



MIT Open Access Articles

No-go theorem for Gaussian quantum error correction

The MIT Faculty has made this article openly available. **Please share** how this access benefits you. Your story matters.

Citation	Niset, Julien, Jaromir Fiurasek and Nicolas J. Cerf. "No-Go Theorem for Gaussian Quantum Error Correction." Phys. Rev. Lett. 102, 120501 (2009) [4 pages] © 2009 The American Physical Society.
As Published	http://dx.doi.org/10.1103/PhysRevLett.102.120501
Publisher	American Physical Society
Version	Final published version
Citable link	http://hdl.handle.net/1721.1/64768
Terms of Use	Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.

No-Go Theorem for Gaussian Quantum Error Correction

Julien Niset,¹ Jaromír Fiurášek,² and Nicolas J. Cerf^{1,3}

¹*QuIC, Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium*

²*Department of Optics, Palacký University, 17. listopadu 50, 77200 Olomouc, Czech Republic*

³*Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

(Received 20 November 2008; published 24 March 2009)

We prove that Gaussian operations are of no use for protecting Gaussian states against Gaussian errors in quantum communication protocols. Specifically, we introduce a new quantity characterizing any single-mode Gaussian channel, called *entanglement degradation*, and show that it cannot decrease via Gaussian encoding and decoding operations only. The strength of this no-go theorem is illustrated with some examples of Gaussian channels.

DOI: 10.1103/PhysRevLett.102.120501

PACS numbers: 03.67.Pp, 42.50.Dv

Quantum information processing based on continuous variables has attracted a lot of attention over recent years due to both its conceptual simplicity and experimental advantages. In particular, the set of Gaussian states and operations have been shown to enable many quantum information primitives, such as teleportation [1], key distribution [2], and cloning [3]. Interestingly, when the quadratures of the electromagnetic field are used to carry information, the entire set of Gaussian operations can be implemented by combining passive linear optical components such as beam splitters and phase shifters together with squeezers and homodyne detection followed by feed-forward. All these elements are, up to some degree, readily accessible in today's optical laboratories. However, manipulating Gaussian states with Gaussian operations also leads to some limitations. Probably the most significant one is the impossibility to distill entanglement from Gaussian entangled states with Gaussian local operations and classical communication [4–6]. As a result, some important quantum primitives, such as quantum repeaters, cannot be implemented within the Gaussian regime and hence require the use of experimentally more demanding non-Gaussian resources, such as photon subtraction [7] or de-Gaussification operations [8]. Given the present state of technology, understanding what is possible or not within the Gaussian regime is thus of great importance as it underpins the “main stream” use of optical continuous variables in quantum information protocols.

Recently, several schemes have been developed to fight noise and losses in continuous-variable quantum transmission lines. Given the well-known connection between quantum error correction and entanglement distillation for discrete-variable quantum systems [9], it was implicitly assumed that correcting Gaussian errors with Gaussian operations would be impossible. Logically, these schemes were thus all focused on non-Gaussian error models, such as discrete errors [10,11], phase-diffusion noise [12], probabilistic phase-space kicks [13], or probabilistic losses [14,15]. However, the sole existence of a no-go theorem for Gaussian error correction had yet remained unresolved.

In this Letter, we address this problem by introducing a new intrinsic feature of single-mode Gaussian channels, which we call *entanglement degradation* D . This parameter characterizes the extent to which the channel degrades entanglement when acting on one-half of two-mode squeezed vacuum at the limit of infinite squeezing. By exploiting a connection between quantum error correction and entanglement distillation in the Gaussian regime, we prove that D can never decrease when one is restricted to Gaussian encoding and decoding operations. Our result is thus of the form of a *no-go theorem*, establishing the impossibility of improving the transmission of Gaussian states in a Gaussian channel with Gaussian error correction only.

