Quantum Coding with Finite Resources

INSTITUTE FOR QUANTUM INFORMATION AND MATTER
Caltech

Mario Berta

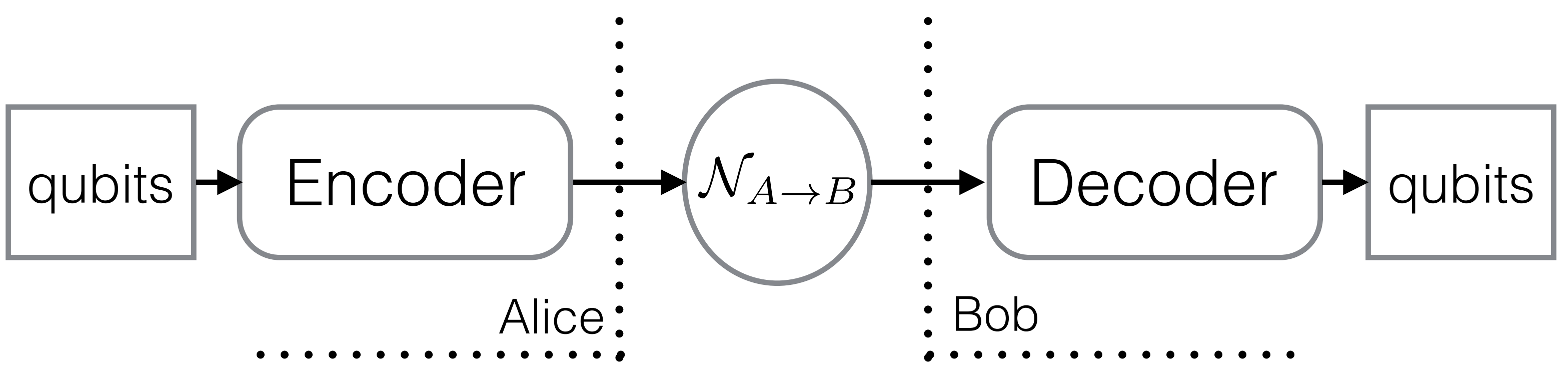
joint work with Joseph M. Renes (ETH Zurich) and Marco Tomamichel (University of Sydney) -
Nature Communications 7, 11419 (2016)

Quantum Coding I

- Reliable **transmission of qubits** over noisy quantum channels $\mathcal{N} = \mathcal{N}_{A \to B}$

  —> any physical evolution by means of a completely positive and trace-preserving map (from input quantum state to output quantum state)

point to point communication:

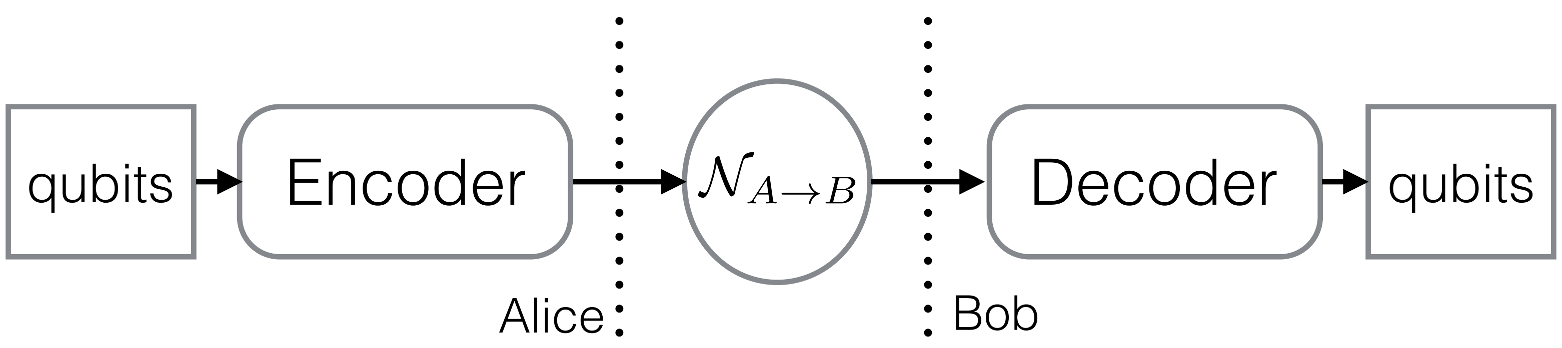


Quantum Coding I

- Reliable **transmission of qubits** over noisy quantum channels $\mathcal{N} = \mathcal{N}_{A\to B}$

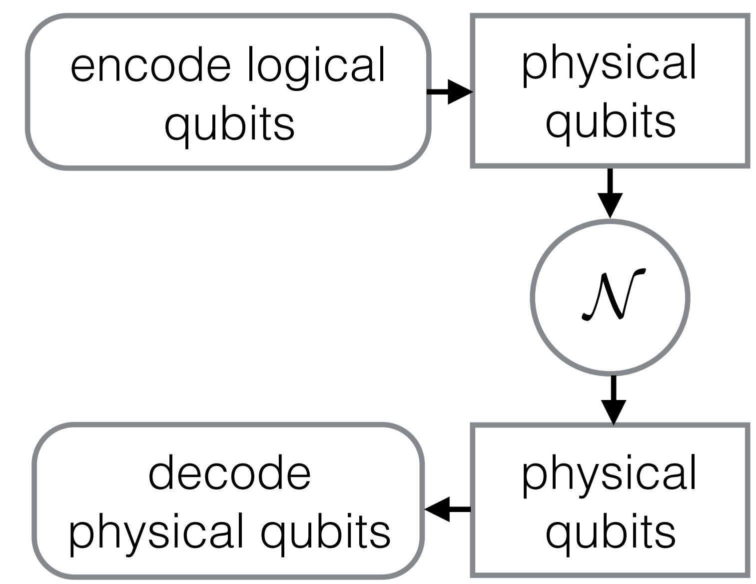
  —> any physical evolution by means of a completely positive and trace-preserving map (from input quantum state to output quantum state)

point to point communication:



or

logical vs. physical qubits:

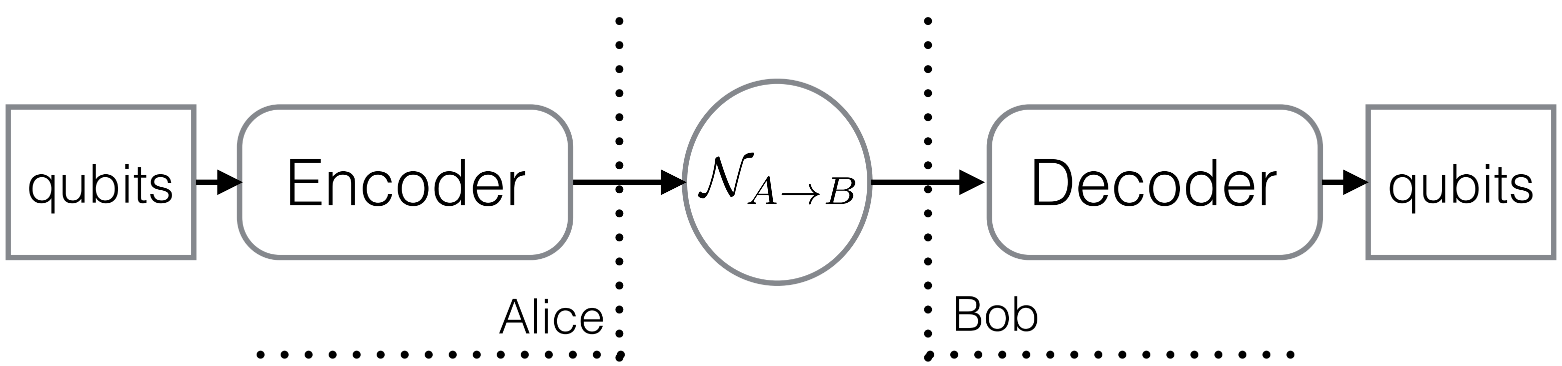


Quantum Coding I

- Reliable **transmission of qubits** over noisy quantum channels $\mathcal{N} = \mathcal{N}_{A \to B}$

