# Exact solution for the quantum and private capacities of bosonic dephasing channels

Ludovico Lami*, and Mark M. Wilde†°

arXiv:2205.05736

*University of Ulm, Germany

†Louisiana State University, LA, USA
°Cornell University, NY, USA

Unterstützt von / Supported by

Alexander von Humboldt
Stiftung/Foundation

# Quantum states & channels

# Quantum states & channels

Single harmonic oscillator (a.k.a. single mode):

$\mathcal{H} \simeq L^2(\mathbb{R}) \simeq \ell^2(\mathbb{N})$ spanned by Fock basis $|0\rangle$, $|1\rangle$, $|2\rangle$, etc.

# Quantum states & channels

Single harmonic oscillator (a.k.a. single mode):
$\mathcal{H} \simeq L^2(\mathbb{R}) \simeq \ell^2(\mathbb{N})$ spanned by Fock basis $|0\rangle$, $|1\rangle$, $|2\rangle$, etc.

Density operator $\rho \longrightarrow$ infinite matrix (in Fock basis)

$$\rho = \begin{pmatrix} \rho_{00} & \rho_{01} & \rho_{02} & \cdots \\ \rho_{01}^* & \rho_{11} & \rho_{12} & \cdots \\ \rho_{02}^* & \rho_{12}^* & \rho_{22} & \\ \vdots & & & \ddots \end{pmatrix} \tag{1}$$

Quantum channels:

- Model transformations undergone by open quantum systems:

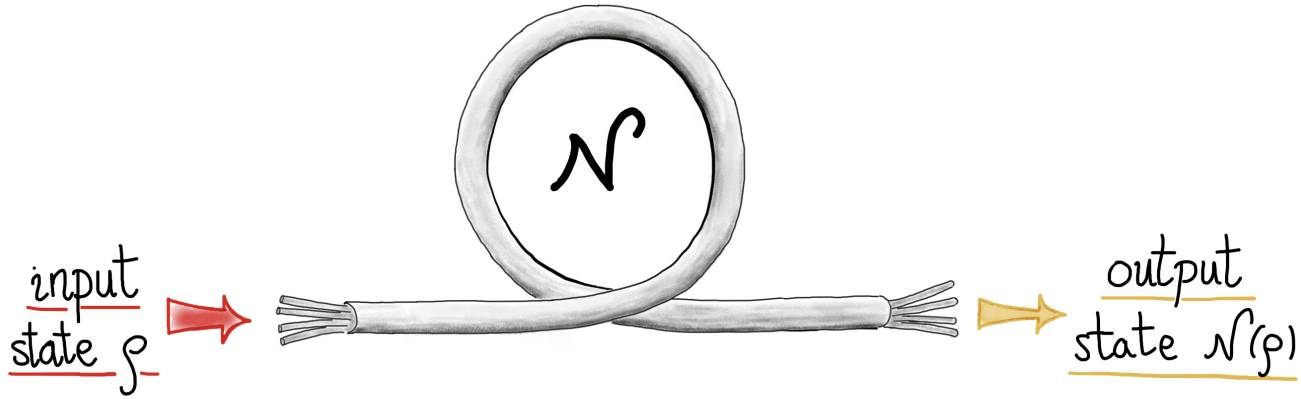
$$\mathscr{N}(\rho_S) := \mathrm{Tr}_E \left[ U_{SE} \left( \rho_S \otimes |0\rangle\langle 0|_E \right) U_{SE}^\dagger \right], \tag{2}$$

Quantum channels:

- Model transformations undergone by open quantum systems:

$$\mathcal{N}(\rho_S) := \mathrm{Tr}_E \left[ U_{SE} \left( \rho_S \otimes |0\rangle\langle 0|_E \right) U_{SE}^\dagger \right], \tag{2}$$

e.g. travelling across an optical fibre:

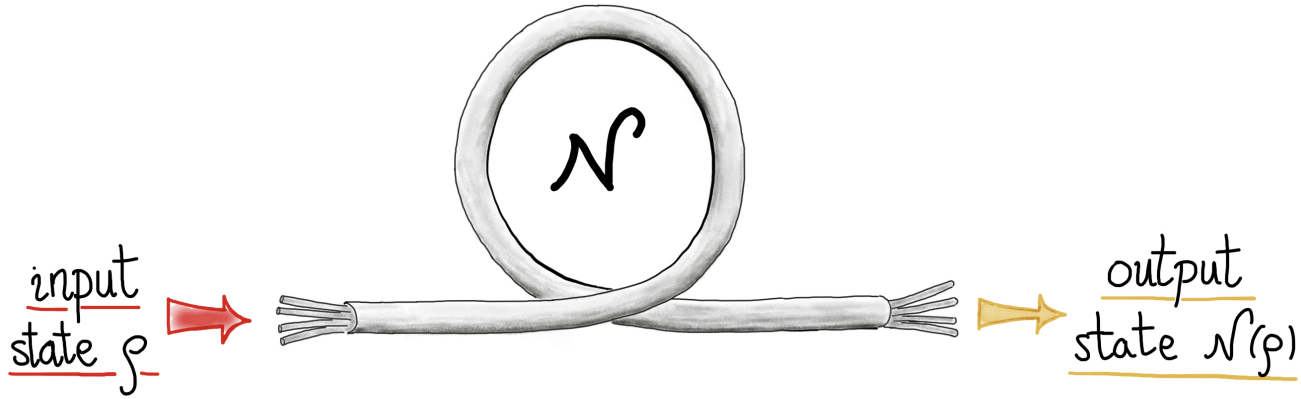


Quantum channels:

- Model transformations undergone by open quantum systems:

$$\mathcal{N}(\rho_S) := \mathrm{Tr}_E \left[ U_{SE} \left( \rho_S \otimes |0\rangle\langle 0|_E \right) U_{SE}^\dagger \right], \tag{2}$$

  e.g. travelling across an optical fibre:




- Kraus representation

$$\mathcal{N}(\rho) = \sum_k M_k \rho M_k^\dagger; \tag{3}$$

  normalisation requires $\sum_k M_k^\dagger M_k = \mathbb{1}$.

# Our model

## Bosonic dephasing channel

Single mode with phase uncertainty:

$$\mathcal{N}_p(\rho) := \int_{-\pi}^{\pi} d\phi \; p(\phi) \; e^{-i\, a^\dagger a\, \phi} \rho \, e^{i\, a^\dagger a\, \phi}, \tag{4}$$

$p : [-\pi, \pi] \to \mathbb{R}_+$ probability distribution, $a^\dagger a$ number operator.

# Our model

## Bosonic dephasing channel

Single mode with phase uncertainty:

$$\mathcal{N}_p(\rho) := \int_{-\pi}^{\pi} d\phi \; p(\phi) \; e^{-i\, a^\dagger a\, \phi} \rho \, e^{i\, a^\dagger a\, \phi}, \tag{4}$$

$p : [-\pi, \pi] \to \mathbb{R}_+$ probability distribution, $a^\dagger a$ number operator.

Models phase fluctuations in the fibre $\longrightarrow$ temperature variations, path length imprecisions, ...

# Our model

## Bosonic dephasing channel

Single mode with phase uncertainty:

$$\mathcal{N}_p(\rho) := \int_{-\pi}^{\pi} d\phi \; p(\phi) \; e^{-i\, a^\dagger a\, \phi} \rho \, e^{i\, a^\dagger a\, \phi}, \tag{4}$$

$p : [-\pi, \pi] \to \mathbb{R}_+$ probability distribution, $a^\dagger a$ number operator.

Models phase fluctuations in the fibre $\longrightarrow$ temperature variations, path length imprecisions, ...

$\mathcal{N}_p$ is <u>not</u> a Gaussian channel!

# Our model

## Bosonic dephasing channel

Single mode with phase uncertainty:

$$\mathscr{N}_p(\rho) := \int_{-\pi}^{\pi} d\phi \; p(\phi) \; e^{-i\, a^\dagger a\, \phi} \rho \, e^{i\, a^\dagger a\, \phi}, \tag{4}$$

$p : [-\pi, \pi] \to \mathbb{R}_+$ probability distribution, $a^\dagger a$ number operator.

Models phase fluctuations in the fibre $\longrightarrow$ temperature variations, path length imprecisions, ...

$\mathscr{N}_p$ is <u>not</u> a Gaussian channel!

**Example.** Wrapped Gaussian:[1] $p_\gamma(\phi) := \dfrac{1}{\sqrt{2\pi\gamma}} \displaystyle\sum_{k=-\infty}^{+\infty} e^{-\frac{1}{2\gamma}(\phi+2\pi k)^2}$.

[1] AMM, *Phys. Rev. A* 102:042413, 2020.

Fock basis representation:

$$\mathscr{N}_p(|n\rangle\langle m|) = \int_{-\pi}^{\pi} d\phi \; p(\phi) \; e^{-i\, a^\dagger a\, \phi} \, |n\rangle\langle m| \; e^{i\, a^\dagger a\, \phi}$$

Fock basis representation:

$$\mathcal{N}_p(|n\rangle\langle m|) = \int_{-\pi}^{\pi} d\phi \; p(\phi) \; e^{-i\, a^\dagger a\, \phi} \, |n\rangle\langle m| \; e^{i\, a^\dagger a\, \phi}$$
$$= \left( \int_{-\pi}^{\pi} d\phi \; p(\phi) \; e^{-i\,(n-m)\phi} \right) |n\rangle\langle m|$$

Fock basis representation:

$$\begin{aligned}\mathcal{N}_p(|n\rangle\langle m|) &= \int_{-\pi}^{\pi} d\phi\ p(\phi)\ e^{-i\, a^\dagger a\, \phi}\, |n\rangle\langle m|\ e^{i\, a^\dagger a\, \phi} \\ &= \left( \int_{-\pi}^{\pi} d\phi\ p(\phi)\ e^{-i\,(n-m)\phi} \right) |n\rangle\langle m| \\ &=: (T_p)_{nm}\, |n\rangle\langle m|\end{aligned}$$

Fock basis representation:

$$\begin{aligned}\mathscr{N}_p(|n\rangle\langle m|) &= \int_{-\pi}^{\pi} d\phi\ p(\phi)\ e^{-i\,a^\dagger a\,\phi}\,|n\rangle\langle m|\ e^{i\,a^\dagger a\,\phi} \\ &= \left(\int_{-\pi}^{\pi} d\phi\ p(\phi)\ e^{-i\,(n-m)\phi}\right)|n\rangle\langle m| \\ &=: (T_p)_{nm}\,|n\rangle\langle m|\end{aligned}$$

$$\implies \mathscr{N}_p(\rho) = \begin{pmatrix} \rho_{00}\,(T_p)_{00} & \rho_{01}\,(T_p)_{01} & \cdots \\ \rho_{01}^*\,(T_p)_{01}^* & \rho_{11}\,(T_p)_{11} & \cdots \\ \vdots & & \ddots \end{pmatrix} = \boldsymbol{\rho \circ T_p}\,,$$

Fock basis representation:

$$\begin{aligned}\mathscr{N}_p(|n\rangle\langle m|) &= \int_{-\pi}^{\pi} d\phi\ p(\phi)\ e^{-i\,a^\dagger a\,\phi}\,|n\rangle\langle m|\ e^{i\,a^\dagger a\,\phi} \\ &= \left(\int_{-\pi}^{\pi} d\phi\ p(\phi)\ e^{-i\,(n-m)\phi}\right)|n\rangle\langle m| \\ &=: (T_p)_{nm}\,|n\rangle\langle m|\end{aligned}$$

$$\implies \mathscr{N}_p(\rho) = \begin{pmatrix} \rho_{00}\,(T_p)_{00} & \rho_{01}\,(T_p)_{01} & \cdots \\ \rho_{01}^*\,(T_p)_{01}^* & \rho_{11}\,(T_p)_{11} & \cdots \\ \vdots & & \ddots \end{pmatrix} = \boldsymbol{\rho \circ T_p}\,,$$

$\boldsymbol{X \circ Y}$ = Hadamard product = entry-wise product.