Let us briefly remind the Gaussian formalism. Any n -mode Gaussian state is completely characterized by its first and second moments \mathbf{d} and γ , respectively. Introducing the vector of quadratures $\mathbf{r} = (x_1, p_1, \dots, x_n, p_n)$, the coherent vector and covariance matrix read $d_j = \langle r_j \rangle$ and $\gamma_{ij} = \langle r_i r_j + r_j r_i \rangle - 2d_i d_j$. A quantum Gaussian channel is a trace-preserving completely positive map T that transforms Gaussian states into Gaussian states according to $\rho \rightarrow T(\rho)$. It can be understood as resulting from a Gaussian unitary operation U (associated with a quadratic bosonic Hamiltonian) acting on the state ρ together with its environment in a Gaussian state ρ_E , i.e., $T(\rho) = \text{Tr}_E U(\rho \otimes \rho_E) U^\dagger$, where Tr_E denotes partial trace with respect to the environment [16]. Gaussian channels are known to model many physical lines, e.g., the transmission through a lossy optical fiber. At the level of covariance matrices, the action of T is completely characterized by two matrices M and N , namely

$$\gamma \rightarrow M\gamma M^T + N, \quad (1)$$

where M is real and $N \geq 0$ is real and symmetric. In the case of a single-mode channel, the condition of complete positivity of the map implies that

$$\det N \geq (\det M - 1)^2, \quad (2)$$

which means that any map $\gamma \rightarrow M\gamma M^T$ can be approxi-

mately realized provided that sufficient noise N is added. An important subclass of Gaussian operations are symplectic transformations, corresponding to $N = 0$ and $\det M = 1$. Well-known examples of such operations are phase shifters and squeezers, with symplectic matrices

$$M_{\text{PS}} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \quad M_{\text{Sq}} = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^r \end{pmatrix}. \quad (3)$$

Let us now define a Gaussian Error-Correcting Code (GECC) associated with the Gaussian channel T , as depicted in Fig. 1. It consists of a finite number $n - 1$ of ancillas in a vacuum state $|0\rangle$, Gaussian unitary operations for encoding E and decoding D acting each on n modes, and n uses of the channel T . The code is denoted by $G(n, E, D)$, and its overall effect is to turn the Gaussian channel T with matrices M and N into a Gaussian channel T_{GC} with matrices M_{GC} and N_{GC} .

We are now ready to turn to the proof of our no-go theorem, which can be greatly simplified by introducing two Lemmas. For discrete systems, it is well known that any error-correcting code is equivalent to a one-way entanglement distillation protocol, and vice versa [9]. For continuous variables, this relation is not as straightforward, but one can nevertheless prove the following lemma:

Lemma 1.—If $|\phi_r\rangle$ is a two-mode squeezed vacuum state with squeezing parameter r , the code $G(n, E, D)$ transforming the Gaussian channel T into the Gaussian channel T_{GC} is equivalent to a one-way protocol transforming n copies of the state $\chi = \lim_{r \rightarrow \infty} \mathbb{1} \otimes T(|\phi_r\rangle\langle\phi_r|)$ into one copy of the state $\chi_{\text{GC}} = \lim_{r \rightarrow \infty} \mathbb{1} \otimes T_{\text{GC}}(|\phi_r\rangle\langle\phi_r|)$ by local Gaussian operations only.

Proof.—Our main tool is the well-known isomorphism between CP maps and positive operators [17]. In particular, to any Gaussian CP map T acting on a Hilbert space \mathcal{H} corresponding to one mode, one can associate a Gaussian positive operator χ on $\mathcal{H} \otimes \mathcal{H}$ defined as

$$\chi = \lim_{r \rightarrow \infty} \mathbb{1} \otimes T(|\phi_r\rangle\langle\phi_r|), \quad (4)$$

where $|\phi_r\rangle = \sqrt{1 - \tanh^2(r)} \sum_n \tanh^n(r) |n, n\rangle$ is a two-mode squeezed vacuum state. Acting with T on a Gaussian state ρ can thus be seen as teleporting ρ through the quantum gate defined by the resource state χ [6]. It

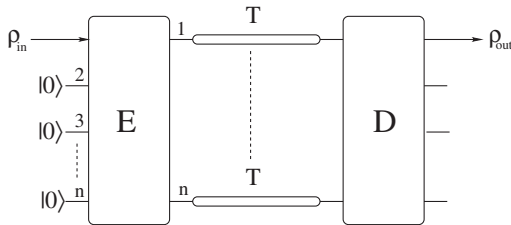


FIG. 1. Scheme of a Gaussian error-correcting code $G(n, E, D)$ for a Gaussian channel T , where E and D are n -mode unitary Gaussian operations used for encoding and decoding, respectively.