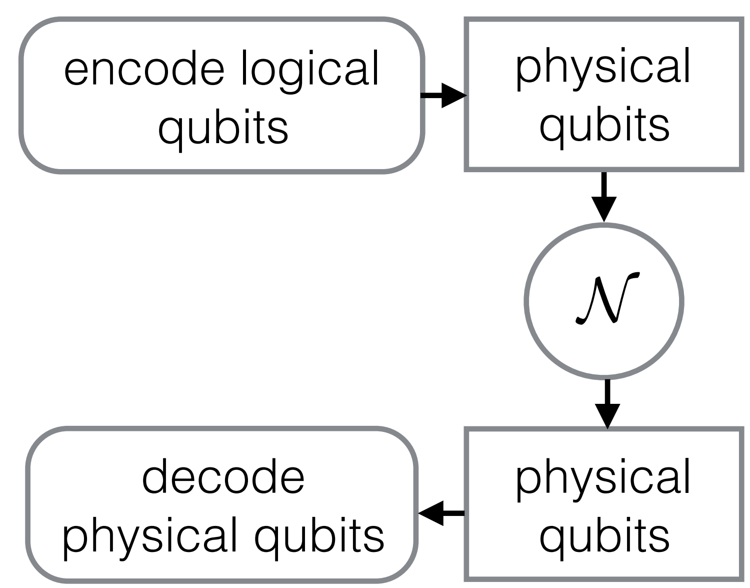
  —> any physical evolution by means of a completely positive and trace-preserving map (from input quantum state to output quantum state)

point to point communication:



or

logical vs. physical qubits:



- Ex: qubit dephasing channel $\mathcal{Z}_\gamma : \rho \mapsto (1-\gamma)\rho + \gamma Z \rho Z$ with $\gamma \in [0,1]$,

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

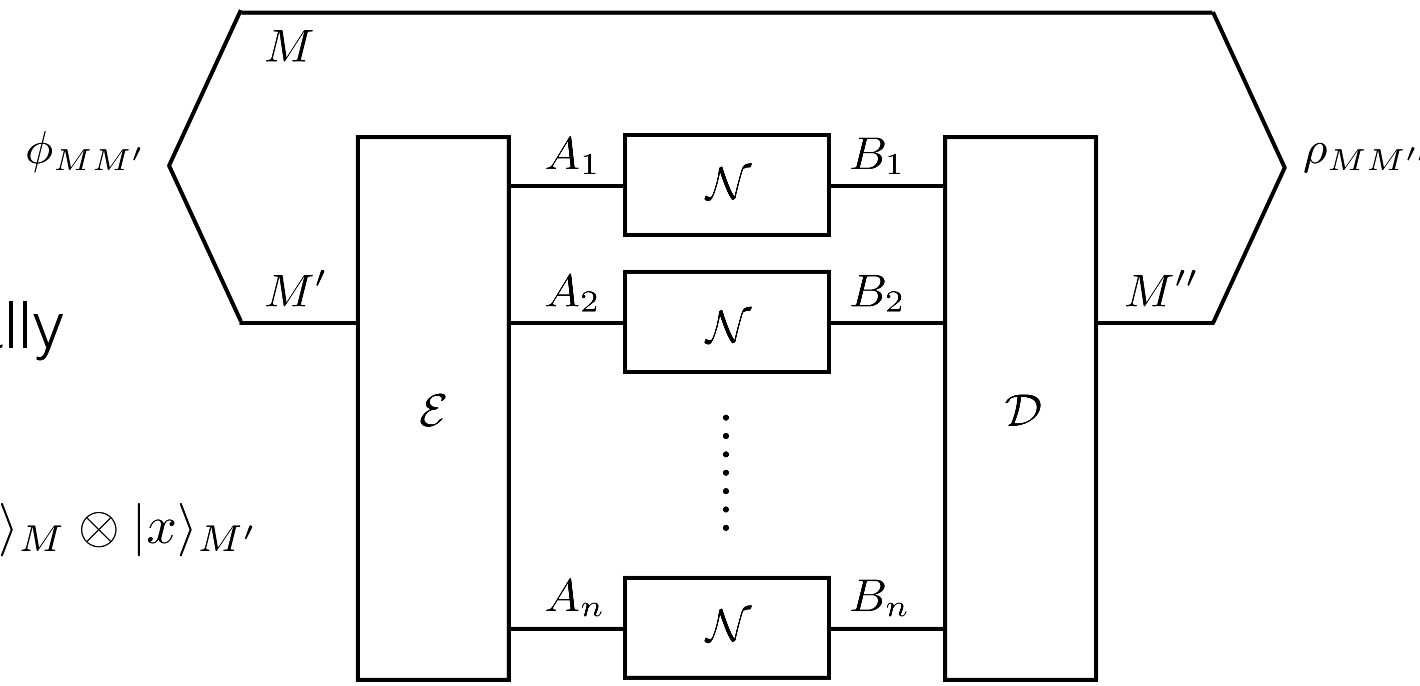
  —> so, e.g., $\mathcal{Z}_\gamma(|\psi^+\rangle\langle\psi^+|) = (1-\gamma)|\psi^+\rangle\langle\psi^+| + \gamma|\psi^-\rangle\langle\psi^-|$

$$\left(|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \, |\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \right)$$

Quantum Coding II

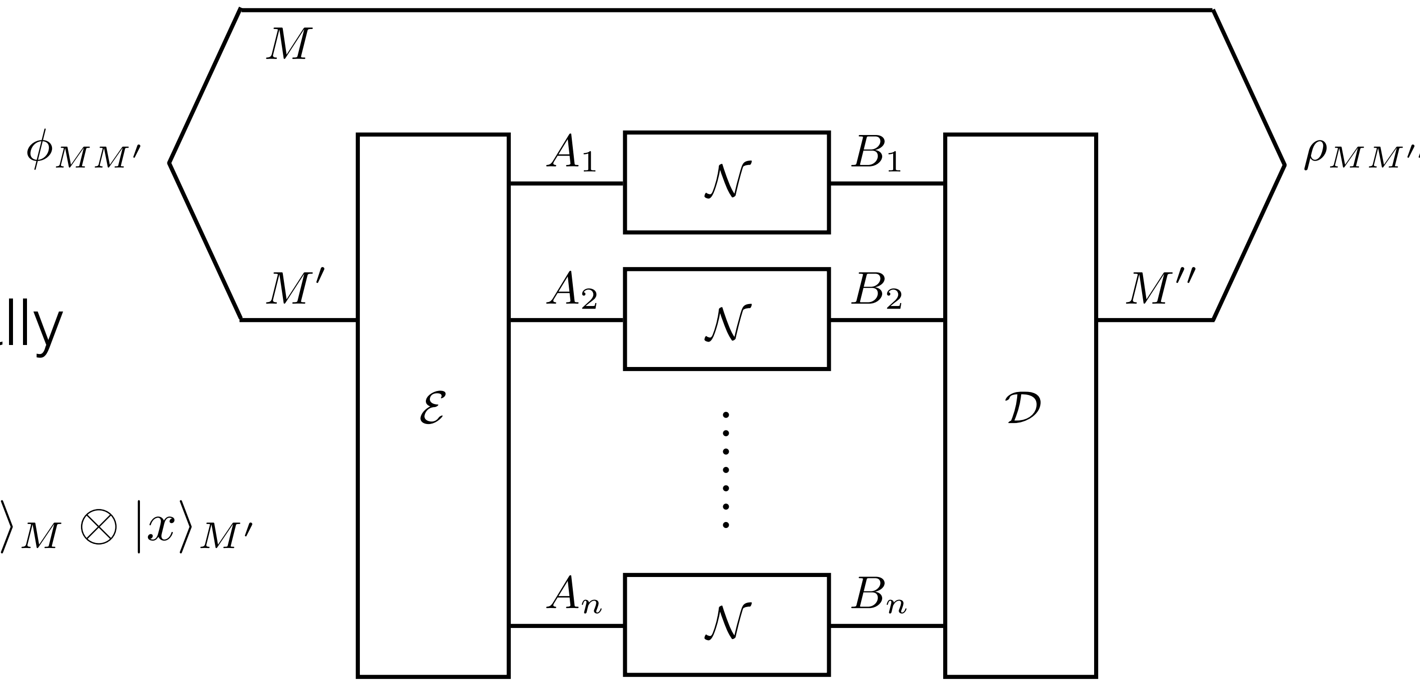
- **Many uses** of a channel $\mathcal{N} = \mathcal{N}_{A \to B}$:
- **Entanglement transmission**: maximally entangled state

$$\phi_{MM'} = |\phi\rangle\langle\phi|_{MM'} \text{ with } |\phi\rangle_{MM'} = \frac{1}{\sqrt{|M|}} \sum_{x=1}^{|M|} |x\rangle_M \otimes |x\rangle_{M'}$$



