dt} S \left(X + \sqrt{t} Z \right) \right|_{t=0} \quad (28)$$

exploited in the proof of the Entropy Power Inequality (2) of Ref. [3].

Corollary 11. *Let X be a random variable on \mathbb{R}^n correlated with the quantum system M such that $\|X\|^2$ has finite average and the function $x \mapsto \rho(x)$ is continuous in the trace norm, where for any $x \in \mathbb{R}^n$, $\rho(x)$ is the quantum state of M conditioned on $X = x$. Let Z be a normal Gaussian random variable on \mathbb{R}^n independent on both X and M . Then, for any $t \geq 0$*

$$\frac{d}{dt} S \left(X + \sqrt{t} Z \middle| M \right) = J \left(X + \sqrt{t} Z \middle| M \right), \quad (29)$$

Proof. We have

$$\begin{aligned}
\frac{d}{dt} S \left(X + \sqrt{t} Z \middle| M \right) &= \frac{d}{ds} S \left(X + \sqrt{t+s} Z \middle| M \right) \Big|_{s=0} \\
&= \frac{d}{ds} S \left(X + \sqrt{t} Z_1 + \sqrt{s} Z_2 \middle| M \right) \Big|_{s=0} \\
&= J \left(X + \sqrt{t} Z_1 \middle| M \right) , \tag{30}
\end{aligned}$$

where Z_1 and Z_2 are independent normal Gaussian random variables uncorrelated from X , Z and M , the second equality follows from Lemma 3 and the last equality follows from Proposition 9. \square

Theorem 12 (Stam inequality with quantum conditioning). *Let X and Y be random variables with values in \mathbb{R}^n correlated with the quantum system M such that $\|X\|^2$ and $\|Y\|^2$ have finite average and the function $(x, y) \mapsto \rho(x, y)$ is continuous in the trace norm, where for any $x, y \in \mathbb{R}^n$, $\rho(x, y)$ is the quantum state of M conditioned on $X = x$ and $Y = y$. Let us assume that X and Y are conditionally independent given M , i.e.,*

$$I(X : Y | M) = 0 . \tag{31}$$

Then, for any $0 \leq \lambda \leq 1$ the following linear Stam inequality holds:

$$J(X + Y | M) \leq \lambda^2 J(X | M) + (1 - \lambda)^2 J(Y | M) . \tag{32}$$

Choosing

$$\lambda = \frac{J(Y | M)}{J(X | M) + J(Y | M)} , \tag{33}$$

(32) becomes the Stam inequality

$$\frac{1}{J(X + Y | M)} \geq \frac{1}{J(X | M)} + \frac{1}{J(Y | M)} . \tag{34}$$

Proof. We have

$$\begin{aligned}
& I\left(X + Y + \sqrt{t}Z : Z \middle| M\right) \stackrel{(a)}{\leq} I\left(X + \lambda\sqrt{t}Z, Y + (1 - \lambda)\sqrt{t}Z : Z \middle| M\right) \\
& \stackrel{(b)}{=} I\left(X + \lambda\sqrt{t}Z : Z \middle| M\right) + I\left(Y + (1 - \lambda)\sqrt{t}Z : Z \middle| M\right) \\
& + I\left(X + \lambda\sqrt{t}Z : Y + (1 - \lambda)\sqrt{t}Z \middle| MZ\right) \\
& - I\left(X + \lambda\sqrt{t}Z : Y + (1 - \lambda)\sqrt{t}Z \middle| M\right) \\
& \stackrel{(c)}{\leq} I\left(X + \lambda\sqrt{t}Z : Z \middle| M\right) + I\left(Y + (1 - \lambda)\sqrt{t}Z : Z \middle| M\right) \\
& + I\left(X + \lambda\sqrt{t}Z : Y + (1 - \lambda)\sqrt{t}Z \middle| MZ\right) \\
& \stackrel{(d)}{=} I\left(X + \lambda\sqrt{t}Z : Z \middle| M\right) + I\left(Y + (1 - \lambda)\sqrt{t}Z : Z \middle| M\right). \tag{35}
\end{aligned}$$

