Transmission of classical information through Gaussian quantum channels

Oleg V. Pilyavets

Université Libre de Bruxelles (ULB), Brussels, Belgium

In collaboration with Evgueni Karpov, Joachim Schäfer, and others

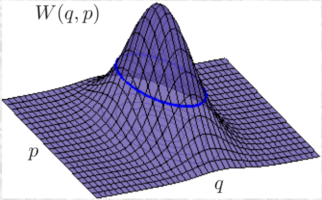
Noise, Information, and Complexity @ Quantum Scale
E. Majorana Centre, Erice, Italy

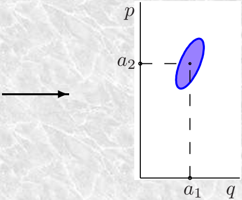
October 10, 2013

- *Bosonic systems* (optical modes) with CCRs $[\hat{a}_h, \hat{a}_l^\dagger] = \delta_{hl}$, $[\hat{a}_h, \hat{a}_l] = 0$ $\quad (\hbar = 1,\ \omega_k = 1)$.
- *Gaussian states* of bosonic field modes:
  - Wigner function in quadratures phase space is Gaussian
  - The most general case is *rotated thermal squeezed displaced* state

$$\hat{\rho} \longleftrightarrow \{\mathbf{a}, V\} \longleftrightarrow W(\mathbf{x}) = \frac{1}{\sqrt{\det V}}\, e^{-\frac{1}{2}(\mathbf{x}-\mathbf{a}, V^{-1}(\mathbf{x}-\mathbf{a}))}$$

$$\mathbf{x} := (q_1, p_1, \ldots, q_n, p_n) \qquad \mathbf{a} := \sqrt{2}(\mathrm{Re}(\alpha_1), \mathrm{Im}(\alpha_1), \ldots, \mathrm{Re}(\alpha_n), \mathrm{Im}(\alpha_n))$$





- Examples of single-mode states:
  - Vacuum state is $\{0, \frac{\mathrm{Id}}{2}\}$
  - Coherent state is $\left\{\sqrt{2}(\mathrm{Re}(\alpha), \mathrm{Im}(\alpha)), \frac{\mathrm{Id}}{2}\right\}$
  - Non-displaced diagonal squeezed state is $\{0, V\}$, where quadratures *covariance matrix*

$$V = \begin{pmatrix} \sigma_{qq} & \sigma_{qp} \\ \sigma_{qp} & \sigma_{pp} \end{pmatrix} = \left[\mathcal{N} + \frac{1}{2}\right] \begin{pmatrix} e^{2s} & 0 \\ 0 & e^{-2s} \end{pmatrix} = \left[\mathcal{N} + \frac{1}{2}\right] \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix}$$

Parameters of the single-mode diagonal quadratures covariance matrix for the state $\hat{\rho}$:

$$V = \begin{pmatrix} \sigma_{qq} & \sigma_{qp} \\ \sigma_{qp} & \sigma_{pp} \end{pmatrix} = \left[\mathcal{N} + \frac{1}{2}\right] \begin{pmatrix} e^{2s} & 0 \\ 0 & e^{-2s} \end{pmatrix} = \left[\mathcal{N} + \frac{1}{2}\right] \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix}$$

- $\mathcal{N} \geqslant 0$ is the *amount of **thermal** photons* in quantum state
- $s \in \mathbb{R}$, $0 \leqslant s \leqslant \infty$ is the *squeezing of quantum state* (we will always assume $s \geqslant 0$)
- $\omega \in [0, 1]$, $\omega = e^{-2s}$ is the *"frequency"*
- $N \geqslant 0$ is the *(average) amount of photons (energy)* in quantum state:

$$N = \mathrm{Tr}\left(\hat{a}^\dagger \hat{a} \hat{\rho}\right) \qquad \frac{1}{2}\mathrm{Tr}(V) = N + \frac{1}{2}$$