Quantum Coding II

- **Many uses** of a channel $\mathcal{N} = \mathcal{N}_{A \to B}$:



- **Entanglement transmission**: maximally entangled state

$$\phi_{MM'} = |\phi\rangle\langle\phi|_{MM'} \text{ with } |\phi\rangle_{MM'} = \frac{1}{\sqrt{|M|}} \sum_{x=1}^{|M|} |x\rangle_M \otimes |x\rangle_{M'}$$

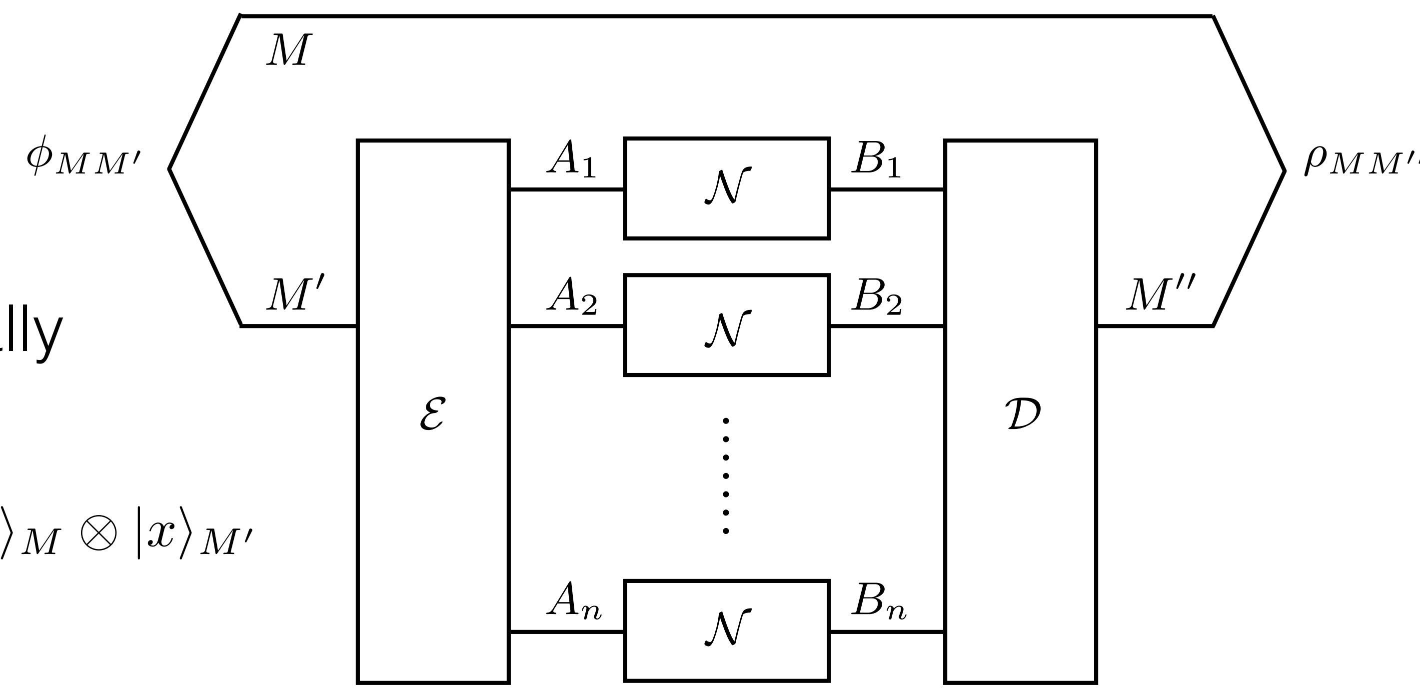
- If there exists an encoder $\mathcal{E}$ and a decoder $\mathcal{D}$ with

$$F\left(\phi_{MM'}, (\mathcal{D} \circ \mathcal{N}^{\otimes n} \circ \mathcal{E})(\phi_{MM'})\right) \geq 1 - \epsilon$$

we say that $\left(R = \frac{1}{n} \log |M|, n, \epsilon\right)$ is **achievable**

Quantum Coding II

- **Many uses** of a channel $\mathcal{N} = \mathcal{N}_{A\to B}$:



- **Entanglement transmission**: maximally entangled state

$$\phi_{MM'} = |\phi\rangle\langle\phi|_{MM'} \text{ with } |\phi\rangle_{MM'} = \frac{1}{\sqrt{|M|}} \sum_{x=1}^{|M|} |x\rangle_M \otimes |x\rangle_{M'}$$

- If there exists an encoder $\mathcal{E}$ and a decoder $\mathcal{D}$ with

$$F\left(\phi_{MM'}, (\mathcal{D} \circ \mathcal{N}^{\otimes n} \circ \mathcal{E})(\phi_{MM'})\right) \geq 1 - \epsilon$$

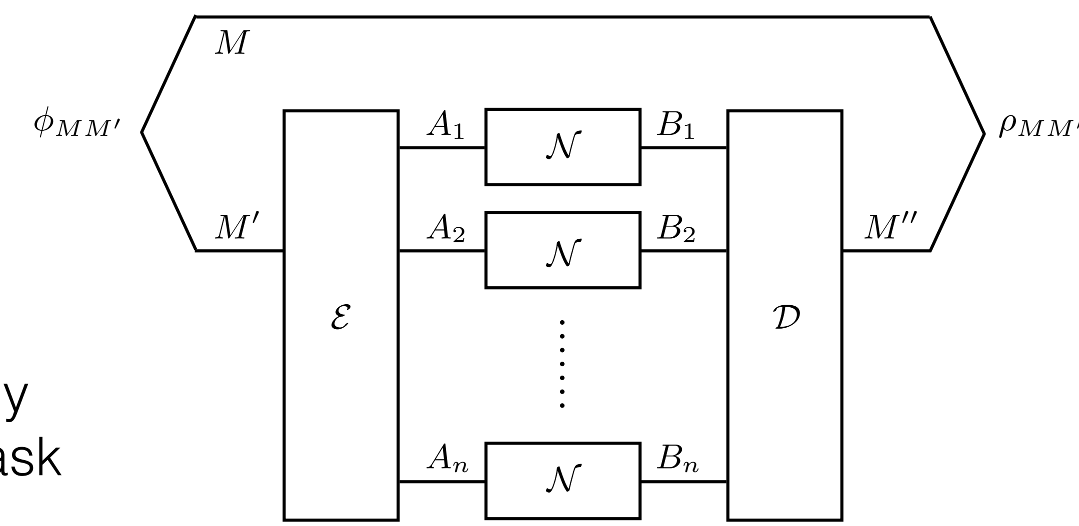
we say that $\left(R = \frac{1}{n} \log |M|, n, \epsilon\right)$ is **achievable**

- Given fixed $\mathcal{N}^{\otimes n}$ and $\epsilon \geq 0$, what is the highest possible rate R?

$$\hat{R}_{\mathcal{N}}(n;\epsilon) = \max\{R : (R, n, \epsilon) \text{ is achievable on } \mathcal{N}\}$$

Quantum Coding III

$$\hat{R}_{\mathcal{N}}(n;\epsilon) = \max\{R : (R, n, \epsilon) \text{ is achievable on } \mathcal{N}\}$$



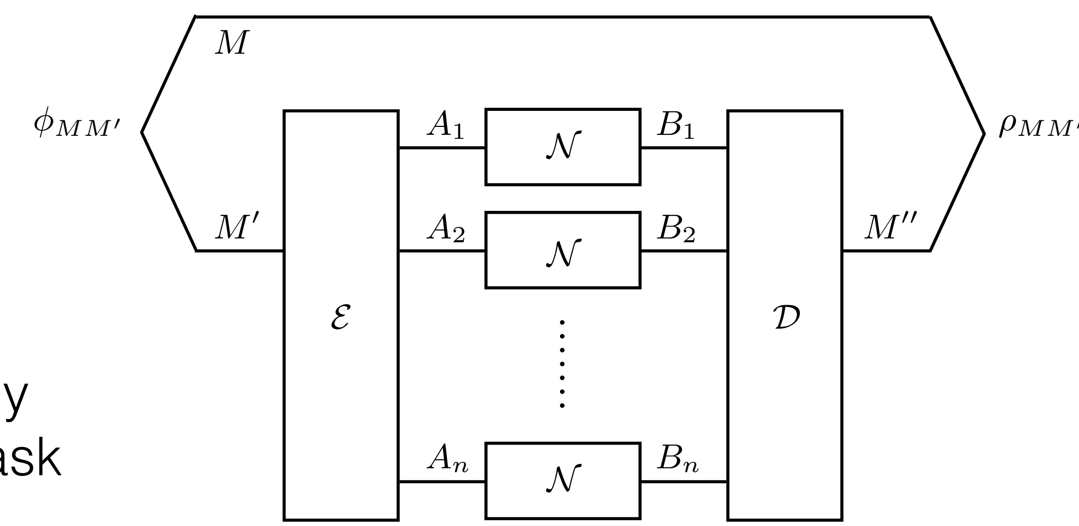
- **Quantum capacity**:

$$Q(\mathcal{N}) = \lim_{\epsilon\to 0} \lim_{n\to\infty} \hat{R}_{\mathcal{N}}(n;\epsilon)$$