Fock basis representation:

$$\begin{aligned}\mathscr{N}_p(|n\rangle\langle m|) &= \int_{-\pi}^{\pi} d\phi\; p(\phi)\; e^{-i\, a^\dagger a\, \phi}\, |n\rangle\langle m|\; e^{i\, a^\dagger a\, \phi} \\ &= \left(\int_{-\pi}^{\pi} d\phi\; p(\phi)\; e^{-i\,(n-m)\phi}\right) |n\rangle\langle m| \\ &=: (T_p)_{nm}\, |n\rangle\langle m|\end{aligned}$$

$$\implies \mathscr{N}_p(\rho) = \begin{pmatrix} \rho_{00}\,(T_p)_{00} & \rho_{01}\,(T_p)_{01} & \cdots \\ \rho_{01}^*\,(T_p)_{01}^* & \rho_{11}\,(T_p)_{11} & \cdots \\ \vdots & & \ddots \end{pmatrix} = \boldsymbol{\rho \circ T_p}\,,$$

$\boldsymbol{X \circ Y}$ = Hadamard product = entry-wise product.

**Note:** $T_p$ is a Toeplitz matrix, i.e. $(T_p)_{nm} = f(n-m)$.

Fock basis representation:

$$\begin{aligned}\mathcal{N}_p(|n\rangle\langle m|) &= \int_{-\pi}^{\pi} d\phi\ p(\phi)\ e^{-i\,a^\dagger a\,\phi}\,|n\rangle\langle m|\ e^{i\,a^\dagger a\,\phi} \\ &= \left(\int_{-\pi}^{\pi} d\phi\ p(\phi)\ e^{-i\,(n-m)\phi}\right)|n\rangle\langle m| \\ &=: (T_p)_{nm}\,|n\rangle\langle m|\end{aligned}$$

$$\implies \mathcal{N}_p(\rho) = \begin{pmatrix} \rho_{00}\,(T_p)_{00} & \rho_{01}\,(T_p)_{01} & \cdots \\ \rho_{01}^*\,(T_p)_{01}^* & \rho_{11}\,(T_p)_{11} & \cdots \\ \vdots & & \ddots \end{pmatrix} = \boldsymbol{\rho \circ T_p}\,,$$

$\boldsymbol{X \circ Y}$ = Hadamard product = entry-wise product.

**Note:** $T_p$ is a Toeplitz matrix, i.e. $(T_p)_{nm} = f(n-m)$.

**Example.** Wrapped Gaussian: $(T_{p_\gamma})_{nm} = e^{-\frac{\gamma}{2}(n-m)^2}$.

# The capacity zoo

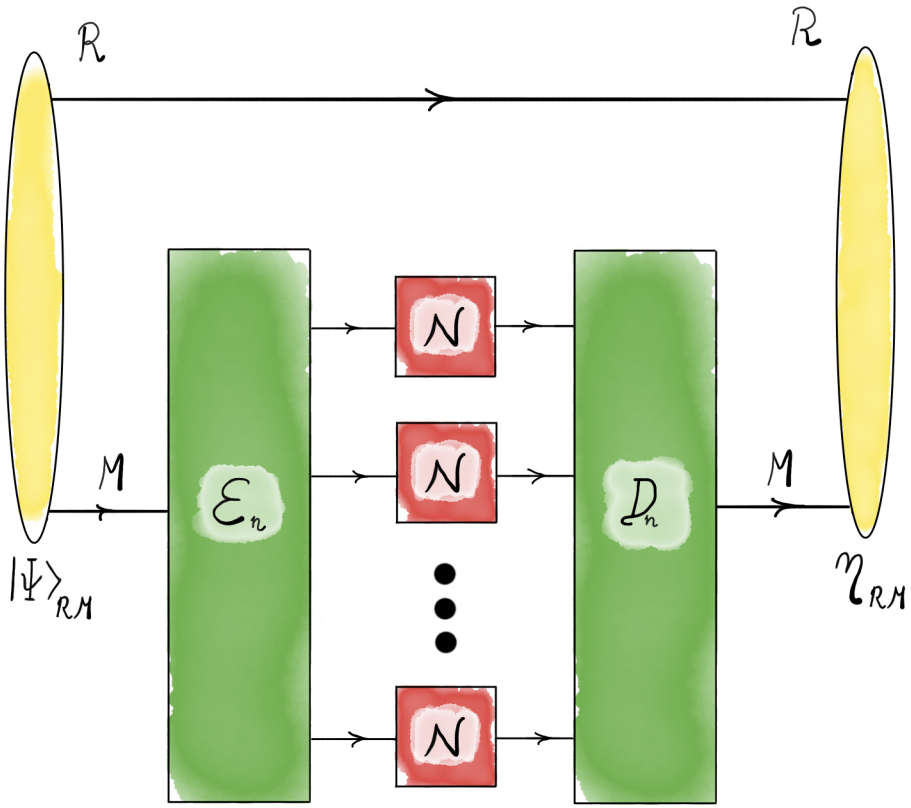
We want to use $\mathscr{N}$ to:

1. send qubits $\longrightarrow$ quantum capacity $Q(\mathscr{N})$

# The capacity zoo

We want to use $\mathcal{N}$ to:

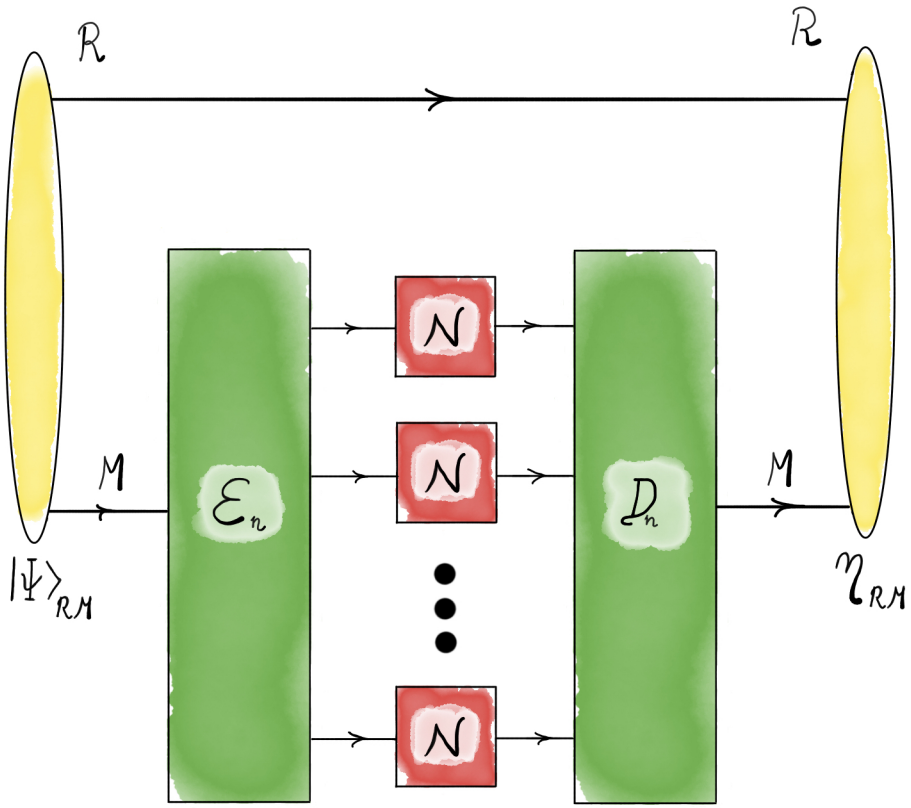
1. send qubits $\longrightarrow$ quantum capacity $Q(\mathcal{N})$



# The capacity zoo

We want to use $\mathcal{N}$ to:

1. send qubits $\longrightarrow$ quantum capacity $Q(\mathcal{N})$

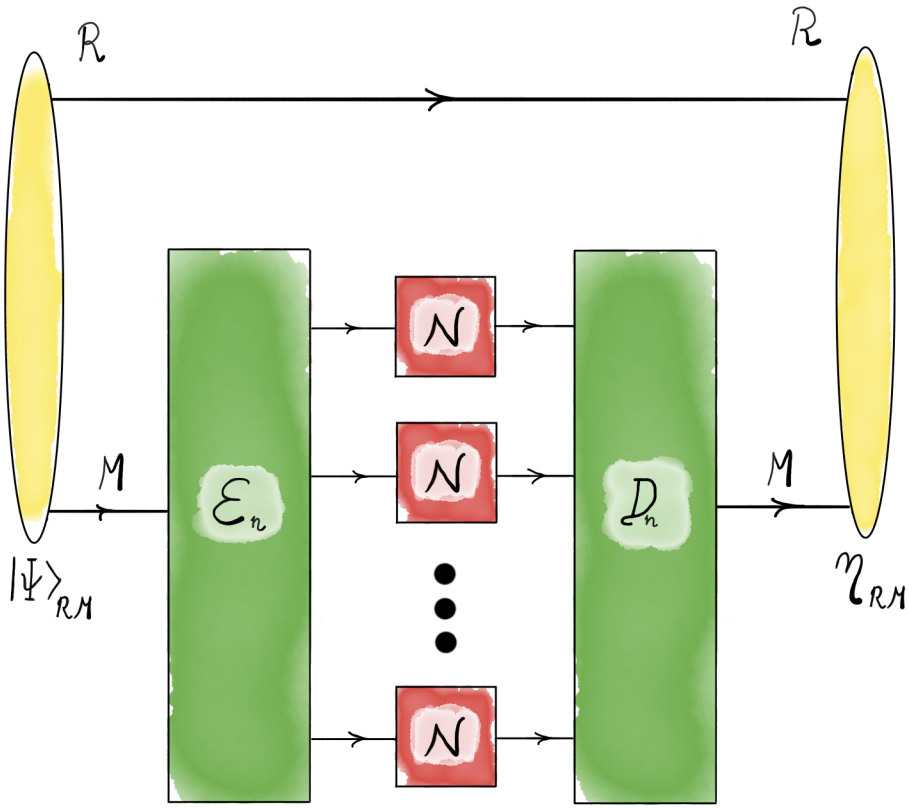



$M$ = transmitted system
$R$ = reference system

# The capacity zoo

We want to use $\mathcal{N}$ to:

1. send qubits $\longrightarrow$ quantum capacity $Q(\mathcal{N})$



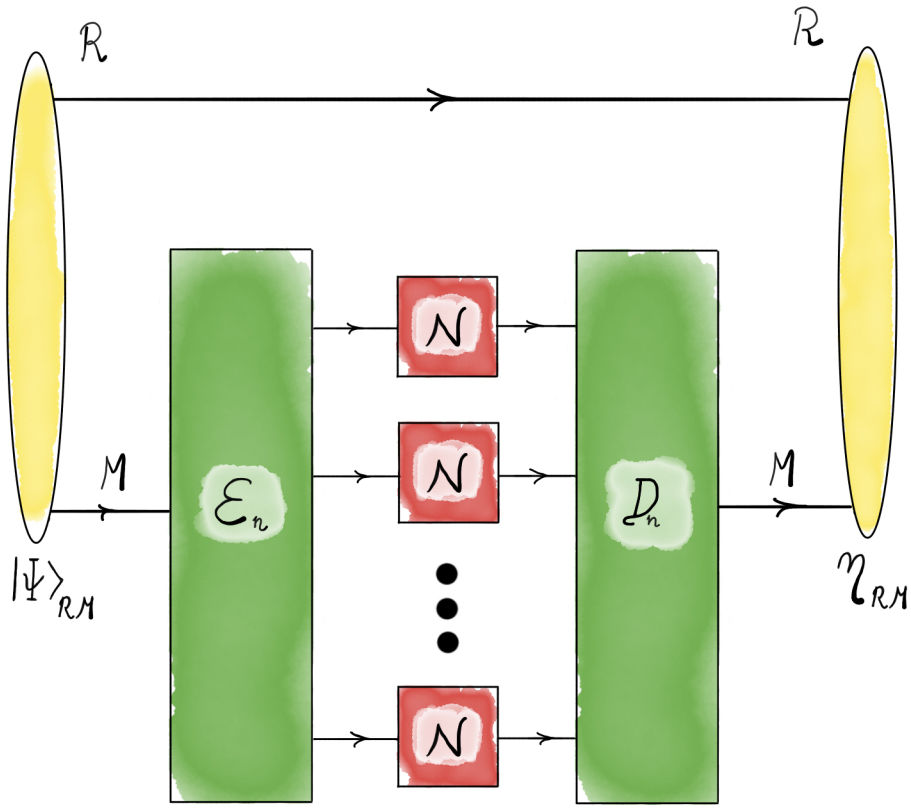

$M$ = transmitted system
$R$ = reference system

$\mathcal{E}_n, \mathcal{D}_n$ = encoding, decoding

# The capacity zoo

We want to use $\mathcal{N}$ to:

1. send qubits $\longrightarrow$ quantum capacity $Q(\mathcal{N})$




$M$ = transmitted system
$R$ = reference system

$\mathcal{E}_n, \mathcal{D}_n$ = encoding, decoding

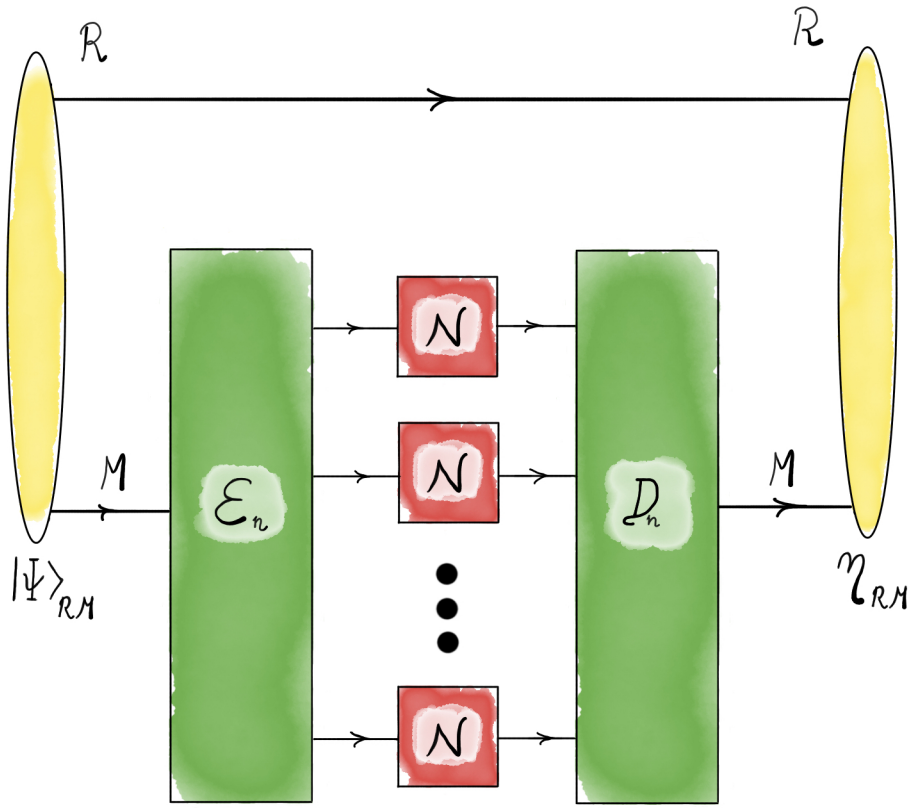
$n$ uses of $\mathcal{N}$

transmission successful if
$\eta_{RM} \approx_{\varepsilon_n} |\Psi\rangle\langle\Psi|_{RM}$, with
$\varepsilon_n \xrightarrow[n\to\infty]{} 0$ ✓

# The capacity zoo

We want to use $\mathcal{N}$ to:

1. send qubits $\longrightarrow$ quantum capacity $Q(\mathcal{N})$




$M$ = transmitted system
$R$ = reference system

$\mathcal{E}_n, \mathcal{D}_n$ = encoding, decoding

$n$ uses of $\mathcal{N}$

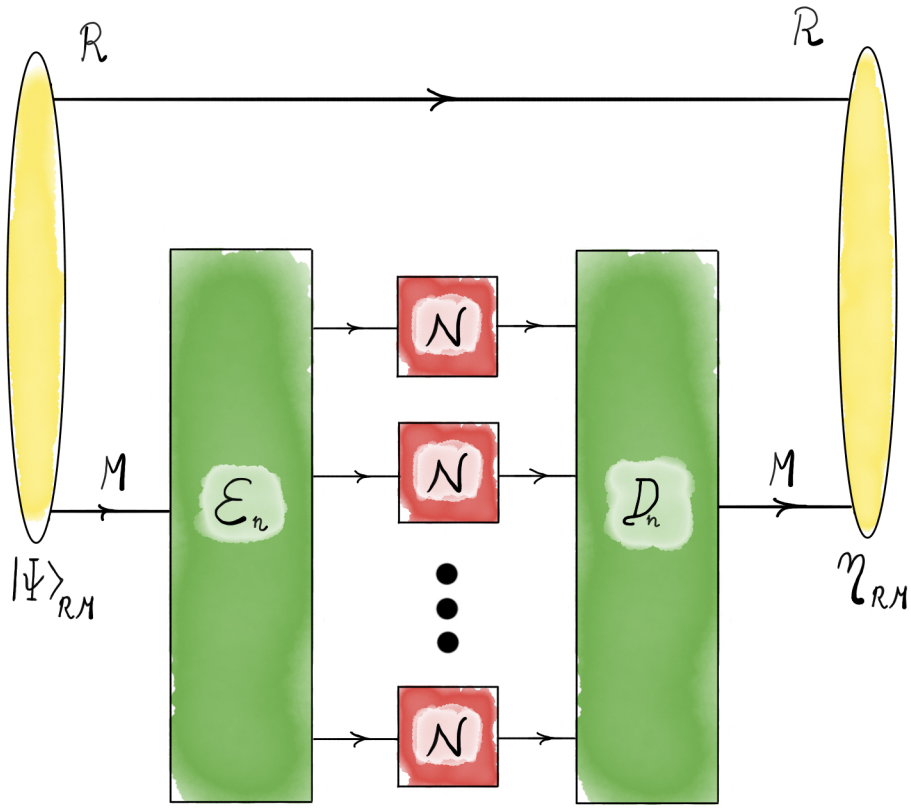
transmission successful if
$\eta_{RM} \approx_{\varepsilon_n} |\Psi\rangle\langle\Psi|_{RM}$, with
$\varepsilon_n \xrightarrow[n\to\infty]{} 0$ ✓

# qubits sent per channel use
$= \frac{1}{n} \log_2 \dim \mathcal{H}_M =$ **rate** $R$

# The capacity zoo

We want to use $\mathcal{N}$ to:

1. send qubits $\longrightarrow$ quantum capacity $Q(\mathcal{N})$




$M$ = transmitted system
$R$ = reference system

$\mathcal{E}_n, \mathcal{D}_n$ = encoding, decoding

$n$ uses of $\mathcal{N}$

transmission successful if
$\eta_{RM} \approx_{\varepsilon_n} |\Psi\rangle\langle\Psi|_{RM}$, with
$\varepsilon_n \xrightarrow[n\to\infty]{} 0$ ✓

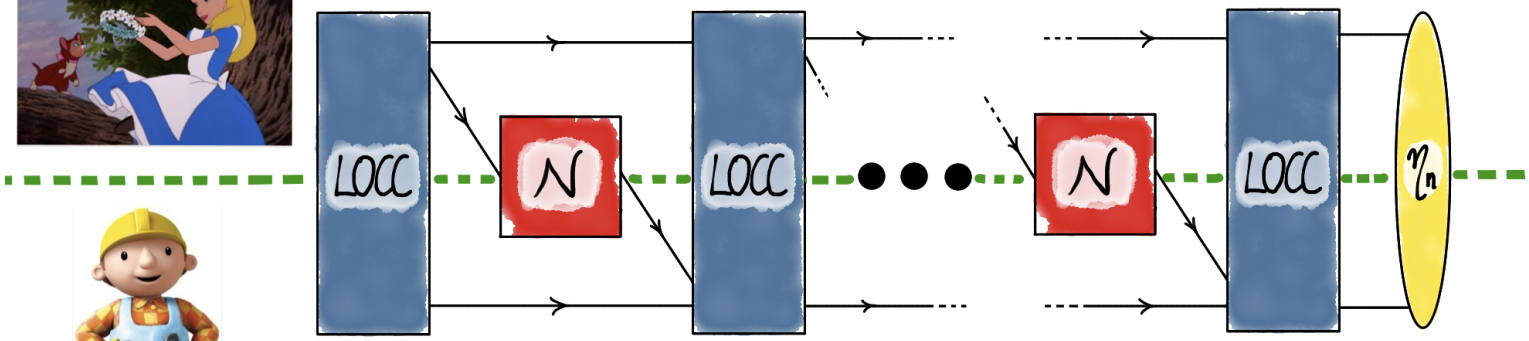
# qubits sent per channel use
$= \frac{1}{n} \log_2 \dim \mathcal{H}_M =$ **rate** $R$

Quantum capacity $= Q(\mathcal{N}) := \sup\{\text{achievable rates } R\}$.