follows that the n uses of T appearing in the GECC can be replaced by n teleportations associated with the resource state χ , as shown in Fig. 2. Note that the operations involved in the teleportation, i.e., Bell measurement, one-way classical communication, and displacement all maintain the overall Gaussian character of the scheme. If the input of the GECC is now chosen to be one half of the state $|\phi_r\rangle$, then $G(n, E, D)$ is turned into a one-way Gaussian protocol that transforms n copies of state χ into one copy of state $\sigma_r = \mathbb{1} \otimes T_{\text{GC}}(|\phi_r\rangle\langle\phi_r|)$. The protocol is the following: Alice prepares the entangled state $|\phi_r\rangle$ and $n - 1$ ancillas, then applies the Gaussian operation E on the ancillas and one half of $|\phi_r\rangle$. Next, she performs n Bell measurements using the n copies of the resource state χ and communicates the results to Bob. Bob displaces his shares of the n resource states accordingly, and applies the Gaussian operation D . Alice and Bob now share one copy of the state σ_r . In particular, if Alice prepares the entangled state $\lim_{r \rightarrow \infty} |\phi_r\rangle$, the state they finally share is $\chi_{\text{GC}} = \lim_{r \rightarrow \infty} \sigma_r$. ■

The preceding Lemma does not say anything about the entanglement of the resource state χ and final state χ_{GC} , which is why we referred to a one-way protocol, not a one-way *entanglement distillation* protocol. For the protocol to be a true entanglement distillation protocol, one has to show that it increases entanglement, i.e., that $E[\chi_{\text{GC}}] > E[\chi]$ for some entanglement measure E . This is addressed by the following Lemma.

Lemma 2.—Given a Gaussian channel T with matrices M and N acting on one half of the entangled state $\rho_{\text{in}} = \lim_{r \rightarrow \infty} |\phi_r\rangle\langle\phi_r|$, the entanglement of the output state $\rho_{\text{out}} = \lim_{r \rightarrow \infty} \mathbb{1} \otimes T(|\phi_r\rangle\langle\phi_r|)$ is completely characterized by the *entanglement degradation* of the channel

$$D[T] = \min\left\{\frac{\det N}{(1 + \det M)^2}, 1\right\}. \quad (5)$$

In particular, the logarithmic negativity is the decreasing function $E_N[\rho_{\text{out}}] = -\frac{1}{2} \log D[T]$.

Proof.—Let us first assume that $\det M > 0$. Without restriction, we can choose $M = \eta \mathbb{1}$ since the channel can always be transformed into another Gaussian channel with $M' = SVMU$ and $N' = SVNVT S$ by adding two phase shifts of symplectic matrices U and V at the input and output, respectively, followed by a single-mode squeezer

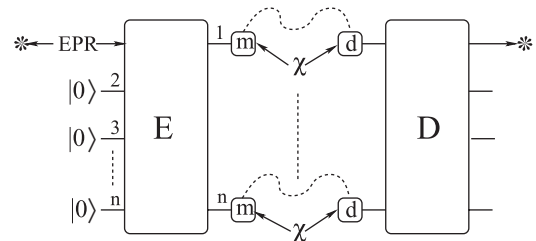


FIG. 2. From a GECC to Gaussian entanglement distillation. (m) Bell measurement; (d) displacement.

of symplectic matrix S . Note that these operations are local, so they do not affect the entanglement properties of the channel. By singular value decomposition, U and V can be chosen such that VMU is diagonal. Then, tuning the squeezing appropriately can make M' proportional to the identity, i.e., $M' = \eta\mathbb{1}$. Importantly, the determinant of symplectic matrices being equal to unity, $\det M' = \det M$ and $\det N' = \det N$.