—> in the limit of infinitely many channel uses we ask for perfect transmission

Quantum Coding III

$$\hat{R}_{\mathcal{N}}(n;\epsilon) = \max\{R : (R,n,\epsilon) \text{ is achievable on } \mathcal{N}\}$$



- **Quantum capacity**:

$$Q(\mathcal{N}) = \lim_{\epsilon\to 0}\lim_{n\to\infty} \hat{R}_{\mathcal{N}}(n;\epsilon)$$

—> in the limit of infinitely many channel uses we ask for perfect transmission

---

- Ex: qubit dephasing channel $\mathcal{Z}_\gamma : \rho \mapsto (1-\gamma)\rho + \gamma Z\rho Z$ with $\gamma \in [0,1]$

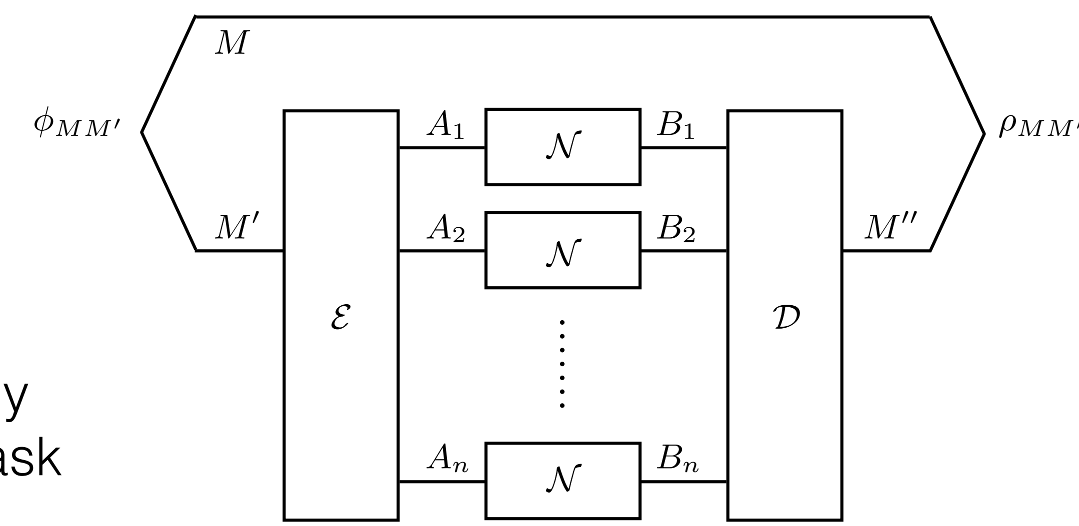
$$Q(\mathcal{Z}_\gamma) = 1 - h(\gamma)$$

$$h(\gamma) = -\gamma\log\gamma - (1-\gamma)\log(1-\gamma)$$

binary entropy

Quantum Coding III

$$\hat{R}_{\mathcal{N}}(n;\epsilon) = \max\{R : (R,n,\epsilon) \text{ is achievable on } \mathcal{N}\}$$



- **Quantum capacity**:

$$Q(\mathcal{N}) = \lim_{\epsilon\to 0}\lim_{n\to\infty} \hat{R}_{\mathcal{N}}(n;\epsilon)$$

—> in the limit of infinitely many channel uses we ask for perfect transmission

---

- Ex: qubit dephasing channel $\mathcal{Z}_\gamma : \rho \mapsto (1-\gamma)\rho + \gamma Z\rho Z$ with $\gamma \in [0,1]$

$$Q(\mathcal{Z}_\gamma) = 1 - h(\gamma)$$

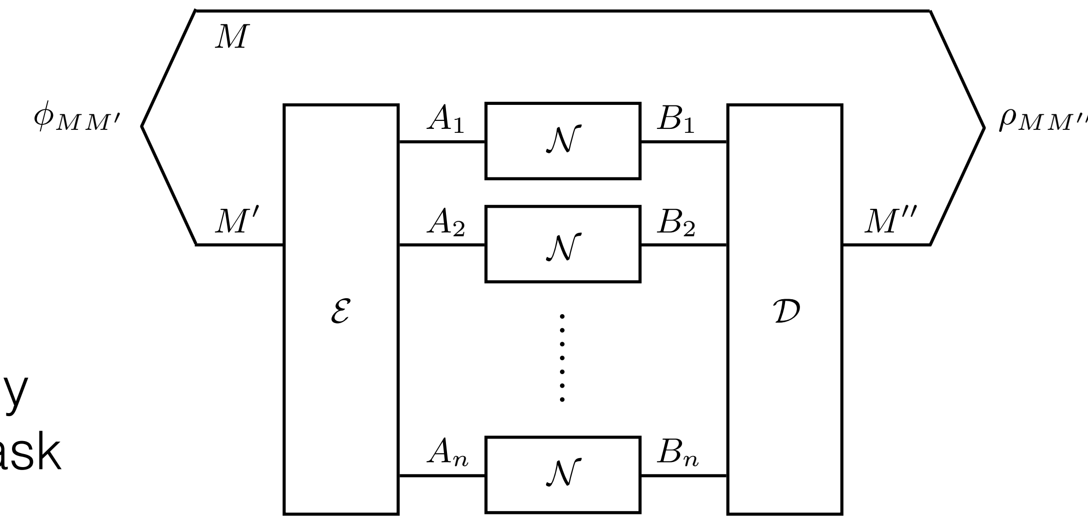
$$h(\gamma) = -\gamma\log\gamma - (1-\gamma)\log(1-\gamma)$$

binary entropy

- For general channels we **do not know how to compute** the quantum capacity!

Quantum Coding III

$$\hat{R}_{\mathcal{N}}(n;\epsilon) = \max\{R : (R,n,\epsilon) \text{ is achievable on } \mathcal{N}\}$$



- **Quantum capacity**:

$$Q(\mathcal{N}) = \lim_{\epsilon\to 0} \lim_{n\to\infty} \hat{R}_{\mathcal{N}}(n;\epsilon)$$

—> in the limit of infinitely many channel uses we ask for perfect transmission

---

- Ex: qubit dephasing channel $\mathcal{Z}_\gamma : \rho \mapsto (1-\gamma)\rho + \gamma Z\rho Z$ with $\gamma \in [0,1]$

$$Q(\mathcal{Z}_\gamma) = 1 - h(\gamma)$$

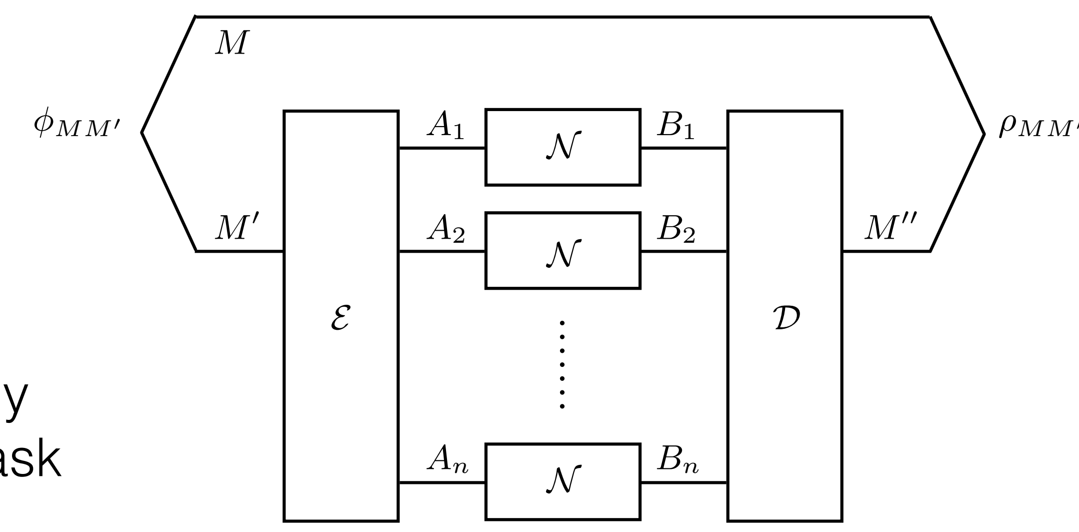
$$h(\gamma) = -\gamma\log\gamma - (1-\gamma)\log(1-\gamma)$$

binary entropy

- For general channels we **do not know how to compute** the quantum capacity!
- We would like to study $\hat{R}_{\mathcal{N}}(n;\epsilon)$ **directly**, or actually $\hat{R}^{\leftrightarrow}_{\mathcal{N}}(n;\varepsilon)$ with **two-way classical communication** assistance)

