Gaussian states minimize the output entropy of one-mode quantum Gaussian channels

Giacomo De Palma,[1] Dario Trevisan,[2] and Vittorio Giovannetti[3]

[1] *QMATH, Department of Mathematical Sciences, University of Copenhagen, Denmark*
[2] *Università degli Studi di Pisa, Pisa, Italy*
[3] *NEST, Scuola Normale Superiore and Istituto Nanoscienze-CNR, Pisa, Italy*

We prove the longstanding conjecture stating that Gaussian thermal input states minimize the output von Neumann entropy of one-mode phase-covariant quantum Gaussian channels among all the input states with a given entropy. Phase-covariant quantum Gaussian channels model the attenuation and the noise that affect any electromagnetic signal in the quantum regime. Our result is crucial to prove the converse theorems for both the triple trade-off region and the capacity region for broadcast communication of the Gaussian quantum-limited amplifier. Our result extends to the quantum regime the Entropy Power Inequality that plays a key role in classical information theory. Our proof exploits a completely new technique based on the recent determination of the $p \to q$ norms of the quantum-limited amplifier [De Palma et al., arXiv:1610.09967]. This technique can be applied to any quantum channel.

Based on arXiv:1610.09970.

Signal attenuation and noise unavoidably affect electromagnetic communications through metal wires, optical fibers or free space. Since the energy carried by an electromagnetic pulse is quantized, quantum effects must be taken into account [1]. They become relevant for low-intensity signals, such as for satellite communications, where the receiver can be reached by only few photons for each bit of information [2]. In the quantum regime, signal attenuation and noise are modeled by phase-covariant quantum Gaussian channels [3–7].

The maximum achievable communication rate of a channel depends on the minimum noise achievable at its output, that is quantified by the output von Neumann entropy [5, 8]. We prove in the case of one mode the longstanding constrained minimum output entropy (CMOE) conjecture [9–14] stating that Gaussian thermal input states minimize the output entropy of phase-covariant quantum Gaussian channels among all the input states with a given entropy.

The classical counterpart of the CMOE conjecture states that Gaussian input probability distributions minimize the output Shannon differential entropy of classical Gaussian channels among all the input probability distributions with a given entropy, and it is implied by the Entropy Power Inequality (EPI) [15, 16]. The EPI is fundamental in classical information theory. It is necessary to prove the optimality of Gaussian encodings for the transmission of information through the classical broadcast and wiretap channels [17, 18], and it provides bounds for the information capacities of non-Gaussian classical communication channels [19] and for the convergence rate in the Central Limit Theorem [20]. A quantum generalization of the proof of the EPI permits to prove the quantum EPI (qEPI) [21–25], that provides a lower bound to the output von Neumann entropy of quantum Gaussian channels in terms of the input entropy. However, the qEPI is *not* saturated by quantum Gaussian states, hence it is not sufficient to prove the CMOE conjecture. The MOE conjecture has first been proven in a completely different way in the version stating that pure Gaussian input states minimize the output entropy of any phase covariant and contravariant quantum Gaussian channel among all the possible pure and mixed input states [7, 26–29]. This fundamental result has permitted to determine the classical communication capacity of these channels [30] and to prove that this capacity is additive under tensor product, i.e. it is not increased by entangling the inputs [7]. The CMOE conjecture has then been proven for the one-mode quantum-limited attenuator [31, 32] using Lagrange multipliers. Unfortunately the same proof does not work in the presence of amplification or noise.

We prove the CMOE conjecture for any one-mode phase-covariant quantum Gaussian channel. This result implies the CMOE conjecture also for one-mode phase-contravariant quantum Gaussian channels ([33], Section VI). Our result both extends the EPI to the quantum regime and generalizes the unconstrained minimum output entropy conjecture of [7, 27–30]. Our result is necessary to prove the converse theorems that guarantee the optimality of Gaussian encodings for two communication tasks involving the quantum-limited amplifier [34]. The first is the triple trade-off coding [35], that allows to simultaneously transmit both classical and quantum information and to generate shared entanglement, or to simultaneously transmit both public and private classical information and to generate a shared secret key. The second is broadcast communication [36, 37], i.e. classical communication with two receivers.

Our proof exploits a completely new technique that links the CMOE conjecture to the $p \to q$ norms [7, 38], and is based on the result stating that Gaussian thermal input states saturate the $p \to q$ norms of the one-mode quantum-limited amplifier [39]. This technique can be used to determine the minimum output entropy for fixed input entropy for any quantum channel whose $p \to q$ norms are known.