- $\nu \geqslant \frac{1}{2}$ is the *symplectic eigenvalue*:

$$\nu = \sqrt{\det(V)} = \mathcal{N} + \frac{1}{2}$$

- $S(\hat{\rho}) = -\mathrm{Tr}(\hat{\rho} \log_2 \hat{\rho})$ is *von Neumann entropy*:

$$S(V) = g(\mathcal{N}) \qquad g(x) := (x+1)\log_2(x+1) - x \log_2 x$$

Notations for n mode separable state with covariance matrix V and amount of photons N are the same (index k is added to each symbol to label kth mode):

$$V = \bigoplus_{k=1}^{n} V_{\mathrm{ind},k} \qquad N = \frac{1}{n}\sum_{k=1}^{n} N_k$$

- *Memory quantum channel* Φ: sequence of CPTP-maps

$$\{\Phi_1, \Phi_2, \Phi_3, \dots\}, \quad \text{where} \quad \dim(\Phi_k) = [\dim(\Phi_1)]^k$$

- *Memoryless quantum channel* Φ: sequence of CPTP-maps

$$\{\Phi, \Phi^{\otimes 2}, \Phi^{\otimes 3}, \dots\}$$

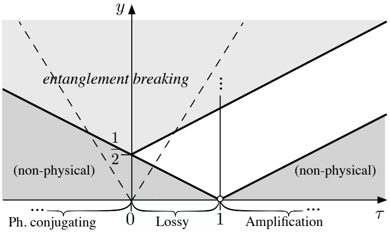
- Memory channel is memoryless if $\Phi_n = \Phi_1^{\otimes n}$.
- $\Phi^{\otimes n}$ is associated with *n channel uses*
- Single-mode *Gaussian quantum channel* Φ is a sequence of maps $\{\Phi_n\}$, where each Φ_n:
  - CPTP map that is closed on the set of Gaussian states
  - Characterized by the *triad* $(\mathbf{d}_n, X_n, Y_n)$
    - $\mathbf{d}_n \in \mathbb{R}^{2n}$ a displacement vector
    - X_n and Y_n are real $2n \times 2n$-matrices obeying inequality

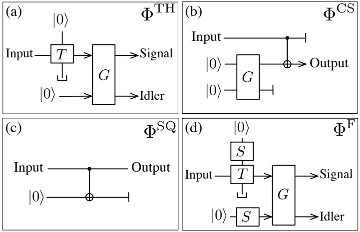
$$Y_n + \frac{i}{2}\left(\Sigma - X_n^\top \Sigma X_n\right) \geqslant 0$$

    - Y_n is a valid covariance matrix ($Y_n^\top = Y_n$, $Y_n \geqslant 0$).
  - Maps the first and the second moments as $\{\mathbf{a}, V\} \mapsto \{X_n^\top \mathbf{a} + \mathbf{d}_n, X_n^\top V X_n + Y_n\}$
- *n* uses of single-mode channel can always be treated as the single use of *n* mode channel
- Single-mode Gaussian quantum channel:

$$\tau = \det X, \qquad y = \sqrt{\det Y} \qquad \longrightarrow \qquad y \geqslant \frac{1}{2}|\tau - 1|$$