Let us now consider the action of T on one-half of the state $|\phi_r\rangle\langle\phi_r|$ with covariance matrix $\gamma_{\text{in}}^{(r)}$. Recalling that covariance matrices of two-mode Gaussian states can be decomposed in four 2×2 blocks, we easily find the input and output covariance matrices to be

$$\gamma_{\text{in}}^{(r)} = \begin{pmatrix} A_r & C_r \\ C_r & A_r \end{pmatrix}, \quad \gamma_{\text{out}}^{(r)} = \begin{pmatrix} A_r & \eta C_r \\ \eta C_r & \eta^2 A_r + N \end{pmatrix}, \quad (6)$$

with

$$A_r = \cosh(2r) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad C_r = \sinh(2r) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Now, remember that the entanglement of a two-mode Gaussian state with covariance matrix

$$\gamma = \begin{pmatrix} A & B \\ B^T & C \end{pmatrix}$$

is fully characterized by the smallest symplectic eigenvalue ν_- of the partially transposed state [18]. In particular, the logarithmic negativity is given by $E_N = \max\{0, -\log \nu_-\}$. One can calculate ν_- from γ using

$$2\nu_-^2 = \tilde{\Delta} - \sqrt{\tilde{\Delta}^2 - 4 \det \gamma},$$

where $\tilde{\Delta} = \det A + \det C - 2 \det B$ [19]. For the output state $\rho_{\text{out}}^{(r)} = \mathbb{1} \otimes T(|\phi_r\rangle\langle\phi_r|)$ of covariance matrix $\gamma_{\text{out}}^{(r)}$, a few lines of calculation yields

$$\begin{aligned} \tilde{\Delta} &= \cosh^2(2r)(1 + \eta^2)^2 + O(\cosh(2r)), \\ \det \gamma_{\text{out}}^{(r)} &= \cosh^2(2r) \det N + O(\cosh(2r)), \end{aligned} \quad (7)$$

where we have used some known rules for the determinant of block matrices and the relation $\det(A + \lambda\mathbb{1}) = \det A + \lambda \text{Tr} A + \lambda^2$, which is valid for 2×2 matrices. We can now calculate ν_-^2 for the state $\rho_{\text{out}} = \lim_{r \rightarrow \infty} \mathbb{1} \otimes T(|\phi_r\rangle\langle\phi_r|)$. Using Eq. (7) and $\sqrt{1-x} = 1 - x/2 + O(x^2)$, we find

$$\begin{aligned} \lim_{r \rightarrow \infty} 2\nu_-^2 &= \lim_{r \rightarrow \infty} \tilde{\Delta} - \sqrt{\tilde{\Delta}^2 - 4 \det \gamma_{\text{out}}^{(r)}} \\ &= \lim_{r \rightarrow \infty} \frac{2 \det \gamma_{\text{out}}^{(r)}}{\tilde{\Delta}} \\ &= \frac{2 \det N}{(1 + \eta^2)^2}. \end{aligned} \quad (8)$$

Recalling that $\det M = \eta^2$, we obtain the logarithmic negativity of the state ρ_{out}

$$E_N[\rho_{\text{out}}] = -\frac{1}{2} \log \left(\min \left\{ \frac{\det N}{(1 + \det M)^2}, 1 \right\} \right). \quad (9)$$

Let us now consider a second class of channels, characterized by $\det M < 0$. An example of such channel is the approximate phase-conjugation map [20]. Using the same arguments as before, it is easy to show that we can restrict our attention to $M = \eta\Lambda$, where Λ is a real diagonal matrix with $\det \Lambda = -1$. The two symplectic invariants can again be easily calculated, and while $\det \gamma_{\text{out}}^{(r)}$ is unchanged, now $\tilde{\Delta} = \cosh^2(2r)(1 - \eta^2)^2 + O(\cosh(2r))$. Remembering that $\det M = -\eta^2$, we find again

$$\lim_{r \rightarrow \infty} 2\nu_-^2 = \frac{2 \det N}{(1 + \det M)^2}. \quad (10)$$

Moreover, combining this expression with the condition (2) of complete positivity, one finds that for such channel ν_- is always larger than 1, i.e., $E_N[\rho_{\text{out}}] = 0$, so that the output state ρ_{out} can never be entangled. These channels are called entanglement breaking channels. Finally, the last class of channels, characterized by $\det M = 0$, can easily be proven to be entanglement breaking using similar arguments, which completes the proof. ■

We are now in a position to prove our main result.