(a) and (b) follow from the data-processing inequality and the chain rule for the quantum conditional mutual information, respectively; (c) follows from the positivity of the quantum conditional mutual information; (d) follows from (31) since

$$\begin{aligned}
I\left(X + \lambda\sqrt{t}Z : Y + (1 - \lambda)\sqrt{t}Z \middle| MZ\right) &= I(X : Y | MZ) \\
&= I(X : Y | M) = 0. \tag{36}
\end{aligned}$$

Since Z is uncorrelated from X , Y and M , we have

$$I(X + Y : Z | M) = I(X : Z | M) = I(Y : Z | M) = 0, \tag{37}$$

hence both members of (35) vanish for $t = 0$. The claim (32) then follows taking the derivative with respect to t of both members of (35) at $t = 0$. \square

Remark 13. If the quantum system M is trivial, the Stam inequality with quantum conditioning (34) becomes the Stam inequality

$$\frac{1}{J(X + Y)} \geq \frac{1}{J(X)} + \frac{1}{J(Y)} \tag{38}$$

on which the proof of the Entropy Power Inequality (2) of Ref. [3] is based.

In the proof of the Entropy Power Inequality we also need the asymptotic scaling of the entropy under the heat semigroup evolution.

Theorem 14 (asymptotic scaling of entropy with quantum conditioning [18, Theorem 4]). *Let X be a random variable with values in \mathbb{R}^n correlated with the quantum system M such that X and M both have finite entropy. Then,*

$$\lim_{t \rightarrow \infty} \left(S \left(X + \sqrt{t} Z \middle| M \right) - n \frac{\ln t + 1}{2} \right) = 0, \quad (39)$$

where Z is a normal Gaussian random variable on \mathbb{R}^n independent on both X and M .

4 The Entropy Power Inequality with quantum conditioning

Theorem 15 (Entropy Power Inequality with quantum conditioning). *Let X and Y be random variables with values in \mathbb{R}^n correlated with the quantum system M such that $\|X\|^2$ and $\|Y\|^2$ have finite average and the function $(x, y) \mapsto \rho(x, y)$ is continuous in the trace norm, where for any $x, y \in \mathbb{R}^n$, $\rho(x, y)$ is the quantum state of M conditioned on $X = x$ and $Y = y$. Let us assume that X and Y are conditionally independent given M , i.e.,*

$$I(X : Y | M) = 0. \quad (40)$$

Then, the following Entropy Power Inequality holds:

$$\exp \frac{2S(X + Y | M)}{n} \geq \exp \frac{2S(X | M)}{n} + \exp \frac{2S(Y | M)}{n}. \quad (41)$$

Proof. We will prove the following linear Entropy Power Inequality for any $0 \leq \lambda \leq 1$:

$$S(X + Y | M) \geq \lambda S(X | M) + (1 - \lambda) S(Y | M) - n \frac{\lambda \ln \lambda + (1 - \lambda) \ln (1 - \lambda)}{2}. \quad (42)$$

The Entropy Power Inequality (41) follows choosing

$$\lambda = \frac{\exp \frac{2S(X | M)}{n}}{\exp \frac{2S(X | M)}{n} + \exp \frac{2S(Y | M)}{n}} \quad (43)$$

in (42).

Let Z_1 , Z_2 and Z be independent normal Gaussian random variables on \mathbb{R}^n uncorrelated from both X and M . We define for any $t \geq 0$

$$\begin{aligned} \phi(t) &= S\left(X + Y + \sqrt{t}Z \middle| M\right) \\ &\quad - \lambda S\left(X + \sqrt{\lambda t}Z_1 \middle| M\right) - (1 - \lambda) S\left(Y + \sqrt{(1 - \lambda)t}Z_2 \middle| M\right). \end{aligned} \quad (44)$$