Classification of the single-mode Gaussian quantum channels





Channel	**Class**	X_C	Y_C	τ	**Domain of** τ	**Domain of** y
Zero-Transmission		0	$(G-1/2)\mathbb{I}$	0	0	$[1/2,\infty)$
Classical additive noise		$\mathbb{I}$	$(G-1)\mathbb{I}$	$TG=1$	1	$[0,\infty)$
Lossy	$\Phi^{\rm TH}$	$\sqrt{\tau}\mathbb{I}$	$[G(1-T/2)-1/2]\mathbb{I}$	TG	$[0,1]$	$[(1-\tau)/2,\infty)$
Amplification		$\sqrt{\tau}\mathbb{I}$	$[G(1-T/2)-1/2]\mathbb{I}$	TG	$[1,\infty)$	$[(\tau-1)/2,\infty)$
Phase conjugating		$\sqrt{\lvert\tau\rvert}\sigma_z$	$[(1-T)(G-1)+G]/2\mathbb{I}$	$-T(G-1)$	$(-\infty,0]$	$[(1-\tau)/2,\infty)$
Classical-signal	$\Phi^{\rm CS}$	$(\mathbb{I}+\sigma_z)/2$	$(G-1/2)\mathbb{I}$	$\mathbf{0}$	$\mathbf{0}$	$[1/2,\infty)$
Single-quad. cl. noise	$\Phi^{\rm SQ}$	$\mathbb{I}$	$(\mathbb{I}-\sigma_z)/4$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{0}$

- Classification of single-mode Gaussian quantum channels according to ranks of matrices $X_{\rm C}$ and $Y_{\rm C}$:

$$\Phi = U_2 \circ \Phi^{\rm C} \circ U_1, \quad \text{where} \quad \Phi^{\rm C} = (d_{\rm C}, X_{\rm C}, Y_{\rm C})$$

  - F. Caruso, V. Giovannetti, and A. S. Holevo, New J. Phys. **8**, 310 (2006)
  - A. S. Holevo, Probl. Inf. Trans. 43, 1 (2007)

- New classification in terms of *fiducial channel* $\Phi^{\rm F} = (d_{\rm F}, X_{\rm F}, Y_{\rm F})$ that can be completely specified by three parameters (τ, y, s):

$$X_{\rm F} = X_{\rm TH}, \qquad Y_{\rm F} = y\begin{pmatrix} e^{2s} & 0 \\ 0 & e^{-2s}\end{pmatrix}, \qquad X = MX_{\rm F}(\tau)\Theta, \qquad Y = MY_{\rm F}(y,s)M^{\top}$$

  - J. Schäfer, E. Karpov, R. García-Patrón, O. V. Pilyavets, and N. J. Cerf, Phys. Rev. Lett. 111, 030503 (2013).

Classical information transmission:

$\{\alpha\in\mathbb{R}\}$ alphabet $\Longrightarrow$ $\{\hat{\rho}_{\rm in}^{(\alpha)}\}$ input states $\xrightarrow{\text{QUANTUM CHANNEL}}$ $\{\hat{\rho}_{\rm out}^{(\alpha)}\}$ output states $\Longrightarrow$ $\{\pi\}$ measurement

- Given input ensemble of symbol states $\{\hat{\rho}_{\rm in}^{(\alpha)}\}$ with weights (*modulation*) $\{P_\alpha\}$, maximal amount of information that can be transmitted "in average by using the channel only n times" is given by *Holevo bound* χ:

$$\chi(\Phi_n) = S\left(\hat{\bar{\rho}}_{\rm out}\right) - \int S(\hat{\rho}_{\rm out}^{\alpha}) P_\alpha \, d\alpha, \quad \text{where} \quad \hat{\bar{\rho}}_{\rm out} = \int \Phi_n(\hat{\rho}_{\rm in}^{\alpha}) P_\alpha \, d\alpha, \quad \hat{\rho}_{\rm out}^{\alpha} = \Phi_n(\hat{\rho}_{\rm in}^{\alpha})$$

- In particular, if $S(\hat{\rho}_{\rm out}^{\alpha})$ does not depend on α:

$$\chi(\Phi_n) = S\left(\hat{\bar{\rho}}_{\rm out}\right) - S(\hat{\rho}_{\rm out}^{\alpha})$$