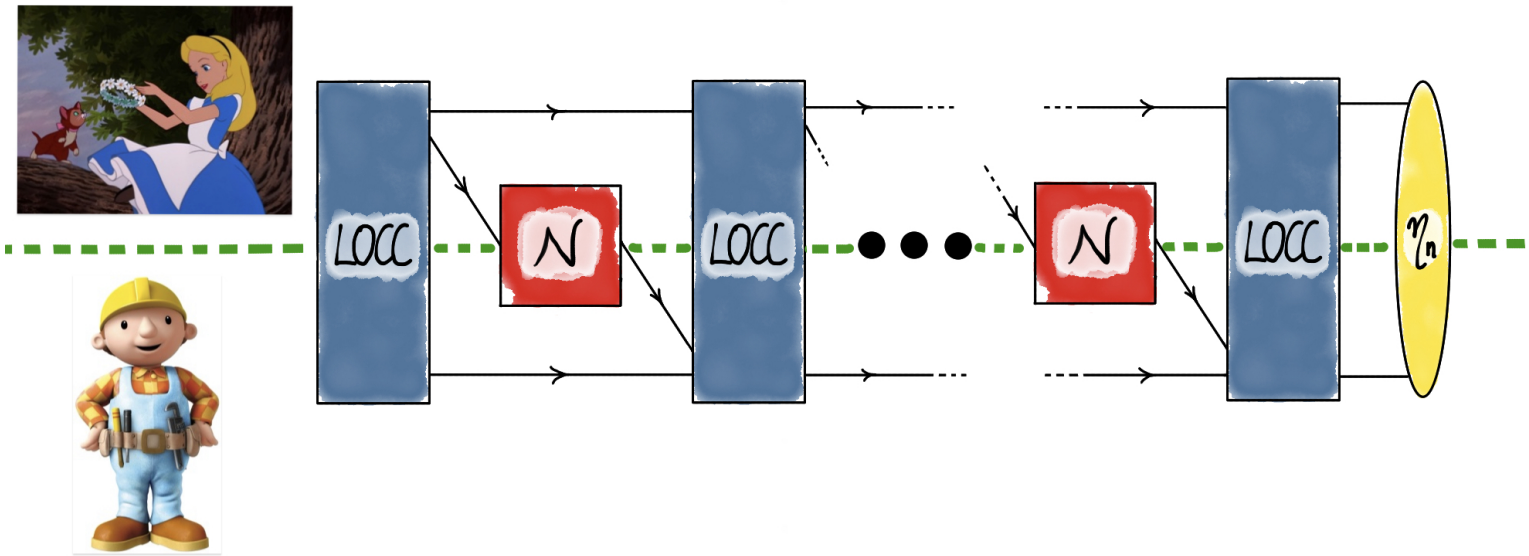
2 establish long-distance entanglement
$\longrightarrow$ two-way–assisted quantum capacity $Q_{\leftrightarrow}(\mathcal{N})$.

2 establish long-distance entanglement

$\longrightarrow$ two-way–assisted quantum capacity $Q_{\leftrightarrow}(\mathcal{N})$.

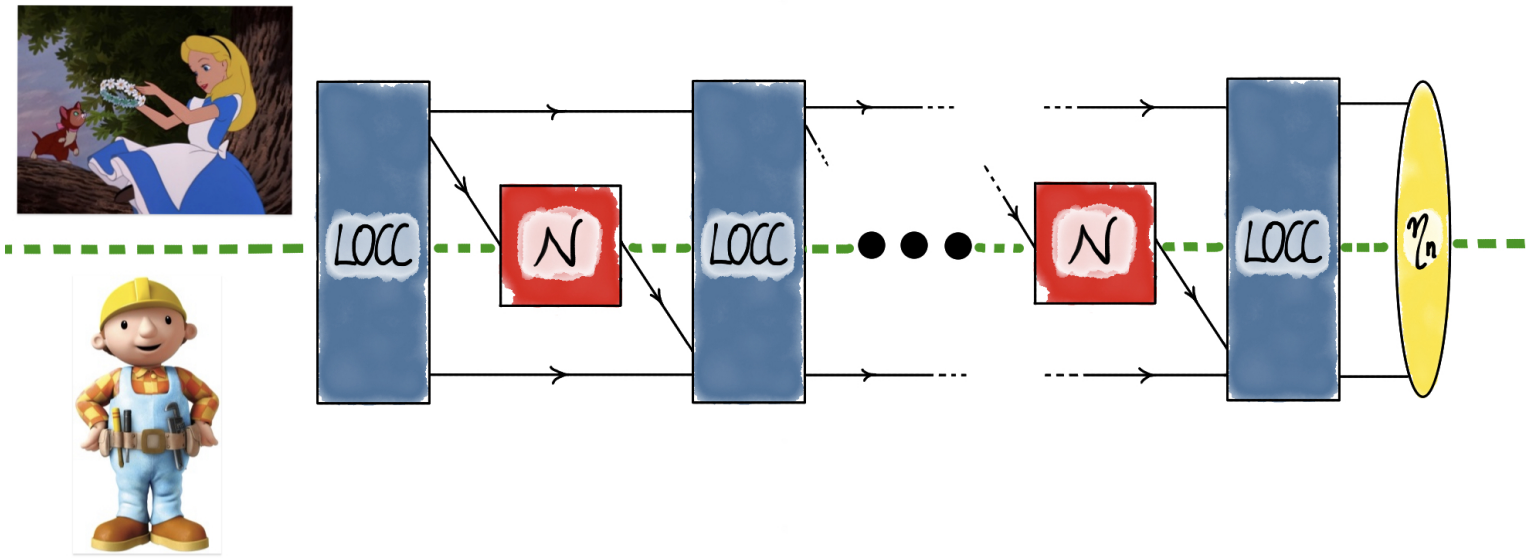


2 establish long-distance entanglement
$\longrightarrow$ two-way–assisted quantum capacity $Q_{\leftrightarrow}(\mathcal{N})$.




Alice and Bob are spatially separated, $n$ uses of $\mathcal{N}_{A\to B}$;

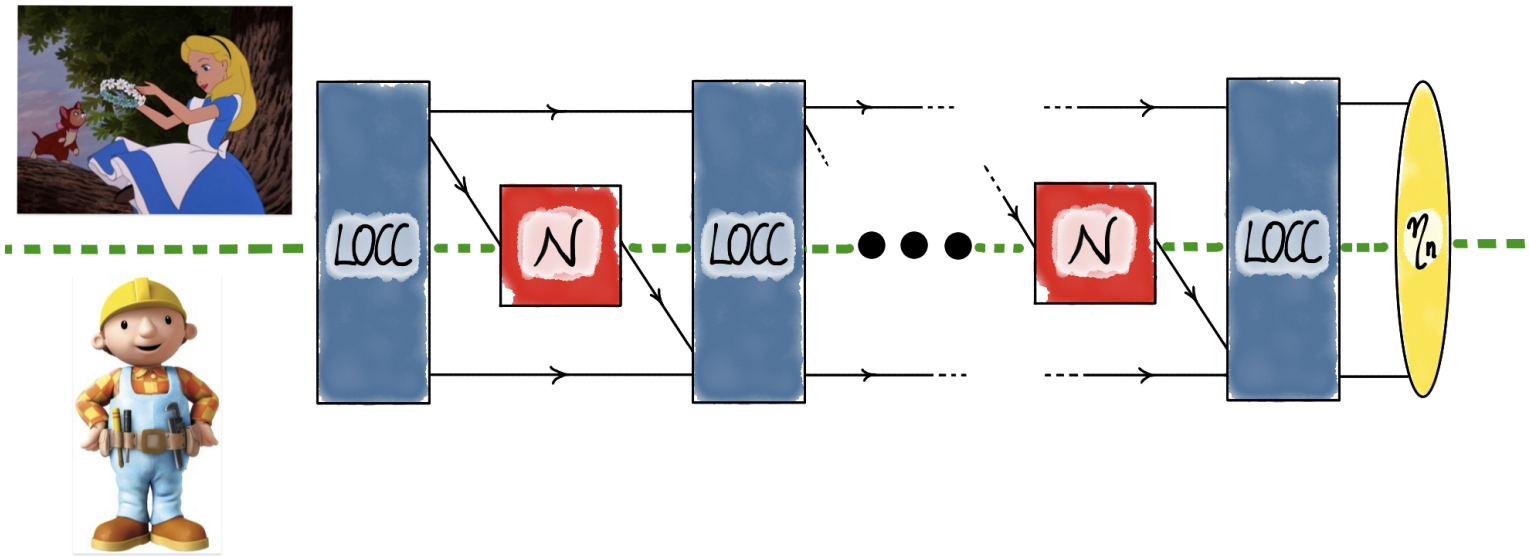
2 establish long-distance entanglement
$\longrightarrow$ two-way–assisted quantum capacity $Q_{\leftrightarrow}(\mathcal{N})$.




Alice and Bob are spatially separated, $n$ uses of $\mathcal{N}_{A\to B}$;

in between local operations and classical communication (LOCC);

2 establish long-distance entanglement
$\longrightarrow$ two-way–assisted quantum capacity $Q_{\leftrightarrow}(\mathcal{N})$.