[1] J. P. Gordon, Proceedings of the IRE **50**, 1898 (1962).
[2] J. Chen, J. L. Habif, Z. Dutton, R. Lazarus, and S. Guha, Nature Photonics **6**, 374 (2012).
[3] V. W. Chan, Lightwave Technology, Journal of **24**, 4750 (2006).
[4] S. L. Braunstein and P. Van Loock, Reviews of Modern Physics **77**, 513 (2005).
[5] A. S. Holevo, *Quantum Systems, Channels, Information: A Mathematical Introduction*, De Gruyter Studies in Mathematical Physics (De Gruyter, 2013).
[6] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Reviews of Modern Physics **84**, 621 (2012).
[7] A. S. Holevo, Uspekhi Matematicheskikh Nauk **70**, 141 (2015).
[8] M. Wilde, *Quantum Information Theory* (Cambridge University Press, 2013).
[9] S. Guha and J. H. Shapiro, in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on* (IEEE, 2007) pp. 1896–1900.
[10] S. Guha, J. H. Shapiro, and B. I. Erkmen, Physical Review A **76**, 032303 (2007).
[11] S. Guha, B. Erkmen, and J. H. Shapiro, in *Information Theory and Applications Workshop, 2008* (IEEE, 2008) pp. 128–130.
[12] S. Guha, J. H. Shapiro, and B. Erkmen, in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on* (IEEE, 2008) pp. 91–95.
[13] M. M. Wilde, P. Hayden, and S. Guha, Physical Review Letters **108**, 140501 (2012).
[14] M. M. Wilde, P. Hayden, and S. Guha, Physical Review A **86**, 062306 (2012).
[15] T. Cover and J. Thomas, *Elements of Information Theory*, A Wiley-Interscience publication (Wiley, 2006).
[16] N. M. Blachman, Information Theory, IEEE Transactions on **11**, 267 (1965).
[17] P. P. Bergmans, Information Theory, IEEE Transactions on **20**, 279 (1974).
[18] S. K. Leung-Yan-Cheong and M. E. Hellman, Information Theory, IEEE Transactions on **24**, 451 (1978).
[19] C. E. Shannon, ACM SIGMOBILE Mobile Computing and Communications Review **5**, 3 (2001).
[20] A. R. Barron, The Annals of probability , 336 (1986).
[21] R. König and G. Smith, Physical review letters **110**, 040501 (2013).
[22] R. König and G. Smith, Nature Photonics **7**, 142 (2013).
[23] R. Konig and G. Smith, Information Theory, IEEE Transactions on **60**, 1536 (2014).
[24] G. De Palma, A. Mari, and V. Giovannetti, Nature Photonics **8**, 958 (2014).
[25] G. De Palma, A. Mari, S. Lloyd, and V. Giovannetti, Physical Review A **91**, 032320 (2015).
[26] R. Garcia-Patron, C. Navarrete-Benlloch, S. Lloyd, J. H. Shapiro, and N. J. Cerf, Physical Review Letters **108**, 110505 (2012).
[27] A. Mari, V. Giovannetti, and A. S. Holevo, Nature communications **5** (2014).
[28] V. Giovannetti, A. Holevo, and R. García-Patrón, Communications in Mathematical Physics **334**, 1553 (2015).
[29] V. Giovannetti, A. S. Holevo, and A. Mari, Theoretical and Mathematical Physics **182**, 284 (2015).
[30] V. Giovannetti, R. García-Patrón, N. Cerf, and A. Holevo, Nature Photonics **8**, 796 (2014).
[31] G. De Palma, D. Trevisan, and V. Giovannetti, IEEE Transactions on Information Theory **63**, 728 (2017).
[32] G. De Palma, D. Trevisan, and V. Giovannetti, IEEE Transactions on Information Theory **62**, 2895 (2016).
[33] H. Qi, M. M. Wilde, and S. Guha, arXiv preprint arXiv:1607.05262 (2016).
[34] H. Qi and M. M. Wilde, arXiv preprint arXiv:1605.04922 (2016).
[35] M. M. Wilde and M.-H. Hsieh, Quantum Information Processing **11**, 1465 (2012).
[36] J. Yard, P. Hayden, and I. Devetak, Information Theory, IEEE Transactions on **57**, 7147 (2011).
[37] I. Savov and M. M. Wilde, Information Theory, IEEE Transactions on **61**, 7017 (2015).
[38] A. S. Holevo, Russian Mathematical Surveys **61**, 301 (2006).
[39] G. De Palma, D. Trevisan, and V. Giovannetti, arXiv preprint arXiv:1610.09967 (2016).