We have from Corollary 11

$$\begin{aligned} \phi'(t) &= J\left(X + Y + \sqrt{t}Z \middle| M\right) \\ &\quad - \lambda^2 J\left(X + \sqrt{\lambda t}Z_1 \middle| M\right) - (1 - \lambda)^2 J\left(Y + \sqrt{(1 - \lambda)t}Z_2 \middle| M\right). \end{aligned} \quad (45)$$

From (40), $X + \sqrt{\lambda t}Z_1$ and $Y + \sqrt{(1 - \lambda)t}Z_2$ are conditionally independent given M since from the data-processing inequality for the quantum conditional mutual information we have

$$I\left(X + \sqrt{\lambda t}Z_1 : Y + \sqrt{(1 - \lambda)t}Z_2 \middle| M\right) \leq I(X : Y | M) = 0. \quad (46)$$

Theorem 12 with the replacements $X \mapsto X + \sqrt{\lambda t}Z_1$ and $Y \mapsto Y + \sqrt{(1 - \lambda)t}Z_2$ implies

$$\begin{aligned} &J\left(X + \sqrt{\lambda t}Z_1 + Y + \sqrt{(1 - \lambda)t}Z_2 \middle| M\right) \\ &\leq \lambda^2 J\left(X + \sqrt{\lambda t}Z_1 \middle| M\right) + (1 - \lambda)^2 J\left(Y + \sqrt{(1 - \lambda)t}Z_2 \middle| M\right). \end{aligned} \quad (47)$$

We have from Lemma 3

$$J\left(X + \sqrt{\lambda t}Z_1 + Y + \sqrt{(1 - \lambda)t}Z_2 \middle| M\right) = J\left(X + Y + \sqrt{t}Z \middle| M\right), \quad (48)$$

hence (45) and (47) imply

$$\phi'(t) \leq 0. \quad (49)$$

We have from Lemma 3 again

$$S\left(X + \sqrt{\lambda t}Z_1 + Y + \sqrt{(1 - \lambda)t}Z_2 \middle| M\right) = S\left(X + Y + \sqrt{t}Z \middle| M\right). \quad (50)$$

Then, from Lemma 7, $\phi(t)$ is a linear combination of concave functions, hence from (49)

$$\phi(t) = \phi(0) + \int_0^t \phi'(s) ds \leq \phi(0) . \quad (51)$$

Hence, we have from Theorem 14

$$\phi(0) \geq \limsup_{t \rightarrow \infty} \phi(t) = -n \frac{\lambda \ln \lambda + (1 - \lambda) \ln (1 - \lambda)}{2} , \quad (52)$$

and the claim (42) follows. \square

5 Conclusions

We have proven the Entropy Power Inequality with quantum conditioning (Theorem 15). This inequality complements the Entropy Power Inequality with classical conditioning [10], the conditional Entropy Power Inequality for bosonic quantum systems [11] and the conditional Entropy Power Inequality for quantum additive-noise channels. The Entropy Power Inequality with classical conditioning was necessary in the field of distributed source coding to prove the converse theorems for the quadratic Gaussian CEO problem with two terminals [10, 12, 13] and for the Gaussian multi-terminal source coding problem with two sources [10, 14]. In the same way, the Entropy Power Inequality with quantum conditioning proven in this paper can be useful to prove the converse theorems for the quantum versions of the same problems, where the encoders can exploit a shared entangled quantum state. The hypothesis of conditional independence is not a limitation to the applicability of the Entropy Power Inequality with quantum conditioning, since the same hypothesis is necessary for the Entropy Power Inequality with classical conditioning and fulfilled in all its applications.

Acknowledgements

GdP acknowledges financial support from the European Research Council (ERC Grant Agreements Nos. 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).

 This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 792557.