Theorem.—Given a Gaussian channel T with matrices M and N , there exists no GECC that transforms T into a Gaussian channel T_{GC} with matrices M_{GC} and N_{GC} having a lower entanglement degradation, i.e., such that

$$\frac{\det N_{\text{GC}}}{(1 + \det M_{\text{GC}})^2} < \min \left\{ \frac{\det N}{(1 + \det M)^2}, 1 \right\}. \quad (11)$$

Proof.—Our proof works by contradiction. Suppose that there exists a GECC as in Fig. 1 whose overall effect is to transform T into T_{GC} , and such that the condition (11) is satisfied. By Lemma 1, there exists a one-way Gaussian protocol as in Fig. 2 which transforms n copies of the state χ into the state $\chi_{\text{GC}} = \lim_{r \rightarrow \infty} \mathbb{1} \otimes T_{\text{GC}}(|\phi_r\rangle\langle\phi_r|)$. Lemma 2 combined with condition (11) shows that $E_N[\chi_{\text{GC}}] > E_N[\chi]$; hence, the resulting one-way protocol is a true entanglement distillation protocol based on Gaussian operations only. This is in clear contradiction with the impossibility to distill entanglement of a Gaussian state with Gaussian operations [21]. We conclude that such a GECC does not exist. ■

We now illustrate this no-go theorem by applying the criterion (11) to some well-known Gaussian channels.

Attenuation channel.—This channel T_η is characterized by $M = \eta\mathbb{1}$ and $N = |1 - \eta^2|\mathbb{1}$, with $\eta < 1$. It is the prototype channel for optical communication through a lossy fiber, and can be modeled by a beam splitter of transmittance η . Its entanglement degradation

$$D[T_\eta] = \frac{(1 - \eta^2)^2}{(1 + \eta^2)^2} < 1 \quad (12)$$

is a decreasing function of η . Hence, by (11), it is impos-

sible to find a GECC that turns T_η into another attenuation channel with less losses. As is well known, one can nevertheless reduce the attenuation by amplifying ($\eta < \eta_{GC} < 1$) but at the expense of an increasing noise N_{GC} . A bound on the minimum achievable noise is given by (11).

Amplification channel.—It is similar to the attenuation channel, but with $\eta > 1$. Thus, Eq. (12) holds, but now D is an increasing function of η , so that it is impossible to make $\eta_{GC} < \eta$. Again, one can reduce the amplification at the expense of an increased noise, e.g., by concatenating the amplification channel with an attenuation channel.

Classical noise channel.—This channel T_N adds Gaussian classical noise to the input state, i.e., $M = 1$ and $N > 0$. Its entanglement degradation is

$$D[T_N] = \min\left\{\frac{\det N}{4}, 1\right\}, \quad (13)$$

so that our theorem implies that it is impossible to reduce the noise when $\det N \leq 4$, and that it is impossible to reduce the noise under 4 when $\det N > 4$. Note that this limit of 4 can always be reached as the number of available ancillas goes to infinity. Alice simply needs to optimally measure the input state and send to Bob an infinite number of states centered on her measurement result. Bob measures the received states and prepares a state centered on the average value of his measurements. This measure-and-prepare strategy yields $\det N = 4$.

To summarize our results, we have introduced an intrinsic property of single-mode Gaussian channels called entanglement degradation, and proven that it cannot be reduced by Gaussian encoding and decoding operations only. Such a no-go theorem for the correction of Gaussian errors with Gaussian operations nicely complements the well-known impossibility to distill the entanglement of Gaussian states with Gaussian local operations. In this Letter we focused on deterministic Gaussian CP maps since these describe the most common practical communication channels. However, the no-go theorem can be straightforwardly extended to probabilistic trace-decreasing Gaussian CP maps isomorphic to generic two-mode Gaussian states χ [5,6]. One only needs to define $D[T] = \min(1, \nu_-)$, where ν_- is the lower symplectic eigenvalue of the covariance matrix of the partially transposed χ .