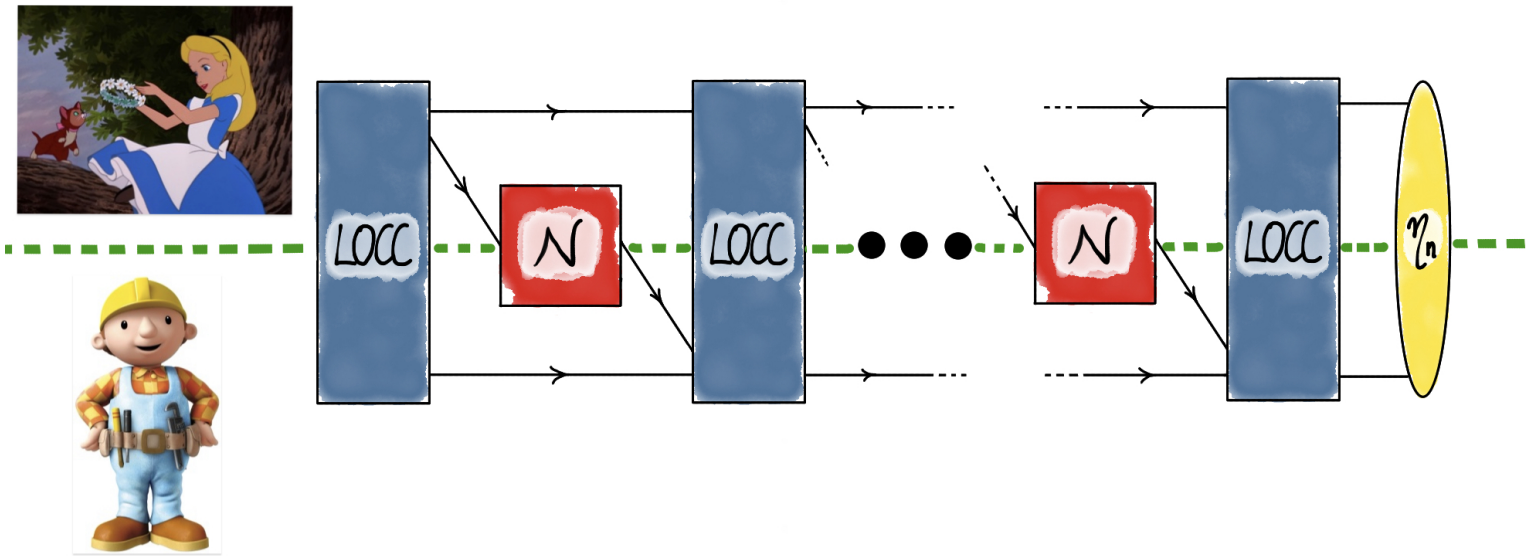



Alice and Bob are spatially separated, $n$ uses of $\mathcal{N}_{A\to B}$;

in between local operations and classical communication (LOCC);

protocol successful if $\eta_n \approx_{\varepsilon_n} \Phi_2^{\otimes\lceil Rn\rceil}$, $\varepsilon_n \xrightarrow[n\to\infty]{} 0$, where $\Phi_2$ single ebit.

2 establish long-distance entanglement
$\longrightarrow$ two-way–assisted quantum capacity $Q_{\leftrightarrow}(\mathcal{N})$.




Alice and Bob are spatially separated, $n$ uses of $\mathcal{N}_{A\to B}$;

in between local operations and classical communication (LOCC);

protocol successful if $\eta_n \approx_{\varepsilon_n} \Phi_2^{\otimes\lceil Rn\rceil}$, $\varepsilon_n \xrightarrow[n\to\infty]{} 0$, where $\Phi_2$ single ebit.

Two-way quantum capacity $= Q_{\leftrightarrow}(\mathcal{N}) := \sup\{\text{achievable rates } R\}$.

Also: private capacity $P(\mathscr{N})$, two-way private capacity $P_{\leftrightarrow}(\mathscr{N})$;

Also: private capacity $P(\mathcal{N})$, two-way private capacity $P_{\leftrightarrow}(\mathcal{N})$;

$+$ strong converse exponents $Q^{\dagger}(\mathcal{N})$, $Q^{\dagger}_{\leftrightarrow}(\mathcal{N})$, $P^{\dagger}(\mathcal{N})$, $P^{\dagger}_{\leftrightarrow}(\mathcal{N})$
($\limsup_{n\to\infty} \varepsilon_n < 1$ instead of $\lim_{n\to\infty} \varepsilon_n = 0$).

Also: private capacity $P(\mathcal{N})$, two-way private capacity $P_{\leftrightarrow}(\mathcal{N})$;

+ strong converse exponents $Q^{\dagger}(\mathcal{N})$, $Q^{\dagger}_{\leftrightarrow}(\mathcal{N})$, $P^{\dagger}(\mathcal{N})$, $P^{\dagger}_{\leftrightarrow}(\mathcal{N})$ ($\limsup_{n\to\infty} \varepsilon_n < 1$ instead of $\lim_{n\to\infty} \varepsilon_n = 0$).

**Problem**[2]

Compute $\mathscr{C}(\mathcal{N}_p)$, for $\mathscr{C} = Q, Q_{\leftrightarrow}, P, P_{\leftrightarrow}, Q^{\dagger}, Q^{\dagger}_{\leftrightarrow}, P^{\dagger}, P^{\dagger}_{\leftrightarrow}$.

[2] Jiang and Chen, *in Quantum and Nonlinear Optics* 7846:244, 2010. AMM, *Phys. Rev. A* 102:042413, 2020.

# Main result

**Theorem**

*For* $\mathscr{C} = Q, Q_{\leftrightarrow}, P, P_{\leftrightarrow}, Q^{\dagger}, Q^{\dagger}_{\leftrightarrow}, P^{\dagger}, P^{\dagger}_{\leftrightarrow}$ *and any* $p$ *such that*

$$\int_{-\pi}^{+\pi} d\phi \; p(\phi)^{\alpha_0} < \infty \tag{5}$$

*for some* $\alpha_0 > 1$,

$$\mathscr{C}(\mathscr{N}_p) = \log_2(2\pi) - h(p)\,, \tag{6}$$

*where* $h(p) := -\int_{-\pi}^{\pi} d\phi \; p(\phi) \log_2 p(\phi)$ *is the differential entropy of the probability density* $p$.

# Main result

**Theorem**

*For* $\mathscr{C} = Q, Q_{\leftrightarrow}, P, P_{\leftrightarrow}, Q^{\dagger}, Q^{\dagger}_{\leftrightarrow}, P^{\dagger}, P^{\dagger}_{\leftrightarrow}$ *and any* $p$ *such that*

$$\int_{-\pi}^{+\pi} d\phi \; p(\phi)^{\alpha_0} < \infty \tag{5}$$

*for some* $\alpha_0 > 1$,

$$\mathscr{C}(\mathscr{N}_p) = \log_2(2\pi) - h(p)\,, \tag{6}$$

*where* $h(p) := -\int_{-\pi}^{\pi} d\phi \; p(\phi) \log_2 p(\phi)$ *is the differential entropy of the probability density* $p$.

- Unlimited classical communication between sender and receiver does not enhance capacities!

# Main result

**Theorem**

*For* $\mathscr{C} = Q, Q_{\leftrightarrow}, P, P_{\leftrightarrow}, Q^{\dagger}, Q^{\dagger}_{\leftrightarrow}, P^{\dagger}, P^{\dagger}_{\leftrightarrow}$ *and any* $p$ *such that*

$$\int_{-\pi}^{+\pi} d\phi \; p(\phi)^{\alpha_0} < \infty \tag{5}$$

*for some* $\alpha_0 > 1$,

$$\mathscr{C}(\mathscr{N}_p) = \log_2(2\pi) - h(p)\,, \tag{6}$$

*where* $h(p) := -\int_{-\pi}^{\pi} d\phi \; p(\phi) \log_2 p(\phi)$ *is the differential entropy of the probability density* $p$.

- Unlimited classical communication between sender and receiver does not enhance capacities!
- Generating entanglement $\simeq$ generating secret key.

# Main result

**Theorem**

*For* $\mathscr{C} = Q, Q_{\leftrightarrow}, P, P_{\leftrightarrow}, Q^{\dagger}, Q^{\dagger}_{\leftrightarrow}, P^{\dagger}, P^{\dagger}_{\leftrightarrow}$ *and any* $p$ *such that*

$$\int_{-\pi}^{+\pi} d\phi \; p(\phi)^{\alpha_0} < \infty \tag{5}$$

*for some* $\alpha_0 > 1$,

$$\mathscr{C}(\mathscr{N}_p) = \log_2(2\pi) - h(p)\,, \tag{6}$$

*where* $h(p) := -\int_{-\pi}^{\pi} d\phi \; p(\phi) \log_2 p(\phi)$ *is the differential entropy of the probability density* $p$.

- Unlimited classical communication between sender and receiver does not enhance capacities!
- Generating entanglement $\simeq$ generating secret key.
- $\mathscr{C}(\mathscr{N}_p) = D(p\|u)$, where $D(p\|q) := \int d\phi \, p(\phi) \log_2 \frac{p(\phi)}{q(\phi)}$, and $u$ uniform on $[-\pi, \pi]$.

- Immediately generalisable to multi-mode case:

- Immediately generalisable to multi-mode case:

$$\mathcal{N}_p(\rho) := \int_{[-\pi,\pi]^m} d^m\mathbf{\Phi}\; p(\mathbf{\Phi})\, e^{-i\sum_j a_j^\dagger a_j \phi_j}\, \rho\, e^{i\sum_j a_j^\dagger a_j \phi_j}. \qquad (7)$$

- Immediately generalisable to multi-mode case:

$$\mathscr{N}_p(\rho) := \int_{[-\pi,\pi]^m} d^m\mathbf{\Phi}\ p(\mathbf{\Phi})\, e^{-i\sum_j a_j^\dagger a_j \phi_j}\, \rho\, e^{i\sum_j a_j^\dagger a_j \phi_j}. \tag{7}$$

Then

$$\mathscr{C}(\mathscr{N}_p) = D(p\|u) = m\log_2(2\pi) - h(p) \tag{8}$$

provided that

$$\int_{[-\pi,\pi]^m} d^m\mathbf{\Phi}\ p(\mathbf{\Phi})^{\alpha_0} < \infty \tag{9}$$

for some $\alpha_0 > 1$.

