Gaussian capacity of the single-mode Gaussian channel

Joachim Schäfer, Evgueni Karpov, Oleg V. Pilyavets, and N. J. Cerf

Université Libre de Bruxelles (ULB), Brussels, Belgium

21st Central European Workshop on Quantum Optics
Brussels, Belgium

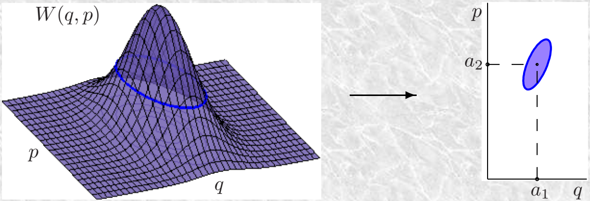
June 27, 2014

Gaussian quantum states

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

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

$$\mathbf{x} := (q, p) \qquad \mathbf{a} := \sqrt{2}\left(\mathrm{Re}(\alpha), \mathrm{Im}(\alpha)\right)$$



- 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 squeezed state $\{0, V\}$ with *diagonal* 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"*
- $N \geqslant 0$ (don't confuse with $\mathcal{N}$) is the *(average) amount of photons (energy)* in quantum state:

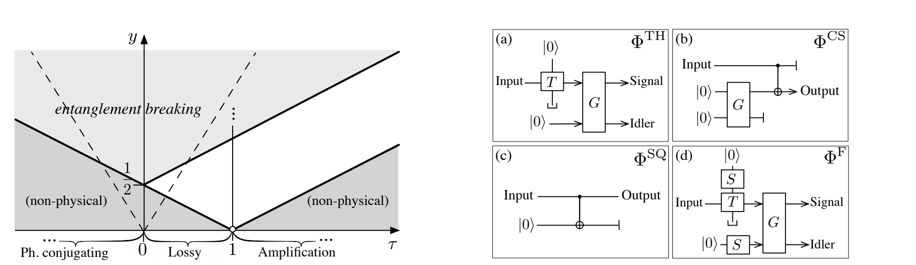
$$N = \mathrm{Tr}\left(\hat{a}^{\dagger}\hat{a}\hat{\rho}\right) \qquad \frac{1}{2}\mathrm{Tr}(V) = N + \frac{1}{2}$$

- $\nu \geqslant \frac{1}{2}$ 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*:

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



Single-mode *Gaussian quantum channel* Φ:

- CPTP map that is closed on the set of Gaussian states
- Characterized by the *triad* $(\mathbf{d}, X, Y)$
  - $\mathbf{d} \in \mathbb{R}^2$ a displacement vector
  - X and Y are real 2×2-matrices obeying inequality

$$y \geqslant \frac{1}{2}|\tau - 1|$$

    where $\tau = \det X$ and $y = \sqrt{\det Y}$
  - Y is some valid covariance matrix ($Y^\top = Y$, $Y \geqslant 0$)
- Maps the first and the second moments as $\{\mathbf{a}, V\} \mapsto \{X^\top \mathbf{a} + \mathbf{d}, X^\top V X + Y\}$

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	Φ^{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	Φ^{CS}	$(\mathbb{I}+\sigma_z)/2$	$(G-1/2)\mathbb{I}$	0	0	$[1/2,\infty)$
Single-quad. cl. noise	Φ^{SQ}	$\mathbb{I}$	$(\mathbb{I}-\sigma_z)/4$	1	1	0

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

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

  - 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* $\Phi^{\mathrm{F}} = (d_{\mathrm{F}}, X_{\mathrm{F}}, Y_{\mathrm{F}})$ that can be completely specified by three parameters (τ, y, s):

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

  - J. Schäfer, E. Karpov, R. García-Patrón, O. V. Pilyavets, and N. J. Cerf, *Phys. Rev. Lett.* **111**, 030503 (2013)
  - C. Lupo, S. Pirandola, P. Aniello, and S. Mancini, *Phys. Scr.* **T143**, 014016 (2011)

Classical capacity

Classical information transmission:

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

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

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

- If $S\left(\hat{\rho}_{\text{out}}^{\alpha}\right)$ does not depend on α:

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

- If, furthemore, both $\hat{\bar{\rho}}_{\text{out}}$ and $\hat{\rho}_{\text{out}}^{\alpha}$ are Gaussian:

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

- Maximal amount of information that can be transmitted "in average" through quantum channel defines its *classical capacity* (so-called *one-shot classical capacity*):

$$C = \max_{\{\hat{\rho}_{\text{in}}^{(\alpha)}, P_\alpha\}} \chi(\Phi)$$

- In the case of Gaussian quantum channels average state at the channel input $\hat{\bar{\rho}}_{\text{in}} = \int \hat{\rho}_{\text{in}}^{\alpha} P_\alpha \, d\alpha$ must have finite energy (average amount of photons should not exceed N per one 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.
5. One can imagine new generation of hard drives ("quantum HDD"), where cells storing classical bits are some qubits. If we will read them using optical beam, the classical capacity is the upper bound on the reading speed from such hard drives.
6. Gaussian noise is somehow fundamental: it gives "worst case capacity."

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. 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)
4. 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)

   (Thanks to a proof of *minimum output entropy conjecture*: V. Giovannetti, R. García-Patrón, N. J. Cerf, and A. S. Holevo, arXiv:1312.6225)

In near future it will be *probably* known also for 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 env. quadratures is infinitely noisy)

- 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 the 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:

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

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

$$\overline{V}_{\mathrm{out}} = \eta \left(V_{\mathrm{in}} + V_{\mathrm{mod}} \right) + (1-\eta) V_{\mathrm{env}}$$

- Channel environment (single-mode):

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

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

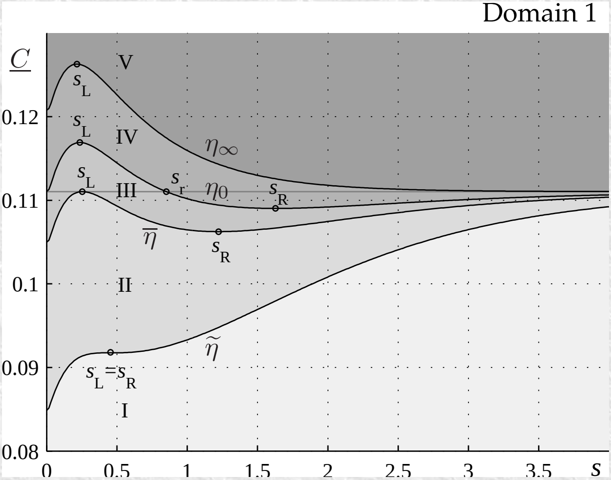
- Example of Ω *memory model*:

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

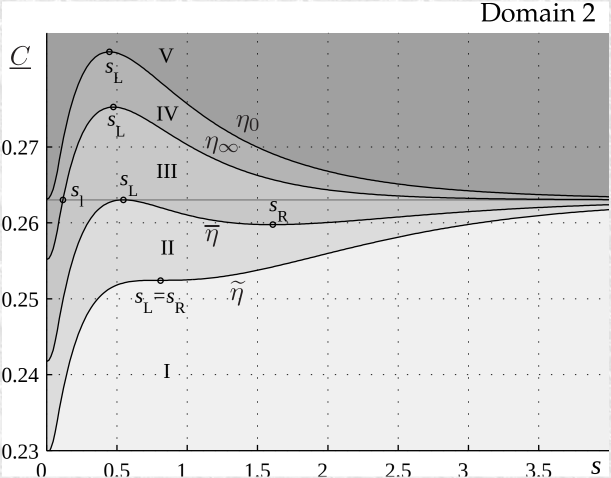
$$\Omega = \begin{pmatrix} 0 & 1 & \ldots\ldots\ldots\ldots & & & 0 \\ 1 & 0 & 1 & \ldots\ldots\ldots & & 0 \\ \vdots & 1 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \\ \vdots & \vdots & & \ddots & \ddots & 1 \\ 0 & 0 & \ldots\ldots & & 1 & 0 \end{pmatrix}$$

- 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*
- It was considered in:
  - O. V. Pilyavets, C. Lupo, and S. Mancini, *IEEE Trans. Inf. Theory* **58**, 6126 (2012)
  - C. Lupo, O. V. Pilyavets, and S. Mancini, *New J. Phys.* **11**, 063023 (2009)
  - O. V. Pilyavets, V. G. Zborovskii, and S. Mancini, *Phys. Rev.* A **77**, 052324 (2008)

- 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:

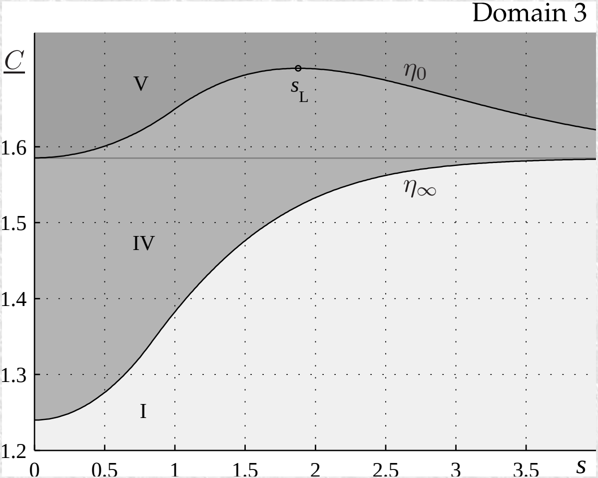


- Domain 2 is the range of channel parameters $(N, \mathcal{N}_{\text{env}})$ where the capacity as a function of squeezing s has the following *five* types of behaviour that depend on the value of transmissivity η:

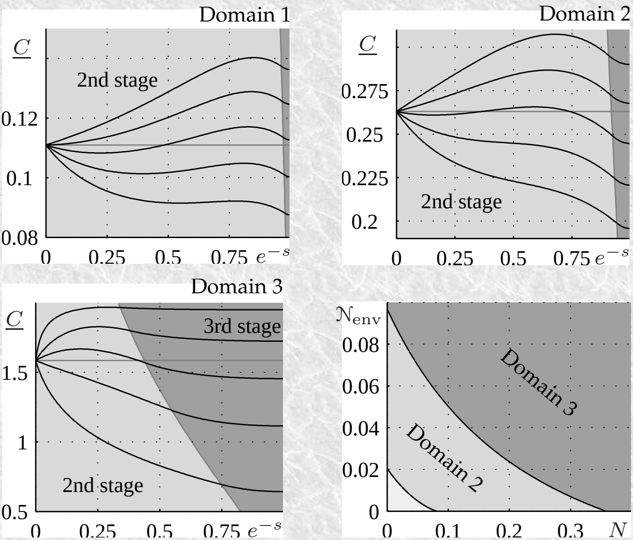


Classical capacity of single-mode LBC: graph for domain 3

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



Capacity (1-mode LBC): graphs for all domains and the domains themselves



Classical capacity of single-mode LBC: 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:

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

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

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

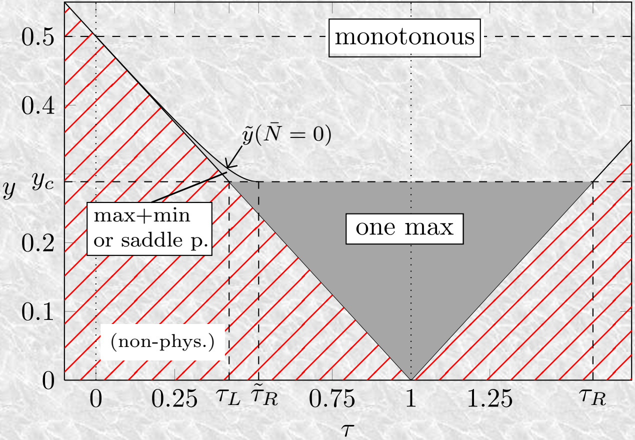
  In particular, the parameters $(N, \mathcal{N}_{\rm env})$ defined by the first two inequalities belong to the third domain

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

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

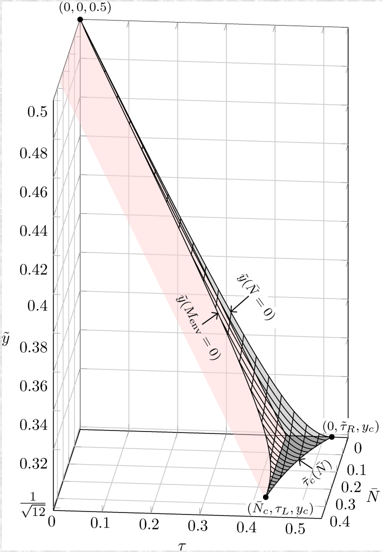
- For $N \to \infty$ the equality $C(s = 0) = C(s \to \infty)$ is possible only if

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



J. Schäfer, E. Karpov, O. V. Pilyavets, and N. J. Cerf: to be published

Classical capacity: the case of general Gaussian quantum channel



J. Schäfer, E. Karpov, O. V. Pilyavets, and N. J. Cerf: to be published thank you!