Quantum Coding III

$$\hat{R}_{\mathcal{N}}(n;\epsilon) = \max\{R : (R,n,\epsilon) \text{ is achievable on } \mathcal{N}\}$$



- **Quantum capacity**:

$$Q(\mathcal{N}) = \lim_{\epsilon\to 0}\lim_{n\to\infty} \hat{R}_{\mathcal{N}}(n;\epsilon)$$

—> in the limit of infinitely many channel uses we ask for perfect transmission

---

- Ex: qubit dephasing channel $\mathcal{Z}_\gamma : \rho \mapsto (1-\gamma)\rho + \gamma Z\rho Z$ with $\gamma \in [0,1]$

$$Q(\mathcal{Z}_\gamma) = 1 - h(\gamma) = Q^{\leftrightarrow}(\mathcal{Z}_\gamma)$$

$$h(\gamma) = -\gamma\log\gamma - (1-\gamma)\log(1-\gamma)$$

binary entropy

- For general channels we **do not know how to compute** the quantum capacity!
- We would like to study $\hat{R}_{\mathcal{N}}(n;\epsilon)$ **directly**, or actually $\hat{R}^{\leftrightarrow}_{\mathcal{N}}(n;\varepsilon)$ with **two-way classical communication** assistance)

Qubit Dephasing Channel I

- $\mathcal{Z}_\gamma : \rho \mapsto (1-\gamma)\rho + \gamma Z \rho Z$ with $\gamma \in [0,1]$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- Corresponding **quantum capacity** (two-way classical communication assisted):

$$Q^{\leftrightarrow}(\mathcal{Z}_\gamma) = 1 - h(\gamma)$$

Qubit Dephasing Channel I

- $\mathcal{Z}_\gamma : \rho \mapsto (1-\gamma)\rho + \gamma Z \rho Z$ with $\gamma \in [0,1]$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

- Corresponding **quantum capacity** (two-way classical communication assisted):

$$Q^{\leftrightarrow}(\mathcal{Z}_\gamma) = 1 - h(\gamma)$$

- We show **third order approximation** for finite resources:

$$\hat{R}^{\leftrightarrow}_{\mathcal{Z}_\gamma}(n;\varepsilon) = 1 - h(\gamma) + \sqrt{\frac{v(\gamma)}{n}}\Phi^{-1}(\varepsilon) + \frac{\log n}{2n} + O\left(\frac{1}{n}\right)$$

$$v(\gamma) = \gamma(\log(\gamma) + h(\gamma))^2 + (1-\gamma)(\log(1-\gamma) + h(\gamma))^2$$

binary entropy variance

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{\infty}^{x} e^{-\frac{y^2}{2}} \mathrm{d}y$$

cumulative standard Gaussian distribution

Qubit Dephasing Channel I

- $\mathcal{Z}_\gamma : \rho \mapsto (1-\gamma)\rho + \gamma Z \rho Z$ with $\gamma \in [0,1]$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

- Corresponding **quantum capacity** (two-way classical communication assisted):

$$Q^{\leftrightarrow}(\mathcal{Z}_\gamma) = 1 - h(\gamma)$$

- We show **third order approximation** for finite resources:

$$\hat{R}^{\leftrightarrow}_{\mathcal{Z}_\gamma}(n;\varepsilon) = 1 - h(\gamma) + \sqrt{\frac{v(\gamma)}{n}}\,\Phi^{-1}(\varepsilon) + \frac{\log n}{2n} + O\left(\frac{1}{n}\right)$$

$$v(\gamma) = \gamma(\log(\gamma) + h(\gamma))^2 + (1-\gamma)(\log(1-\gamma) + h(\gamma))^2$$

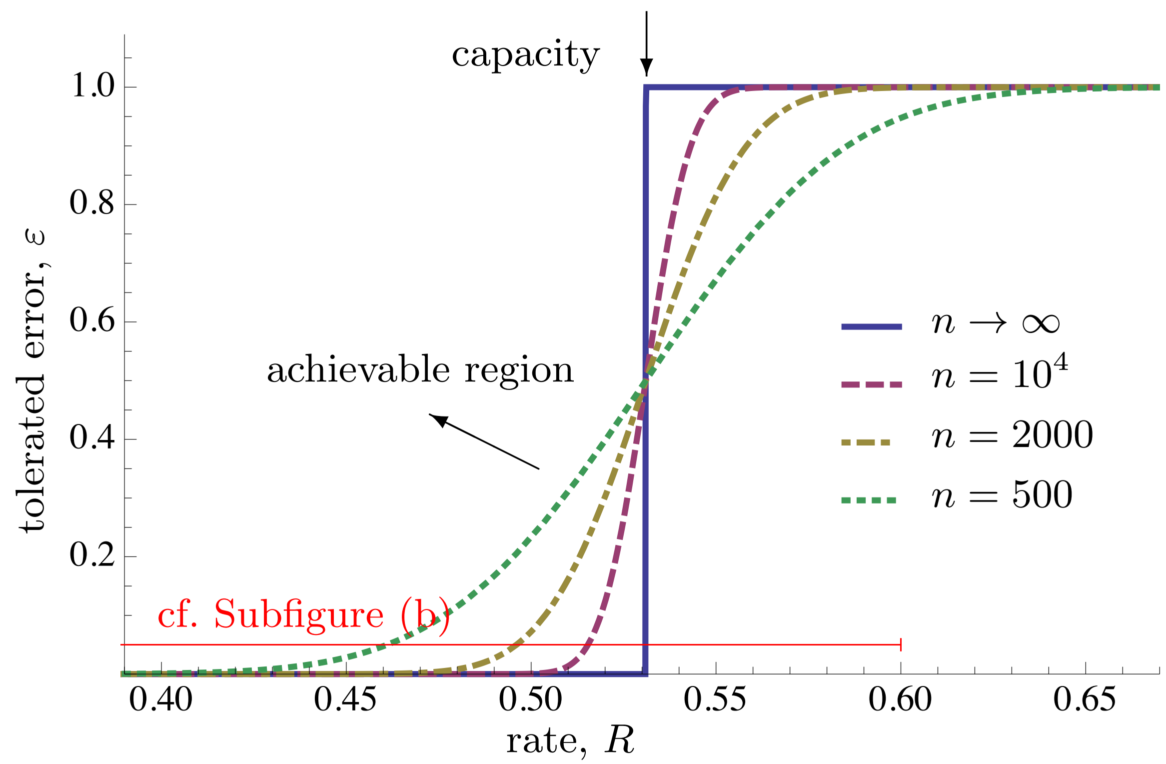
binary entropy variance

second parameter:
quantum channel dispersion

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{\infty}^{x} e^{-\frac{y^2}{2}}\,\mathrm{d}y$$