- Immediately generalisable to multi-mode case:

$$\mathscr{N}_p(\rho) := \int_{[-\pi,\pi]^m} d^m\mathbf{\Phi}\ p(\mathbf{\Phi})\, e^{-i\sum_j a_j^\dagger a_j \phi_j}\, \rho\, e^{i\sum_j a_j^\dagger a_j \phi_j}. \tag{7}$$

Then

$$\mathscr{C}(\mathscr{N}_p) = D(p\|u) = m\log_2(2\pi) - h(p) \tag{8}$$

provided that

$$\int_{[-\pi,\pi]^m} d^m\mathbf{\Phi}\ p(\mathbf{\Phi})^{\alpha_0} < \infty \tag{9}$$

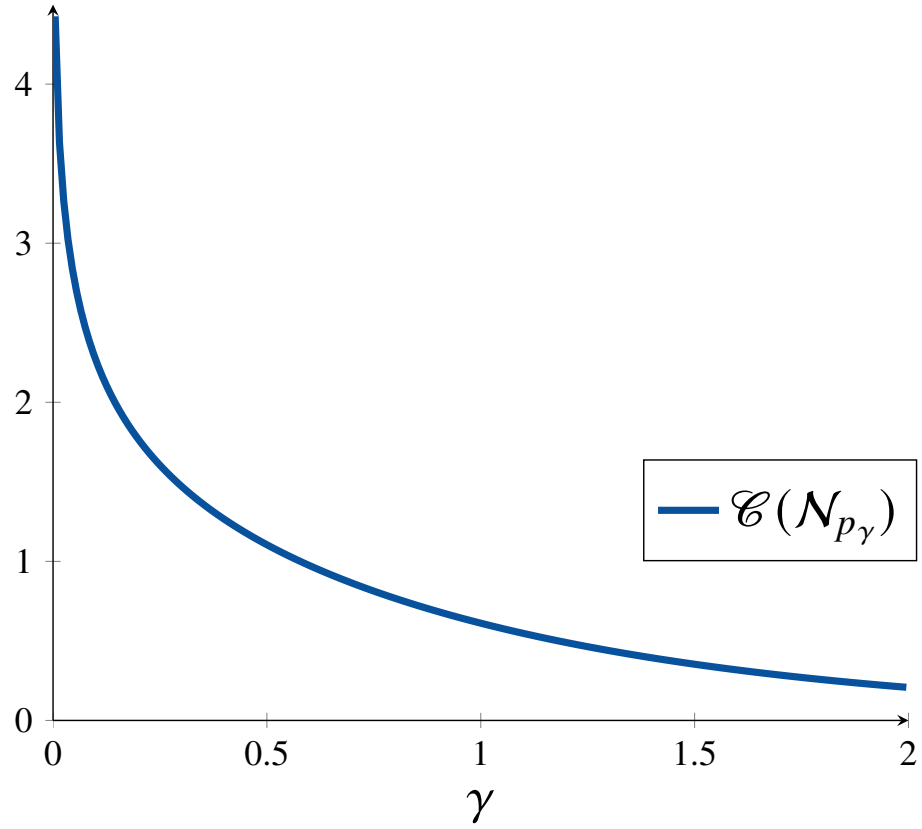
for some $\alpha_0 > 1$.

- Our formula generalises PLOB's formula for finite-dim dephasing channels.[3]

[3] PLOB, *Nat. Commun.* 8:15043, 2017.

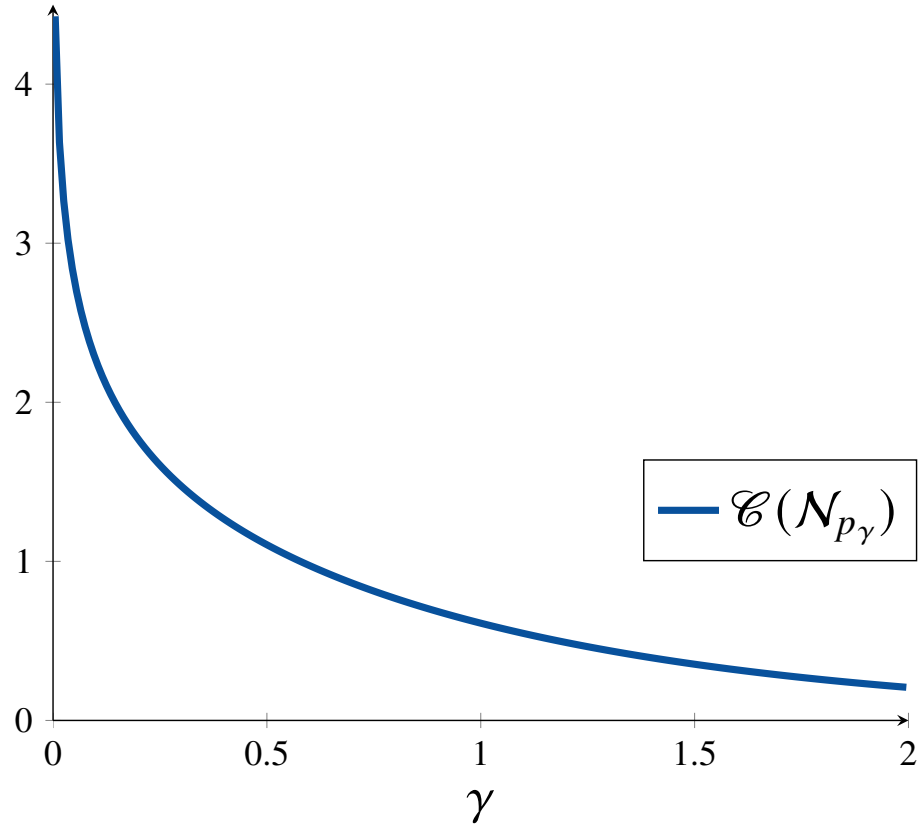
## Example.

Wrapped Gaussian $\mathcal{N}_{p_\gamma}$:



## Example.

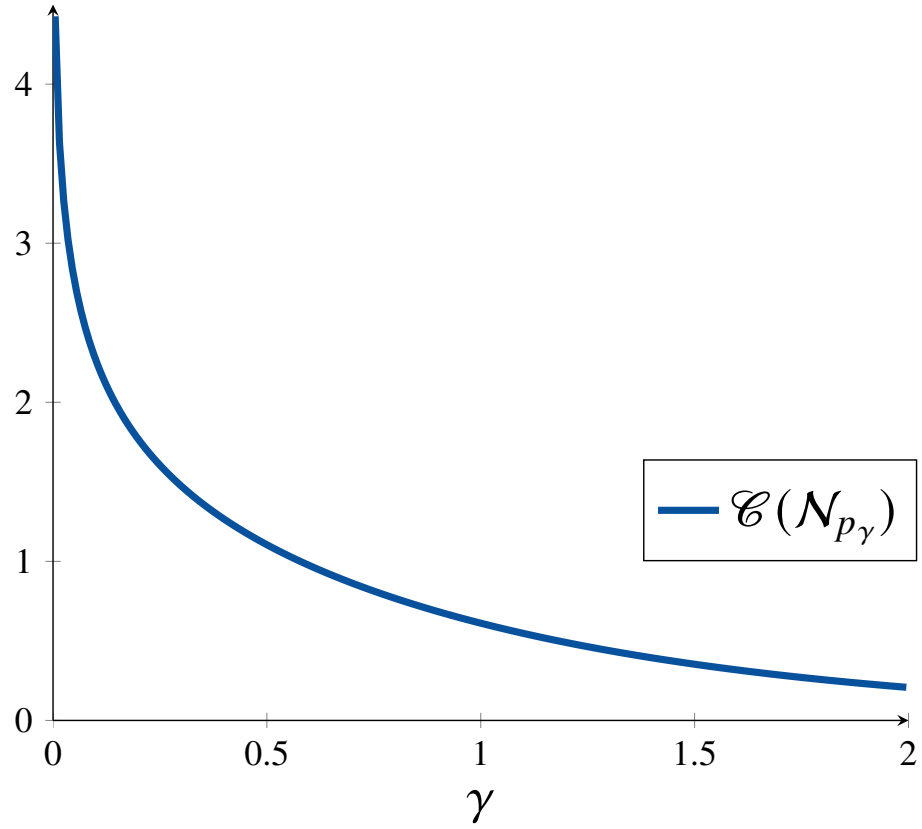
Wrapped Gaussian $\mathcal{N}_{p_\gamma}$:




$$\gamma \lesssim 1 \implies \mathscr{C}(\mathcal{N}_{p_\gamma}) \approx \frac{1}{2} \log_2 \frac{2\pi}{e\gamma}$$

## Example.

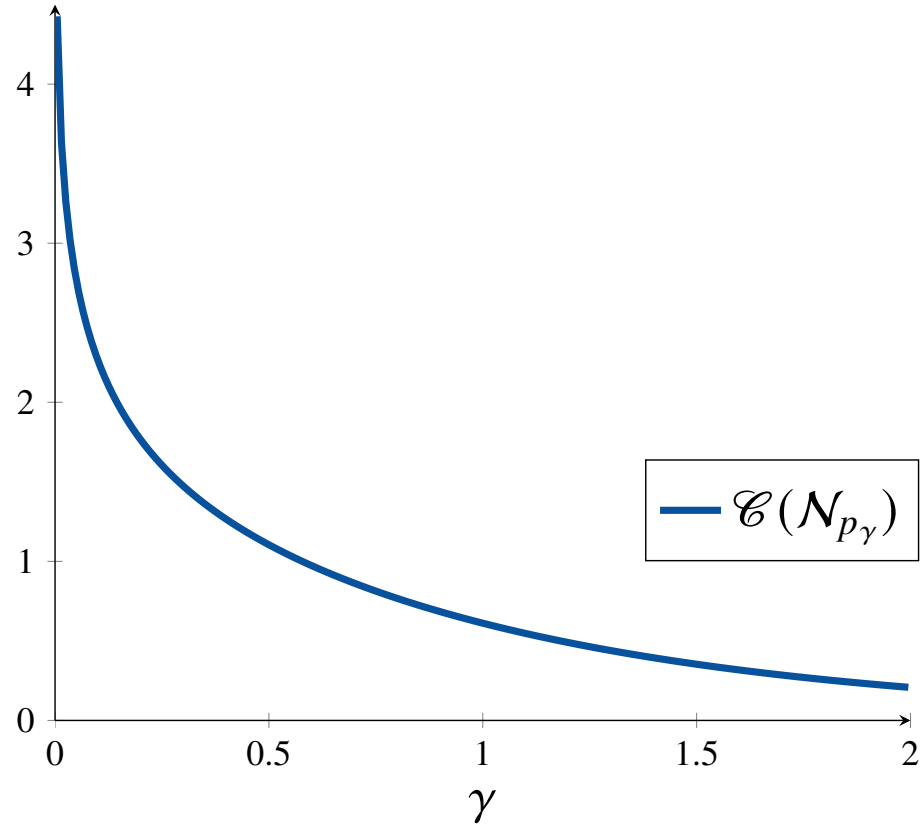
Wrapped Gaussian $\mathcal{N}_{p_\gamma}$:




$$\gamma \lesssim 1 \implies \mathscr{C}(\mathcal{N}_{p_\gamma}) \approx \frac{1}{2}\log_2 \frac{2\pi}{e\gamma} \approx \left(0.6 + \frac{1}{2}\log_2 \frac{1}{\gamma}\right) \text{ bits/channel use},$$

## Example.

Wrapped Gaussian $\mathcal{N}_{p_\gamma}$:




$$\gamma \lesssim 1 \implies \mathscr{C}(\mathcal{N}_{p_\gamma}) \approx \frac{1}{2}\log_2 \frac{2\pi}{e\gamma} \approx \left(0.6 + \frac{1}{2}\log_2 \frac{1}{\gamma}\right) \text{ bits/channel use},$$

$$\gamma \gg 1 \implies \mathscr{C}(\mathcal{N}_{p_\gamma}) \approx \frac{e^{-\gamma}}{\ln 2} \text{ bits/channel use},$$

# Proof ideas

# Proof ideas

To fix ideas: prove that $Q(\mathscr{N}_p) = Q_{\leftrightarrow}(\mathscr{N}_p) = \log_2(2\pi) - h(p)$.