- If, furthemore, both $\hat{\bar{\rho}}_{\rm out}$ and $\hat{\rho}_{\rm out}^{\alpha}$ are Gaussian and the channel is single-mode one:

$$\chi(\Phi) = g(\overline{\mathcal{N}}_{\rm out}) - g(\mathcal{N}_{\rm out})$$

- Maximal amount of information that can be transmitted "in average" through quantum channel defines its *classical capacity*:

$$C = \lim_{n\to\infty}\left[\frac{1}{n}\lim_{m\to\infty}\left(\frac{1}{m}\max_{\{\hat{\rho}_{\rm in}^{(\alpha)}, P_\alpha\}}\chi(\Phi_n^{\otimes m})\right)\right], \qquad \text{where} \qquad \Phi_n^{\otimes m} = \left[\Phi_1^{\otimes n}\right]^{\otimes m}$$

if the single-mode channel is memoryless (one of the limits can be omitted in this case).

- In the case of Gaussian quantum channels average state at the channel input $\hat{\bar{\rho}}_{\rm in} = \int \hat{\rho}_{\rm in}^{\alpha} P_\alpha \, d\alpha$ must have finite energy (average amount of photons should not exceed N per mode / per use).

Final goal

The problem:

Find classical capacity C of arbitrary Gaussian quantum channel (d, X, Y)

Despite the knowledge of the classical capacity is not required in current applications of quantum information theory, there are few connections which could make it useful in future:

1. The classical capacity of quantum channel (as well as the capacity of classical channel) can be treated as a maximal value of mutual information achievable between the channel input and output. This makes its interpretation as the maximal degree of correlations achievable between the channel input and output. The knowledge of this quantity can be potentially useful to prove the security of some quantum protocols.
2. The signal states used by QKD are always fixed by a particular protocol. Therefore, neither the knowledge of capacity nor the knowledge of homodyne/heterodyne rates maximized over all possible encodings is necessary for QKD. However, these quantities potentially may help to design QKD protocols with higher bit rates.
3. The classical capacity is similar to other capacities (e.g. private capacity), which may have independent interest. The tools and methods developed for the calculation of classical capacity may be useful for them too.
4. By studying the properties of classical capacity one can better understand quantum information theory in general, its advantages and disadvantages for information processing.

Now classical capacity is known for:

1. Ideal channel: $C = g(N)$ (Yuen-Ozawa bound).
   - H. P. Yuen and M. Ozawa, Phys. Rev. Lett. 70, 363 (1993).
2. Pure lossy channel with vacuum environment: $C = g(\eta N)$
   - V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, Phys. Rev. Lett. 92, 027902 (2004).
3. Lossy channel with pure environment if input energy is above some threshold:

$$C = g[\eta N + (1-\eta)N_{\mathrm{env}}]$$

   - C. Lupo, O. V. Pilyavets, and S. Mancini, New J. Phys. 11, 063023 (2009).

Soon it will be *probably* known for:

- Abitrary non-patalogical Gaussian channel if input energy is above some threshold

$$C = g\left[|\tau|N + y\cosh(2s) + \frac{|\tau|-1}{2}\right] - g\left[y + \frac{|\tau|-1}{2}\right]$$

  - J. Schäfer, E. Karpov, R. García-Patrón, O. V. Pilyavets, and N. J. Cerf, Phys. Rev. Lett. 111, 030503 (2013)
  - We need to accomplish: proof of *minimum output entropy conjecture*
- Gaussian channel if squeezing in its environment is infinite ($s \to \infty$):

$$C = \log_2(2N+1)$$

  - C. Lupo, O. V. Pilyavets, and S. Mancini, New J. Phys. 11, 063023 (2009)
  - O. V. Pilyavets, C. Lupo, and S. Mancini, IEEE Trans. Inf. Theory 58, 6126 (2012)
  - Fact 1: in this case optimal Gaussian input states realize maximum SNR for given input energy
  - Fact 2: channel is (in some sense) "classical" in this case (one of quadratures is infinitely noisy)