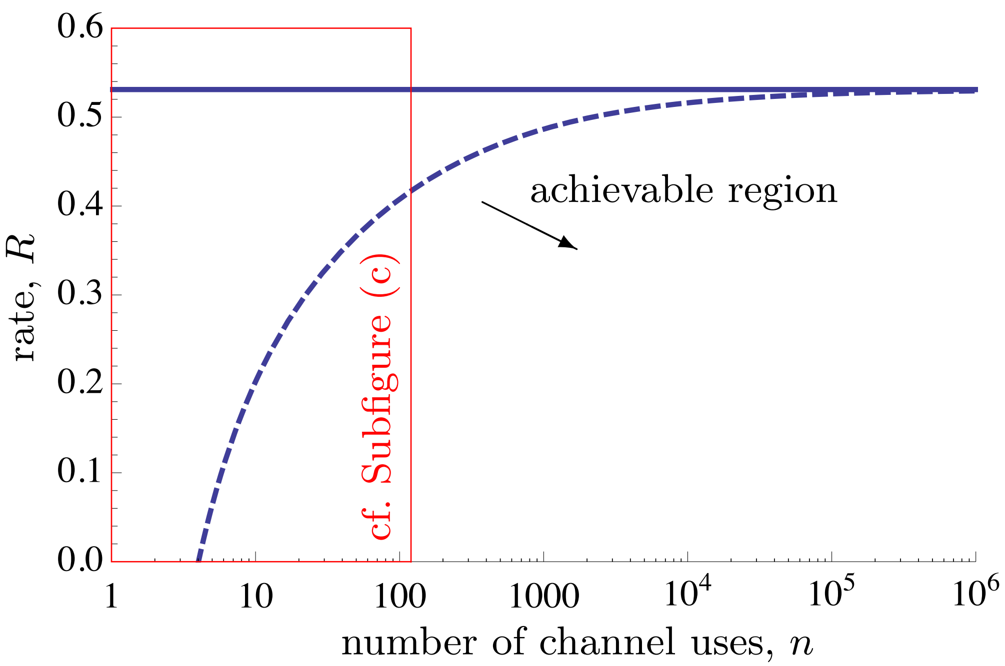
cumulative standard Gaussian distribution

Qubit Dephasing Channel II

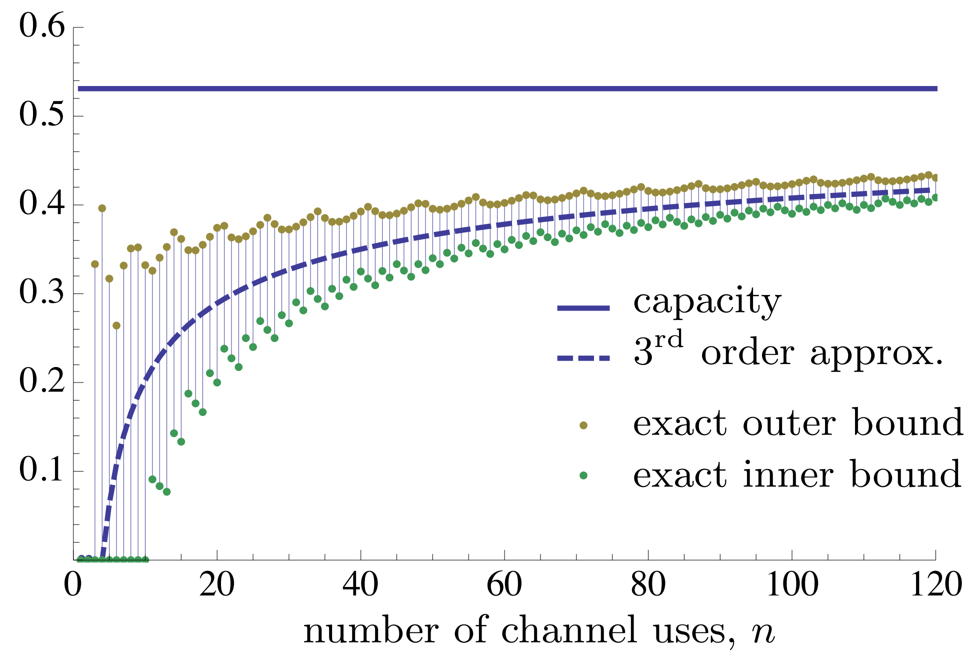


(a) Boundary of the achievable region for different values of n (second order approximation).

- $\mathcal{Z}_\gamma : \rho \mapsto (1-\gamma)\rho + \gamma Z \rho Z$ with $\gamma = 0.1$
- Quantum capacity:
  $$Q^{\leftrightarrow}(\mathcal{Z}_{0.1}) = 1 - h(0.1) \approx 0.531$$
- Strong converse behaviour



(b) Boundary of the achievable region for $\varepsilon = 5\%$ (third order approximation).



(c) Comparison of strict bounds with third order approximation for $\varepsilon = 5\%$.

Qubit Erasure Channel I

- $\mathcal{E}_\beta : \rho \mapsto (1-\beta)\rho + \beta|e\rangle\langle e|$ with $\beta \in [0,1]$ and $|e\rangle\langle e|$ orthogonal

- Corresponding **quantum capacity** (two-way classical communication assisted):

$$Q^{\leftrightarrow}(\mathcal{E}_\beta) = 1 - \beta \qquad (\text{vs. } Q(\mathcal{E}_\beta) = 1 - 2\beta)$$

Qubit Erasure Channel I

- $\mathcal{E}_\beta : \rho \mapsto (1-\beta)\rho + \beta|e\rangle\langle e|$ with $\beta \in [0,1]$ and $|e\rangle\langle e|$ orthogonal

- Corresponding **quantum capacity** (two-way classical communication assisted):

$$Q^{\leftrightarrow}(\mathcal{E}_\beta) = 1-\beta \qquad (\text{vs. } Q(\mathcal{E}_\beta) = 1-2\beta)$$

- We show **exact formula** for finite resources:

$$\varepsilon = \sum_{l=n-k+1}^{n} \binom{n}{l} \beta^l (1-\beta)^{n-l} \left(1 - 2^{n\left(1-\hat{R}^{\leftrightarrow}_{\mathcal{E}_\beta}(n;\varepsilon)\right)-l}\right)$$

- **Third order** expansion: $$\hat{R}^{\leftrightarrow}_{\mathcal{E}_\beta}(n;\varepsilon) = 1-\beta+\sqrt{\frac{\beta(1-\beta)}{n}}\Phi^{-1}(\varepsilon) + O\left(\frac{1}{n}\right)$$

Qubit Erasure Channel I

- $\mathcal{E}_\beta : \rho \mapsto (1-\beta)\rho + \beta|e\rangle\langle e|$ with $\beta \in [0,1]$ and $|e\rangle\langle e|$ orthogonal

- Corresponding **quantum capacity** (two-way classical communication assisted):

$$Q^{\leftrightarrow}(\mathcal{E}_\beta) = 1-\beta \qquad (\text{vs. } Q(\mathcal{E}_\beta) = 1-2\beta)$$

- We show **exact formula** for finite resources:

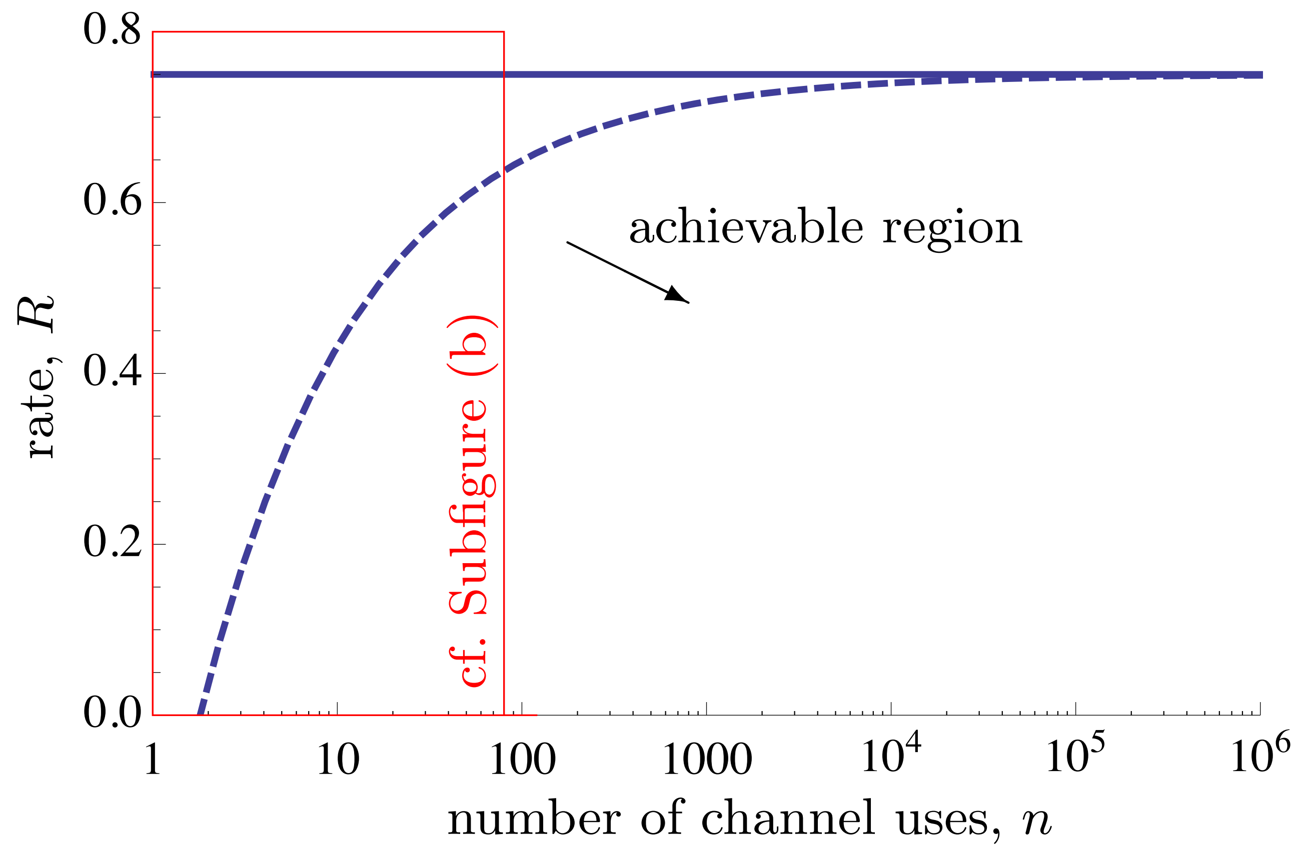
$$\varepsilon = \sum_{l=n-k+1}^{n} \binom{n}{l} \beta^l (1-\beta)^{n-l} \left(1 - 2^{n\left(1-\hat{R}^{\leftrightarrow}_{\mathcal{E}_\beta}(n;\varepsilon)\right)-l}\right)$$