# Proof ideas

To fix ideas: prove that $Q(\mathscr{N}_p) = Q_{\leftrightarrow}(\mathscr{N}_p) = \log_2(2\pi) - h(p)$.

Since $Q(\mathscr{N}_p) \leq Q_{\leftrightarrow}(\mathscr{N}_p)$, we prove that:

a. $Q(\mathscr{N}_p) \geq \log_2(2\pi) - h(p)$;

b. $Q_{\leftrightarrow}(\mathscr{N}_p) \leq \log_2(2\pi) - h(p)$.

# Proof ideas

To fix ideas: prove that $Q(\mathcal{N}_p) = Q_{\leftrightarrow}(\mathcal{N}_p) = \log_2(2\pi) - h(p)$.

Since $Q(\mathcal{N}_p) \leq Q_{\leftrightarrow}(\mathcal{N}_p)$, we prove that:

a. $Q(\mathcal{N}_p) \geq \log_2(2\pi) - h(p)$;

b. $Q_{\leftrightarrow}(\mathcal{N}_p) \leq \log_2(2\pi) - h(p)$.

(a) Lower bound on $Q$ using coherent information (Lloyd–Shor–Devetak theorem):[4]

$$\begin{aligned} Q(\mathcal{N}_p) &\geq \sup_{|\Psi\rangle_{AA'}} I(A\rangle B)_{\mathcal{N}_p^{A'\to B}(\Psi_{AA'})}, \\ I(A\rangle B)_\rho &:= S(\rho_B) - S(\rho_{AB}), \\ S(\omega) &:= -\operatorname{Tr}[\omega \log_2 \omega] \end{aligned} \tag{10}$$

[4] Lloyd, *Phys. Rev. A* 55:1613, 1997. Shor, Lecture notes, 2002. Devetak, *IEEE Trans. Inf. Theory* 51:44, 2005.

$|\Psi\rangle_{AA'} = |\Phi_d\rangle_{AA'} := \frac{1}{\sqrt{d}} \sum_{k=1}^{d} |k\rangle_A |k\rangle_{A'}$ max entangled. Later $d \to \infty$.

$|\Psi\rangle_{AA'} = |\Phi_d\rangle_{AA'} := \frac{1}{\sqrt{d}} \sum_{k=1}^{d} |k\rangle_A |k\rangle_{A'}$ max entangled. Later $d \to \infty$.

$T_p^{(d)} :=$ $d \times d$ upper left corner of $T_p$; then

$$I(A\rangle B)_{\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})} = \frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right]. \tag{11}$$

$|\Psi\rangle_{AA'} = |\Phi_d\rangle_{AA'} := \frac{1}{\sqrt{d}} \sum_{k=1}^{d} |k\rangle_A |k\rangle_{A'}$ max entangled. Later $d \to \infty$.

$T_p^{(d)} :=$ $d \times d$ upper left corner of $T_p$; then

$$I(A\rangle B)_{\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})} = \frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right]. \tag{11}$$

Can we compute the eigenvalues of $T_p^{(d)}$?

[5] Szegő, *Math. Z.* 6:167, 1920. Serra-Capizzano, *Rend. Circ. Mat. Palermo, Ser. II, Suppl.* 68:791, 2002.

$|\Psi\rangle_{AA'} = |\Phi_d\rangle_{AA'} := \frac{1}{\sqrt{d}} \sum_{k=1}^{d} |k\rangle_A |k\rangle_{A'}$ max entangled. Later $d \to \infty$.

$T_p^{(d)} :=$ $d \times d$ upper left corner of $T_p$; then

$$I(A\rangle B)_{\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})} = \frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right]. \tag{11}$$

Can we compute the eigenvalues of $T_p^{(d)}$?

$p(\phi) = \sum_k P_k \delta(\phi - \phi_k)$ supported on $\phi_k = \frac{2\pi k}{d}$, $k \in \mathbb{Z}$

[5] Szegő, *Math. Z.* 6:167, 1920. Serra-Capizzano, *Rend. Circ. Mat. Palermo, Ser. II, Suppl.* 68:791, 2002.

$|\Psi\rangle_{AA'} = |\Phi_d\rangle_{AA'} := \frac{1}{\sqrt{d}} \sum_{k=1}^{d} |k\rangle_A |k\rangle_{A'}$ max entangled. Later $d \to \infty$.

$T_p^{(d)} :=$ $d \times d$ upper left corner of $T_p$; then

$$I(A\rangle B)_{\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})} = \frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right]. \tag{11}$$

Can we compute the eigenvalues of $T_p^{(d)}$?

$p(\phi) = \sum_k P_k \delta(\phi - \phi_k)$ supported on $\phi_k = \frac{2\pi k}{d}$, $k \in \mathbb{Z}$

$\implies$ $T_p^{(d)}$ circulant matrix with eigenvalues $dP_k$

[5] Szegő, *Math. Z.* 6:167, 1920. Serra-Capizzano, *Rend. Circ. Mat. Palermo, Ser. II, Suppl.* 68:791, 2002.

$|\Psi\rangle_{AA'} = |\Phi_d\rangle_{AA'} := \frac{1}{\sqrt{d}} \sum_{k=1}^{d} |k\rangle_A |k\rangle_{A'}$ max entangled. Later $d \to \infty$.

$T_p^{(d)} :=$ $d \times d$ upper left corner of $T_p$; then

$$I(A\rangle B)_{\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})} = \frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right]. \tag{11}$$

Can we compute the eigenvalues of $T_p^{(d)}$?

$p(\phi) = \sum_k P_k \delta(\phi - \phi_k)$ supported on $\phi_k = \frac{2\pi k}{d}$, $k \in \mathbb{Z}$

$\implies$ $T_p^{(d)}$ circulant matrix with eigenvalues $dP_k$

$\implies$ $\frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right] = \log_2 d - H(P)$

[5] Szegő, *Math. Z.* 6:167, 1920. Serra-Capizzano, *Rend. Circ. Mat. Palermo, Ser. II, Suppl.* 68:791, 2002.

$|\Psi\rangle_{AA'} = |\Phi_d\rangle_{AA'} := \frac{1}{\sqrt{d}} \sum_{k=1}^{d} |k\rangle_A |k\rangle_{A'}$ max entangled. Later $d \to \infty$.

$T_p^{(d)} :=$ $d \times d$ upper left corner of $T_p$; then

$$I(A\rangle B)_{\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})} = \frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right]. \tag{11}$$

Can we compute the eigenvalues of $T_p^{(d)}$?

$p(\phi) = \sum_k P_k \delta(\phi - \phi_k)$ supported on $\phi_k = \frac{2\pi k}{d}$, $k \in \mathbb{Z}$

$\implies$ $T_p^{(d)}$ circulant matrix with eigenvalues $dP_k$

$\implies$ $\frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right] = \log_2 d - H(P)$

When $d \to \infty$: generalise to the *continuous* probability distribution $p$?

[5] Szegő, *Math. Z.* 6:167, 1920. Serra-Capizzano, *Rend. Circ. Mat. Palermo, Ser. II, Suppl.* 68:791, 2002.

$|\Psi\rangle_{AA'} = |\Phi_d\rangle_{AA'} := \frac{1}{\sqrt{d}} \sum_{k=1}^{d} |k\rangle_A |k\rangle_{A'}$ max entangled. Later $d \to \infty$.

$T_p^{(d)} :=$ $d \times d$ upper left corner of $T_p$; then

$$I(A\rangle B)_{\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})} = \frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right]. \tag{11}$$

Can we compute the eigenvalues of $T_p^{(d)}$?

$p(\phi) = \sum_k P_k \delta(\phi - \phi_k)$ supported on $\phi_k = \frac{2\pi k}{d}$, $k \in \mathbb{Z}$

$\implies$ $T_p^{(d)}$ circulant matrix with eigenvalues $dP_k$

$\implies$ $\frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right] = \log_2 d - H(P)$

When $d \to \infty$: generalise to the *continuous* probability distribution $p$?

Yes, thanks to Szegő's theorem in asymptotic linear algebra:[5]

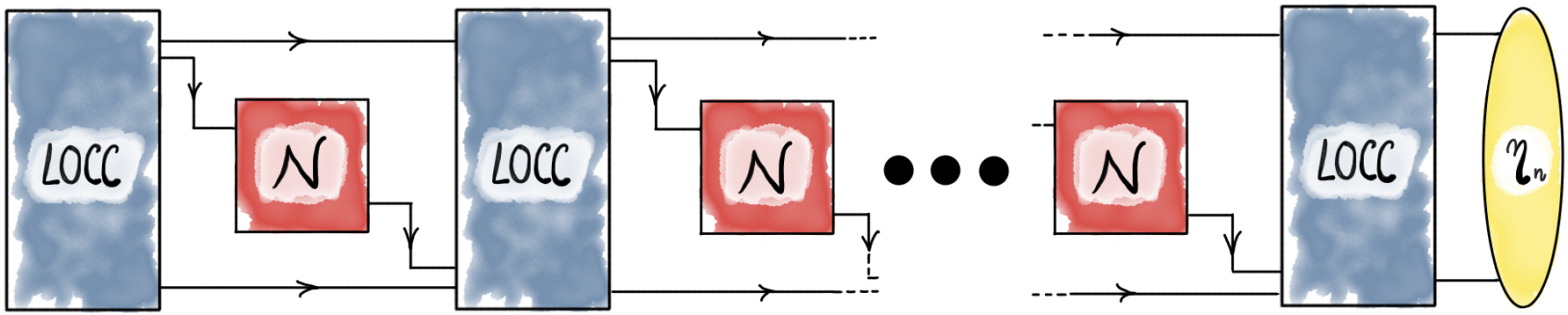
$$Q(\mathcal{N}_p) \geq \lim_{d\to\infty} \frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right] = \log_2(2\pi) - h(p). \tag{12}$$

[5] Szegő, *Math. Z.* 6:167, 1920. Serra-Capizzano, *Rend. Circ. Mat. Palermo, Ser. II, Suppl.* 68:791, 2002.