Gaussian classical capacity

- Optimal input ensemble $\{P_\alpha, \hat{\rho}_{\text{in}}^{\alpha}\}$ is not known in general
- *Gaussian classical capacity*: maximum of Holevo bound on the set of Gaussian states
- Most prominent set $\{P_\alpha, \hat{\rho}_{\text{in}}^{\alpha}\}$: arbitrary Gaussian state displaced in phase space with *Gaussian modulation*

$$P_\alpha = \frac{1}{\pi^n \sqrt{\det V_{\text{mod}}}} \exp\left[-\left(\boldsymbol{\alpha}, V_{\text{mod}}^{-1} \boldsymbol{\alpha}\right)\right]$$

  - J. Eisert, M. M. Wolf, arXiv:0505151 (2005)
- *Hypothesis:* Gaussian ensemble (displacement of the same "seed" Gaussian state) with Gaussian modulation is optimal. Supporting arguments:
  1. If the minimum output entropy conjecture is valid, such encodings are optimal, provided that the input energy is above some threshold value
  2. Similar to the actual capacity the Gaussian capacity (calculated using such encodings) is also concave function of input energy
     - O. V. Pilyavets, C. Lupo, and S. Mancini, IEEE Trans. Inf. Theory 58, 6126 (2012)
     - J. Schäfer, E. Karpov, and N. J. Cerf, Phys. Rev. A 84, 032318 (2011)
  3. Optimality of Gaussian modulation can be shown above some energy threshold if the symbol states are any Gaussian states. Actually, its optimality can be shown in all cases if it is in addition assumed that the averaged (over ensemble) modulated state is also Gaussian
- There are alternative viewpoints:
  - Only coherent state encodings are interesting
  - Input states should be excluded from the energy constraint and treated as a part of the channel environment (energy is spent only for modulation)

- Simplification: $C(\Phi, N) = C(\Phi^{\mathrm{F}}, N)$
  - J. Schäfer, E. Karpov, R. García-Patrón, O. V. Pilyavets, and N. J. Cerf, Phys. Rev. Lett. 111, 030503 (2013)
- Classical capacity above the input energy threshold:

$$C = g\left[|\tau|N + \frac{y}{2}\left(\omega_{\mathrm{env}}^{-1} + \omega_{\mathrm{env}}\right) + \frac{|\tau|-1}{2}\right] - g\left[y + \frac{|\tau|-1}{2}\right]$$

- Below the input energy it is still *hard* problem (in this case capacity depends on the solution of a transcendental equation)
- The solution satisfies Planck equation, where "frequency" represents squeezing:

$$\overline{\mathcal{N}}_{\mathrm{out}} = \frac{1}{e^{\overline{\omega}_{\mathrm{out}}\overline{\beta}_{\mathrm{out}}} - 1}$$

- It also satisfies "resonance equation":

$$\overline{\omega}_{\mathrm{out}} = \sqrt{1 - \frac{\beta_{\mathrm{out}}}{\overline{\beta}_{\mathrm{out}}}\left(\omega_{\mathrm{in}}^2 - \omega_{\mathrm{out}}^2\right)}$$

Here

$$\beta(\mathcal{N}, \omega) := \frac{g'(\mathcal{N})\ln 2}{\omega}, \qquad \beta_{\mathrm{out}} \equiv \beta(\mathcal{N}_{\mathrm{out}}, \omega_{\mathrm{out}}), \qquad \overline{\beta}_{\mathrm{out}} = \beta(\overline{\mathcal{N}}_{\mathrm{out}}, \overline{\omega}_{\mathrm{out}})$$

- Example of Gaussian channel: *lossy bosonic channel* (LBC)
- LBC can be reduced to the following relation between covariance matrices for input, environment and output states:

$$V_{\text{out}} = \eta V_{\text{in}} + (1-\eta) V_{\text{env}}$$

thus, the *average output* state of the channel is given by

$$\overline{V}_{\text{out}} = \eta\,(V_{\text{in}} + V_{\text{mod}}) + (1-\eta) V_{\text{env}}$$