- **Third order** expansion: $\hat{R}^{\leftrightarrow}_{\mathcal{E}_\beta}(n;\varepsilon) = 1-\beta+\sqrt{\frac{\beta(1-\beta)}{n}}\Phi^{-1}(\varepsilon) + O\left(\frac{1}{n}\right)$

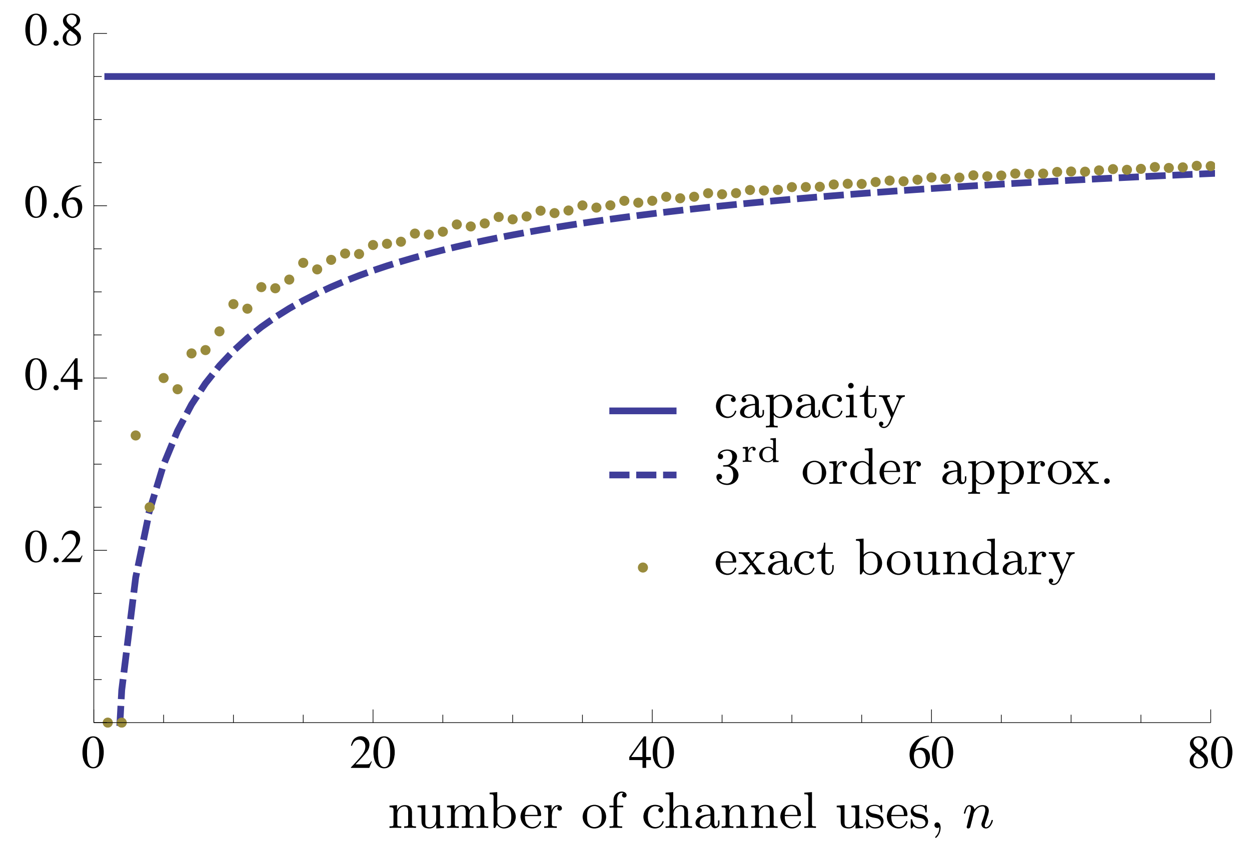
quantum channel dispersion

Qubit Erasure Channel II

- $\mathcal{E}_\beta : \rho \mapsto (1-\beta)\rho + \beta|e\rangle\langle e|$ with $\beta \in [0,1]$ and $|e\rangle\langle e|$ orthogonal
- Coding with two-way classical communication assistance for $\beta = 0.25,\ \epsilon = 0.01$:



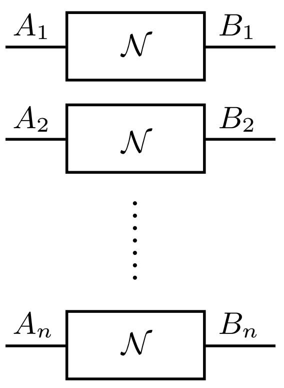
(a) Boundary of the achievable region.



(b) Comparison of exact bounds with third order approximation.

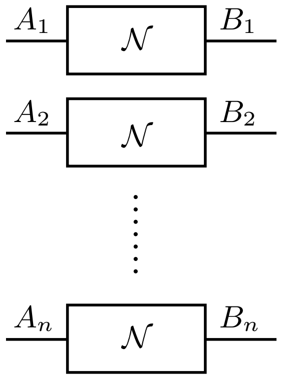
Conclusion

- Finite resources quantum coding: around **1000 (coherent) qubits** are needed to get within 90% of quantum capacity
- Quantum capacity together with **quantum channel dispersion** provide a good characterisation for simple channels



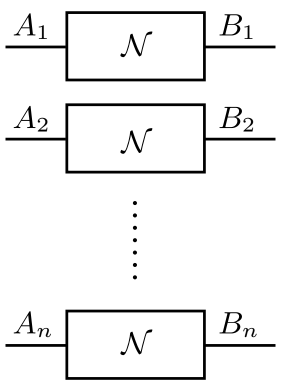
Conclusion

- Finite resources quantum coding: around **1000 (coherent) qubits** are needed to get within 90% of quantum capacity
- Quantum capacity together with **quantum channel dispersion** provide a good characterisation for simple channels
- Our bounds apply to all finite-dimensional quantum channels (but are not necessarily tight)



Conclusion

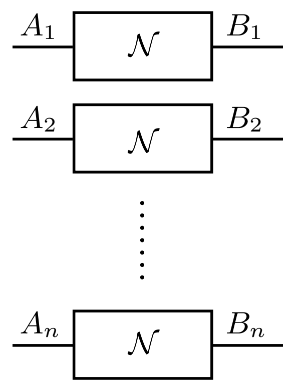
- Finite resources quantum coding: around **1000 (coherent) qubits** are needed to get within 90% of quantum capacity
- Quantum capacity together with **quantum channel dispersion** provide a good characterisation for simple channels
- Our bounds apply to all finite-dimensional quantum channels (but are not necessarily tight)



- Extension to **Gaussian channels** and **private capacity** (key generation) in [Wilde, Tomamichel, B. arXiv:1602.08898]

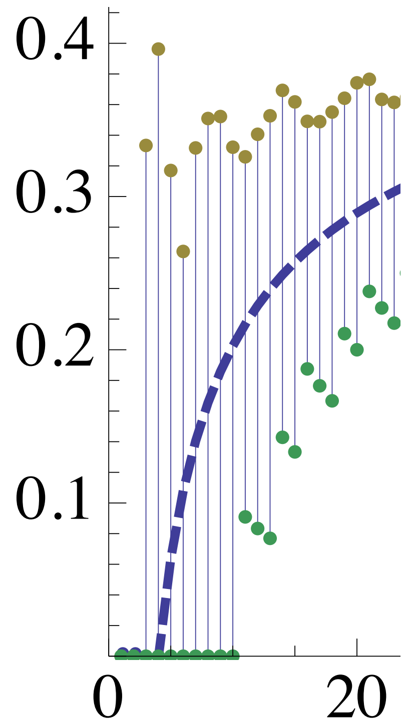
Conclusion

- Finite resources quantum coding: around **1000 (coherent) qubits** are needed to get within 90% of quantum capacity
- Quantum capacity together with **quantum channel dispersion** provide a good characterisation for simple channels
- Our bounds apply to all finite-dimensional quantum channels (but are not necessarily tight)



- Extension to **Gaussian channels** and **private capacity** (key generation) in [Wilde, Tomamichel, B. arXiv:1602.08898]
- What happens for **very small n** =1,2,3,…?