(b) Upper bound $Q_{\leftrightarrow}(\mathscr{N}_p) \leq \log_2(2\pi) - h(p)$?

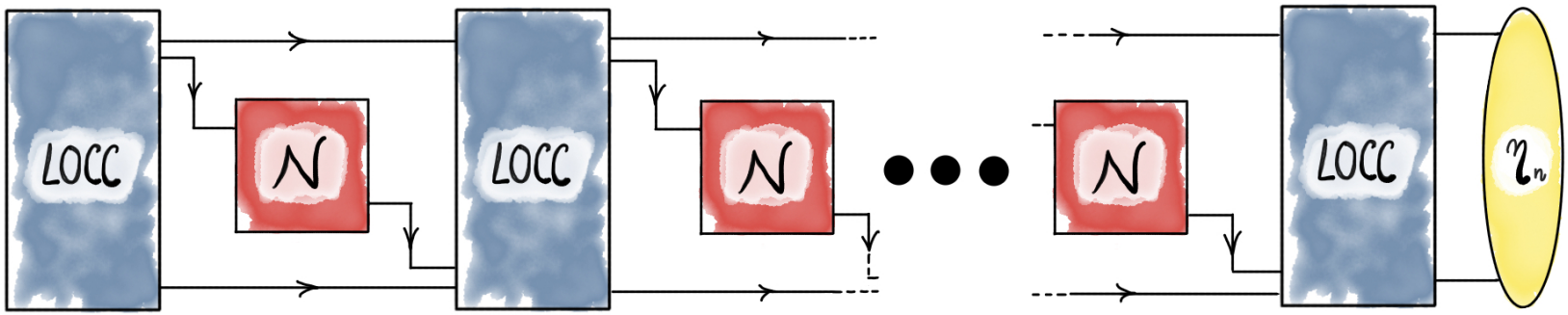
(b) Upper bound $Q_{\leftrightarrow}(\mathscr{N}_p) \leq \log_2(2\pi) - h(p)$?

$Q_{\leftrightarrow}$ requires optimisation over complicated protocols. How to simplify it?



(b) Upper bound $Q_{\leftrightarrow}(\mathcal{N}_p) \leq \log_2(2\pi) - h(p)$?

$Q_{\leftrightarrow}$ requires optimisation over complicated protocols. How to simplify it?



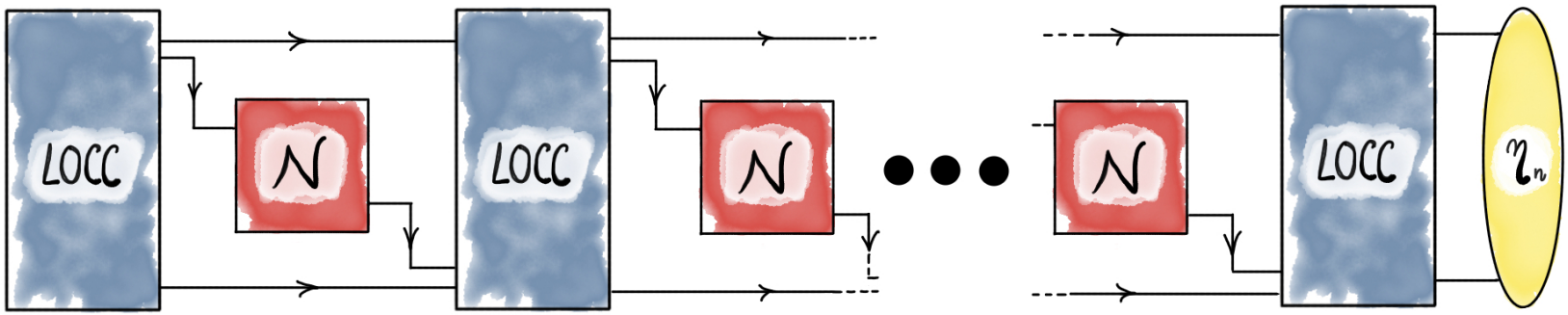

**Key observation**

$\mathcal{N}_p$ is teleportation simulable, i.e.

one use of $\mathcal{N}_p^{A\to B} \overset{d\to\infty}{\simeq}$ Alice and Bob have Choi state $\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})$

(b) Upper bound $Q_{\leftrightarrow}(\mathcal{N}_p) \leq \log_2(2\pi) - h(p)$?

$Q_{\leftrightarrow}$ requires optimisation over complicated protocols. How to simplify it?




**Key observation**

$\mathcal{N}_p$ is teleportation simulable, i.e.

one use of $\mathcal{N}_p^{A\to B} \overset{d\to\infty}{\simeq}$ Alice and Bob have Choi state $\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})$

Whatever Alice and Bob can do on the left, they can do on the right.

Teleportation simulability implies that[6]

$$Q_{\leftrightarrow}(\mathcal{N}_p) \leq \liminf_{d\to\infty} \left( \begin{array}{c} \text{distillable} \\ \text{entanglement} \end{array} \right) (\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'}))$$

[6] BDSW, *Phys. Rev. A* 54:3824, 1996. PLOB, *Nat. Commun.* 8:15043, 2017.

Teleportation simulability implies that[6]

$$Q_{\leftrightarrow}(\mathcal{N}_p) \leq \liminf_{d\to\infty} \left(\begin{array}{c}\text{distillable}\\ \text{entanglement}\end{array}\right)\left(\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})\right)$$

$$\begin{array}{c}\text{relative entropy}\\ \text{of entanglement}\end{array} \to \leq \liminf_{d\to\infty} E_R\left(\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})\right)$$

[6] BDSW, *Phys. Rev. A* 54:3824, 1996. PLOB, *Nat. Commun.* 8:15043, 2017.

Teleportation simulability implies that[6]

$$Q_{\leftrightarrow}(\mathcal{N}_p) \leq \liminf_{d\to\infty} \begin{pmatrix} \text{distillable} \\ \text{entanglement} \end{pmatrix} \left(\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})\right)$$

$$\begin{matrix} \text{relative entropy} \\ \text{of entanglement} \end{matrix} \to \leq \liminf_{d\to\infty} E_R\left(\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})\right)$$

$$\text{ansatz} \to \leq \lim_{d\to\infty} \frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right]$$

[6] BDSW, *Phys. Rev. A* 54:3824, 1996. PLOB, *Nat. Commun.* 8:15043, 2017.

Teleportation simulability implies that[6]

$$
\begin{aligned}
Q_{\leftrightarrow}(\mathcal{N}_p) &\leq \liminf_{d\to\infty} \begin{pmatrix} \text{distillable} \\ \text{entanglement} \end{pmatrix} \left(\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})\right) \\
\begin{matrix} \text{relative entropy} \\ \text{of entanglement} \end{matrix} \to &\leq \liminf_{d\to\infty} E_R\left(\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})\right) \\
\text{ansatz} \to &\leq \lim_{d\to\infty} \frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right] \\
\text{Szegő} \to &= \log_2(2\pi) - h(p)\,.
\end{aligned}
\tag{13}
$$

[6] BDSW, *Phys. Rev. A* 54:3824, 1996. PLOB, *Nat. Commun.* 8:15043, 2017.

Teleportation simulability implies that[6]

$$
\begin{aligned}
Q_{\leftrightarrow}(\mathcal{N}_p) &\leq \liminf_{d\to\infty} \begin{pmatrix} \text{distillable} \\ \text{entanglement} \end{pmatrix} \left(\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})\right) \\
\text{relative entropy of entanglement} \rightarrow &\leq \liminf_{d\to\infty} E_R\left(\mathcal{N}_p^{A'\to B}(\Phi_d^{AA'})\right) \\
\text{ansatz} \rightarrow &\leq \lim_{d\to\infty} \frac{1}{d} \operatorname{Tr}\left[T_p^{(d)} \log_2 T_p^{(d)}\right] \\
\text{Szegő} \rightarrow &= \log_2(2\pi) - h(p)\,.
\end{aligned}
\tag{13}
$$

Second appearance of Szegő's theorem!

[6] BDSW, *Phys. Rev. A* 54:3824, 1996. PLOB, *Nat. Commun.* 8:15043, 2017.

# Conclusions

# Conclusions

- We gave an exact formula for $\mathscr{C}(\mathscr{N}_p)$, for all $p$ and all quantum/private capacities $\mathscr{C}$:

$$\mathscr{C}(\mathscr{N}_p) = \log_2(2\pi) - h(p)\,.$$

# Conclusions

- We gave an exact formula for $\mathscr{C}(\mathscr{N}_p)$, for all $p$ and all quantum/private capacities $\mathscr{C}$:

$$\mathscr{C}(\mathscr{N}_p) = \log_2(2\pi) - h(p)\,.$$

- It generalises capacity formula for finite-dim dephasing channels.[7] $\longrightarrow$ Proof requires substantially new insights.

[7] PLOB, *Nat. Commun.* 8:15043, 2017.

# Conclusions

- We gave an exact formula for $\mathscr{C}(\mathscr{N}_p)$, for all $p$ and all quantum/private capacities $\mathscr{C}$:

$$\mathscr{C}(\mathscr{N}_p) = \log_2(2\pi) - h(p)\,.$$

- It generalises capacity formula for finite-dim dephasing channels.[7] $\longrightarrow$ Proof requires substantially new insights.

- Open: *energy-constrained* capacities?

[7] PLOB, *Nat. Commun.* 8:15043, 2017.

# Conclusions

- We gave an exact formula for $\mathscr{C}(\mathscr{N}_p)$, for all $p$ and all quantum/private capacities $\mathscr{C}$:

$$\mathscr{C}(\mathscr{N}_p) = \log_2(2\pi) - h(p)\,.$$

- It generalises capacity formula for finite-dim dephasing channels.[7] $\longrightarrow$ Proof requires substantially new insights.
- Open: *energy-constrained* capacities?
- Open: what if one adds photon loss, as in $\Lambda_{p,\eta} := \mathscr{N}_p \circ \mathcal{L}_\eta$?

[7] PLOB, *Nat. Commun.* 8:15043, 2017.

# Conclusions

- We gave an exact formula for $\mathscr{C}(\mathscr{N}_p)$, for all $p$ and all quantum/private capacities $\mathscr{C}$:

$$\mathscr{C}(\mathscr{N}_p) = \log_2(2\pi) - h(p)\,.$$

- It generalises capacity formula for finite-dim dephasing channels.[7] $\longrightarrow$ Proof requires substantially new insights.
- Open: *energy-constrained* capacities?
- Open: what if one adds photon loss, as in $\Lambda_{p,\eta} := \mathscr{N}_p \circ \mathcal{L}_\eta$?

Thank you!

[7] PLOB, *Nat. Commun.* 8:15043, 2017.