Interestingly, the entanglement degradation can be related to another important intrinsic properties of channels, namely, the quantum capacity Q . In particular, one can show that the quantum capacity of a single-mode Gaussian channel T is always upper bounded by the function of D

$$Q[T] \leq -\frac{1}{2} \log D[T]. \quad (14)$$

This result follows from [22], where a computable upper bound on the quantum capacity was introduced. This ca-

capacitylike quantity Q_θ can be defined as the maximal entanglement, as measured by the logarithmic negativity, of states transmitted through the channel T , i.e., $Q_\theta[T] = -\frac{1}{2} \log D[T]$ for single-mode Gaussian channels. A natural and promising extension of our Letter would therefore be to investigate whether a Gaussian no-go theorem also holds for the quantum capacity of Gaussian channels.

We acknowledge financial support of the EU under the FET-Open project COMPAS (212008). J. N. acknowledges support from the Belgian FRIA foundation, and J. F. acknowledges support from MSMT (Grants No. LC06007 and No. MSM6198959213).

-
- [1] A. Furusawa *et al.*, *Science* **282**, 706 (1998).
 - [2] F. Grosshans *et al.*, *Nature (London)* **421**, 238 (2003).
 - [3] U. L. Andersen, V. Josse, and G. Leuchs, *Phys. Rev. Lett.* **94**, 240503 (2005).
 - [4] J. Eisert, S. Scheel, and M. B. Plenio, *Phys. Rev. Lett.* **89**, 137903 (2002).
 - [5] J. Fiurášek, *Phys. Rev. Lett.* **89**, 137904 (2002).
 - [6] G. Giedke and J. I. Cirac, *Phys. Rev. A* **66**, 032316 (2002).
 - [7] A. Ourjoumtsev, R. Tualle-Brouiri, J. Laurat, and P. Grangier, *Science* **312**, 83 (2006).
 - [8] J. Eisert *et al.*, *Ann. Phys. (N.Y.)* **311**, 431 (2004).
 - [9] C. H. Bennett *et al.*, *Phys. Rev. A* **54**, 3824 (1996).
 - [10] S. L. Braunstein, *Phys. Rev. Lett.* **80**, 4084 (1998).
 - [11] S. Lloyd and J.-J. E. Slotine, *Phys. Rev. Lett.* **80**, 4088 (1998).
 - [12] A. Franzen *et al.*, *Phys. Rev. Lett.* **97**, 150505 (2006).
 - [13] J. Heersink *et al.*, *Phys. Rev. Lett.* **96**, 253601 (2006).
 - [14] C. Wittmann *et al.*, *Phys. Rev. A* **78**, 032315 (2008).
 - [15] J. Niset, U. L. Andersen, and N. J. Cerf, *Phys. Rev. Lett.* **101**, 130503 (2008).
 - [16] N. J. Cerf, G. Leuchs, and E. S. Polzik, *Quantum Information with Continuous Variables of Atoms and Light* (Imperial College Press, London, 2007).
 - [17] A. Jamiolkowski, *Rep. Math. Phys.* **3**, 275 (1972).
 - [18] G. Adesso and F. Illuminati, *Phys. Rev. A* **72**, 032334 (2005).
 - [19] G. Vidal and R. F. Werner, *Phys. Rev. A* **65**, 032314 (2002).
 - [20] N. J. Cerf and S. Iblisdir, *Phys. Rev. A* **64**, 032307 (2001).
 - [21] Note that in [6], the impossibility is proven using $V(\gamma_{AB})$ as the entanglement measure, where $V(\gamma_{AB})$ is defined as the largest value $p \leq 1$ such that $\gamma_{AB} \geq p(\gamma_A \oplus \gamma_B)$ for some γ_A and γ_B . However, it is shown in the appendix of [6] that for a $1 \times N$ Gaussian state ρ_{AB} , $V(\gamma_{AB})$ is exactly equal to the smallest symplectic eigenvalue of the covariance matrix of the partially transposed state $\rho_{AB}^{T_A}$. It follows that $E_N(\gamma_{AB})$ is a monotonic function of $V(\gamma_{AB})$, so that the result of [6] is equivalent to the impossibility of increasing the logarithmic negativity of $1 \times N$ Gaussian states with Gaussian operations only.
 - [22] A. S. Holevo and R. F. Werner, *Phys. Rev. A* **63**, 032312 (2001).