- Channel environment (single-mode):

$$V_{\text{env}} := V(\mathcal{N}_{\text{env}}, s) = \left[\mathcal{N}_{\text{env}} + \frac{1}{2}\right] \begin{pmatrix} e^{2s} & 0 \\ 0 & e^{-2s} \end{pmatrix}, \qquad \frac{1}{2}\text{Tr}(V_{\text{env}}) = N_{\text{env}} + \frac{1}{2}$$

- Capacity (single-mode case) is the function $C(N, \eta, s, \mathcal{N}_{\text{env}})$

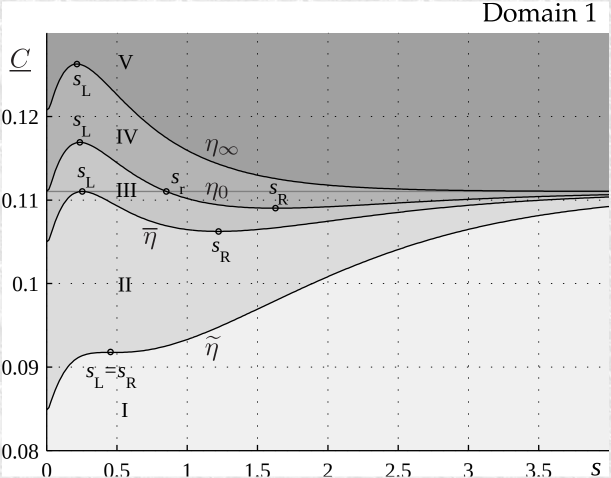
- Example of Ω *memory model*

$$V_{\rm env} = \left(\mathcal{N}_{\rm env} + \frac{1}{2}\right)\begin{bmatrix} e^{s\Omega} & 0 \\ 0 & e^{-s\Omega} \end{bmatrix}, \qquad \lambda_\xi(V_{\rm env}) = \left(\mathcal{N}_{\rm env} + \frac{1}{2}\right) e^{\pm 2s\cos\xi},$$

$$\Omega = \begin{pmatrix} 0 & 1 & \ldots\ldots\ldots\ldots & & & 0 \\ 1 & 0 & 1 & \ldots\ldots & & 0 \\ \vdots & 1 & 0 & 1 & .. & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \\ \vdots & \vdots & & \ddots & \ddots & 1 \\ 0 & 0 & \ldots\ldots & & 1 & 0 \end{pmatrix}$$

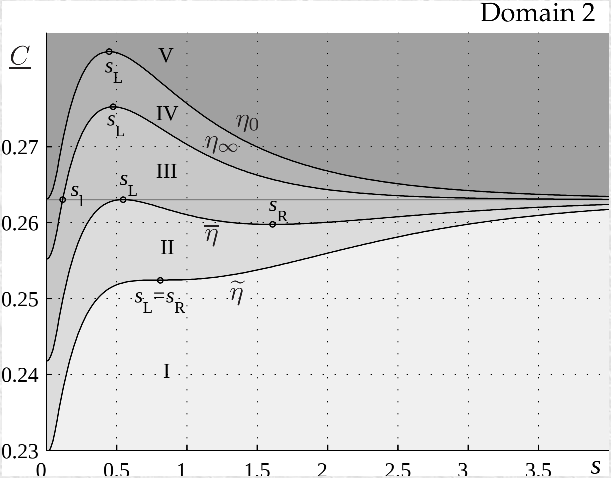
- Properties of Ω-model (*quite realistic*):
  - Memory is *non-Markovian*
  - Correlations between channel uses decreases if the time interval between them increases
  - Decay of correlations is *exponentional*

- Domain 1 is the range of channel parameters $(N, \mathcal{N}_{\mathrm{env}})$ where the capacity as a function of squeezing s has the following *five* types of behaviour that depend on the value of transmissivity η:

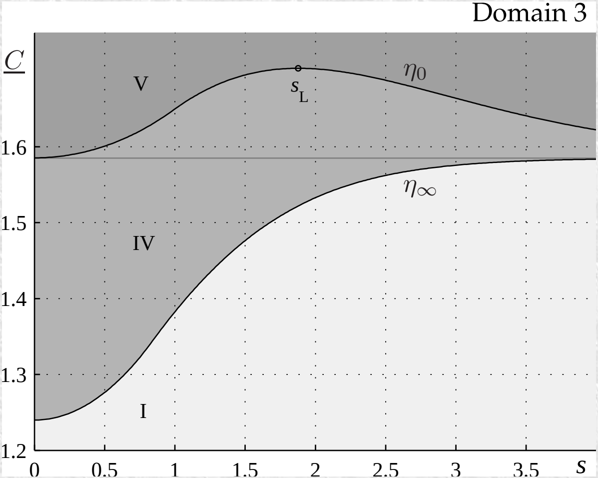


Classical capacity: graph for domain 2

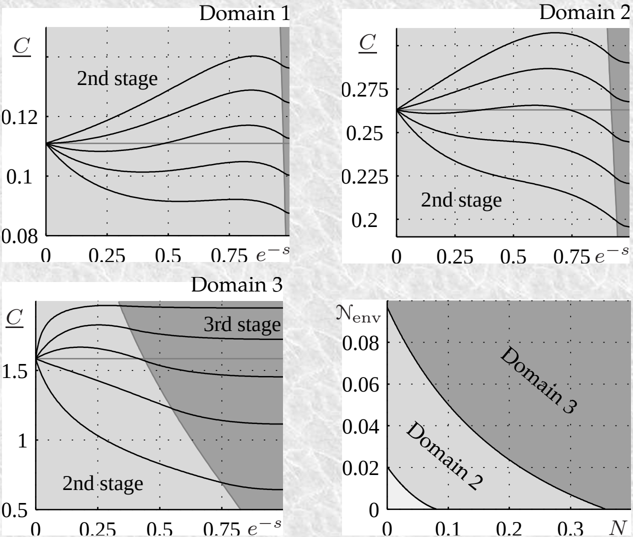
- Domain 2 is the range of channel parameters $(N, \mathcal{N}_{\text{env}})$ where the capacity as a function of squeezing s has the following *five* types of behaviour that depend on the value of transmissivity η:



- Domain 3 is the range of channel parameters $(N, \mathcal{N}_{\rm env})$ where the capacity as a function of squeezing s has the following *three* types of behaviour that depend on the value of transmissivity η:



Classical capacity: graphs for all domains and the domains themselves



Classical capacity: fundamental constants

- Capacity $C(s)$ cannot have two extrema in the interval $0 < s < \infty$ if at least one of the following inequalities is satisfied:

$$N \geqslant \frac{1}{2}\left[\sqrt{\frac{3}{2}+\frac{5}{2\sqrt{3}}}-1\right] \approx 0.3578$$

$$\mathcal{N}_{\mathrm{env}} \geqslant \frac{1}{2}\left[\left(\sqrt{3}-\frac{2}{\sqrt{5}}\right)^{-1}-1\right] \approx 0.0969$$

$$\eta \geqslant \frac{2}{\sqrt{15}} \approx 0.5164$$

  In particular, the parameters $(N, \mathcal{N}_{\mathrm{env}})$ defined by the first two inequalities belong to the third domain

- Capacity $C(s)$ is a monotonically increasing function in the neighborhood of $s \to \infty$ if

$$\eta \leqslant 1 - \frac{1}{\sqrt{3}} \approx 0.4227$$

- For $N \to \infty$ the equality $C(s = 0) = C(s \to \infty)$ is possible only if

$$\eta \geqslant \frac{2}{e} \approx 0.7358$$

thank you!