References

- [1] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. A Wiley-Interscience publication. Wiley, 2006.
- [2] Amir Dembo, Thomas M Cover, and Joy Thomas. Information theoretic inequalities. *Information Theory, IEEE Transactions on*, 37(6):1501–1518, 1991.
- [3] Adriaan J. Stam. Some inequalities satisfied by the quantities of information of fisher and shannon. *Information and Control*, 2(2):101–112, 1959.
- [4] Claude Elwood Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1):3–55, 2001.
- [5] Patrick P Bergmans. A simple converse for broadcast channels with additive white gaussian noise (corresp.). *Information Theory, IEEE Transactions on*, 20(2):279–280, 1974.
- [6] Sik K Leung-Yan-Cheong and Martin E Hellman. The gaussian wire-tap channel. *Information Theory, IEEE Transactions on*, 24(4):451–456, 1978.
- [7] Andrew R Barron. Entropy and the central limit theorem. *The Annals of probability*, pages 336–342, 1986.
- [8] Sergey G Bobkov and Arnaud Marsiglietti. Variants of the entropy power inequality. *IEEE Transactions on Information Theory*, 63(12):7747–7752, 2017.
- [9] Stanislaw J Szarek and Dan Voiculescu. Volumes of restricted minkowski sums and the free analogue of the entropy power inequality. *Communications in Mathematical Physics*, 178(3):563–570, 1996.

- [10] Shuang Wang, Yong Fang, and Samuel Cheng. *Distributed Source Coding: Theory and Practice*. Wiley, 2017.
- [11] Giacomo De Palma and Dario Trevisan. The conditional entropy power inequality for bosonic quantum systems. *Communications in Mathematical Physics*, 360(2):639–662, Jun 2018.
- [12] Yasutada Oohama. Rate-distortion theory for gaussian multiterminal source coding systems with several side informations at the decoder. *IEEE Transactions on Information Theory*, 51(7):2577–2593, 2005.
- [13] Vinod Prabhakaran, David Tse, and Kannan Ramachandran. Rate region of the quadratic gaussian ceo problem. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, page 119. IEEE, 2004.
- [14] Abbas El Gamal and Young-Hani Kim. *Network Information Theory*. Cambridge University Press, 2011.
- [15] Christoph Hirche and David Reeb. Bounds on information combining with quantum side information. *IEEE Transactions on Information Theory*, 2018.
- [16] Salman Beigi and Amin Gohari. On dimension bounds for auxiliary quantum systems. *IEEE Trans. Information Theory*, 60(1):368–387, 2014.
- [17] Robert König. The conditional entropy power inequality for gaussian quantum states. *Journal of Mathematical Physics*, 56(2):022201, 2015.
- [18] Giacomo De Palma and Stefan Huber. The conditional entropy power inequality for quantum additive noise channels. *Journal of Mathematical Physics*, 59(12):122201, 2018.
- [19] Christian Weedbrook, Stefano Pirandola, Raul Garcia-Patron, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621, 2012.
- [20] Alessio Serafini. *Quantum Continuous Variables: A Primer of Theoretical Methods*. CRC Press, 2017.

- [21] Robert König and Graeme Smith. The entropy power inequality for quantum systems. *IEEE Transactions on Information Theory*, 60(3):1536–1548, 2014.
- [22] Robert König and Graeme Smith. Corrections to “the entropy power inequality for quantum systems”. *IEEE Transactions on Information Theory*, 62(7):4358–4359, 2016.
- [23] Giacomo De Palma, Andrea Mari, and Vittorio Giovannetti. A generalization of the entropy power inequality to bosonic quantum systems. *Nature Photonics*, 8(12):958–964, 2014.
- [24] Giacomo De Palma, Andrea Mari, Seth Lloyd, and Vittorio Giovannetti. Multimode quantum entropy power inequality. *Physical Review A*, 91(3):032320, 2015.
- [25] Giacomo De Palma. *Gaussian optimizers and other topics in quantum information*. PhD thesis, Scuola Normale Superiore, Pisa (Italy), September 2016. Supervisor: Prof. Vittorio Giovannetti; arXiv:1710.09395.
- [26] Stefan Huber, Robert König, and Anna Vershynina. Geometric inequalities from phase space translations. *Journal of Mathematical Physics*, 58(1):012206, 2017.
- [27] Saikat Guha, Baris Erkmen, and Jeffrey H Shapiro. The entropy photon-number inequality and its consequences. In *Information Theory and Applications Workshop, 2008*, pages 128–130. IEEE, 2008.
- [28] Giacomo De Palma, Dario Trevisan, and Vittorio Giovannetti. Passive states optimize the output of bosonic gaussian quantum channels. *IEEE Transactions on Information Theory*, 62(5):2895–2906, May 2016.
- [29] Giacomo De Palma, Andrea Mari, Seth Lloyd, and Vittorio Giovannetti. Passive states as optimal inputs for single-jump lossy quantum channels. *Physical Review A*, 93(6):062328, 2016.
- [30] Giacomo De Palma, Dario Trevisan, and Vittorio Giovannetti. Gaussian states minimize the output entropy of the one-mode quantum attenuator. *IEEE Transactions on Information Theory*, 63(1):728–737, 2017.