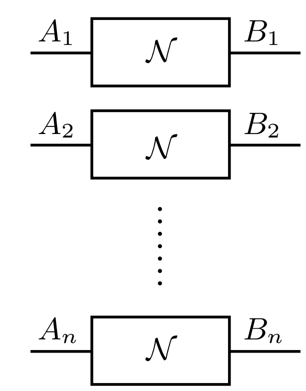
  —> extend efficiently computable bounds from, e.g.:
  [Matthews and Wehner, IEEE Trans. on Info. Th. (2014)],
  [Leung and Matthews, IEEE Trans. on Info. Th. (2015)]



Ex: qubit dephasing channel

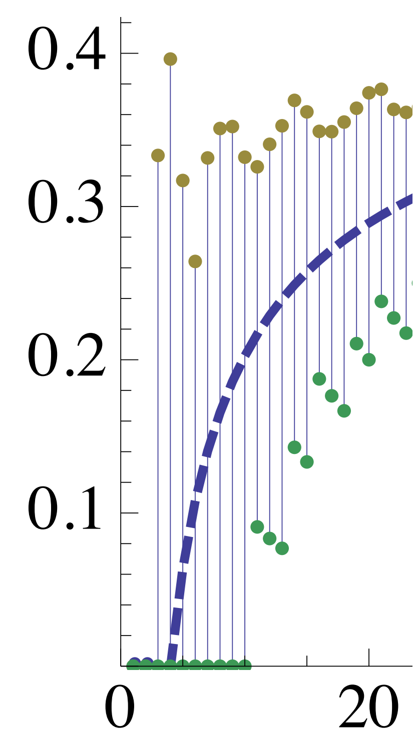
Conclusion

- Finite resources quantum coding: around **1000 (coherent) qubits** are needed to get within 90% of quantum capacity
- Quantum capacity together with **quantum channel dispersion** provide a good characterisation for simple channels
- Our bounds apply to all finite-dimensional quantum channels (but are not necessarily tight)



- Extension to **Gaussian channels** and **private capacity** (key generation) in [Wilde, Tomamichel, B. arXiv:1602.08898]
- What happens for **very small n** =1,2,3,…?

  —> extend efficiently computable bounds from, e.g.:
  [Matthews and Wehner, IEEE Trans. on Info. Th. (2014)],
  [Leung and Matthews, IEEE Trans. on Info. Th. (2015)]
- Study explicit and efficient quantum codes (vs. information-theoretic limit studied here)



Ex: qubit dephasing channel

Thanks!

Extra: Qubit Depolarizing Channel I

- $\mathcal{D}_\alpha : \rho \mapsto (1-\alpha)\rho + \frac{\alpha}{3}(X\rho X + Y\rho Y + Z\rho Z)$ with $\alpha \in [0,1]$ and

—> but $Q(\mathcal{D}_\alpha) = ?$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \; Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \; Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Only **lower and upper bounds** on the quantum capacity, super-additivity of coherent information:

$$1 - h(\alpha) - \alpha \log 3 = I_c(\mathcal{D}_\alpha) < Q(\mathcal{D}_\alpha) \leq \min\{\underbrace{1 - h(\alpha)}_{= Q(\mathcal{Z}_\alpha)}, 1 - 4\alpha\}$$

(slightly better upper bounds known)

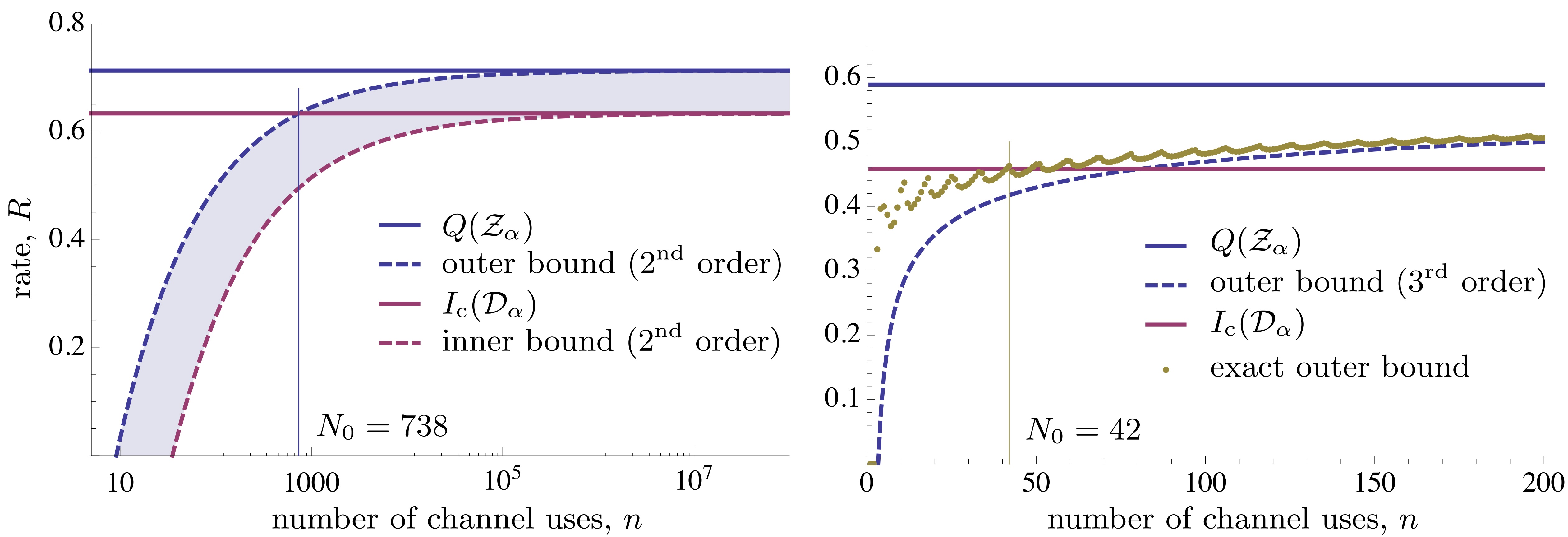
- How many qubits do we need to **coherently manipulate** to witness super-additivity?

- We show **finite resources** converse bound: $\hat{R}_{\mathcal{D}_\alpha}(n;\epsilon) \leq \hat{R}_{\mathcal{Z}_\alpha}(n;\epsilon)$

(where $\mathcal{Z}_\alpha$ is the qubit dephasing channel)

Extra: Qubit Depolarizing Channel II

- $\mathcal{D}_\alpha : \rho \mapsto (1-\alpha)\rho + \frac{\alpha}{3}(X\rho X + Y\rho Y + Z\rho Z)$ with $\alpha \in [0,1]$, but $Q(\mathcal{D}_\alpha) = ?$
- Known bound: $I_c(\mathcal{D}_\alpha) \leq Q(\mathcal{D}_\alpha) \leq Q(\mathcal{Z}_\alpha)$
- We show: $\hat{R}_{\mathcal{D}_\alpha}(n;\epsilon) \leq \hat{R}_{\mathcal{Z}_\alpha}(n;\epsilon)$



(a) Inner and outer bounds for $\alpha = 0.05$ and $\varepsilon = 1\%$. (b) Exact outer bound for $\alpha = 0.0825$ and $\varepsilon = 5.5\%$.