- [31] Haoyu Qi, Mark M Wilde, and Saikat Guha. On the minimum output entropy of single-mode phase-insensitive gaussian channels. *arXiv preprint arXiv:1607.05262*, 2017.
- [32] Giacomo De Palma, Dario Trevisan, and Vittorio Giovannetti. The one-mode quantum-limited gaussian attenuator and amplifier have gaussian maximizers. *Annales Henri Poincaré*, 19(10):2919–2953, Oct 2018.
- [33] Giacomo De Palma, Dario Trevisan, and Vittorio Giovannetti. Gaussian states minimize the output entropy of one-mode quantum gaussian channels. *Physical Review Letters*, 118:160503, Apr 2017.
- [34] Giacomo De Palma, Dario Trevisan, and Vittorio Giovannetti. Multi-mode gaussian optimizers for the wehrl entropy and quantum gaussian channels. *arXiv preprint arXiv:1705.00499*, 2017.
- [35] Giacomo De Palma. New lower bounds to the output entropy of multi-mode quantum gaussian channels. *Submitted to IEEE Transactions on Information Theory, preprint arXiv:1805.12469*, 2018.
- [36] Alexander Semenovich Holevo. Gaussian optimizers and the additivity problem in quantum information theory. *Russian Mathematical Surveys*, 70(2):331, 2015.
- [37] Giacomo De Palma, Dario Trevisan, Vittorio Giovannetti, and Luigi Ambrosio. Gaussian optimizers for entropic inequalities in quantum information. *Journal of Mathematical Physics*, 59(8):081101, 2018.
- [38] Koenraad Audenaert, Nilanjana Datta, and Maris Ozols. Entropy power inequalities for qudits. *Journal of Mathematical Physics*, 57(5):052202, 2016.
- [39] V Giovannetti, AS Holevo, and Raúl García-Patrón. A solution of gaussian optimizer conjecture for quantum channels. *Communications in Mathematical Physics*, 334(3):1553–1571, 2015.
- [40] Alexander Semenovich Holevo. *Quantum Systems, Channels, Information: A Mathematical Introduction*. De Gruyter Studies in Mathematical Physics. De Gruyter, 2013.

- [41] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2017.
- [42] Fabian Furrer, Mario Berta, Marco Tomamichel, Volkher B Scholz, and Matthias Christandl. Position-momentum uncertainty relations in the presence of quantum memory. *Journal of Mathematical Physics*, 55(12):122205, 2014.
- [43] Gerard J. Murphy. Chapter 6 - direct limits and tensor products. In Gerard J. Murphy, editor, *C*Algebras and Operator Theory*, pages 173 – 216. Academic Press, San Diego, 1990.
- [44] Masamichi Takesaki. *Theory of Operator Algebras I*. Encyclopaedia of mathematical sciences. Springer New York, 2012.
- [45] Patrick Hayden, Richard Jozsa, Denes Petz, and Andreas Winter. Structure of states which satisfy strong subadditivity of quantum entropy with equality. *Communications in mathematical physics*, 246(2):359–374, 2004.