One-Shot Quantum Information Theory II: Information transmission

Nilanjana Datta
University of Cambridge,U.K.

UNIVERSITY OF CAMBRIDGE

- *Consider transmission of information through quantum channels in the the one-shot setting:*

  - *transmission of quantum information…..*

  - *and – if time permits - transmission of classical information…….*

- *See how......*
  - *some of the smooth entropies discussed in the previous lecture arise as operational quantities for these tasks.*
  - *the known results for the asymptotic memoryless setting can be obtained from these one-shot results.*

UNIVERSITY OF CAMBRIDGE

Notations & Definitions

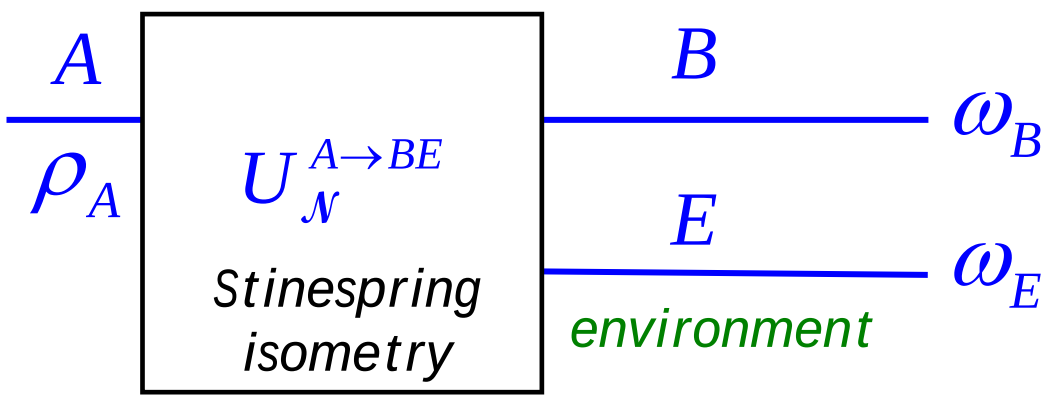
- **Quantum channel :** $\mathcal{N}^{A\to B}$.

- **Stinespring isometry** of $\mathcal{N}$: $U_{\mathcal{N}}^{A\to BE}$

$$\omega_B := \mathcal{N}^{A\to B}(\rho_A) = \mathrm{Tr}_E U_{\mathcal{N}}^{A\to BE}(\rho_A)$$

- **Complementary channel**: $\tilde{\mathcal{N}}^{A\to E}$,

$$\omega_E := \tilde{\mathcal{N}}^{A\to E}(\rho_A) = \mathrm{Tr}_B U_{\mathcal{N}}^{A\to BE}(\rho_A)$$



UNIVERSITY OF CAMBRIDGE

Mathematical Tools

(1) Choi-Jamilkowski (C-J) Isomorphism

Quantum operations ⟷ Positive operators

Let $\mathcal{H}_R \simeq \mathcal{H}_A$ with orthonormal basis $\{|i\rangle\}_{i=1}^{d}$

$$\Phi_{RA} := |\Phi_{RA}\rangle\langle\Phi_{RA}|; \qquad |\Phi_{RA}\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i\rangle|i\rangle \in \mathcal{H}_R \otimes \mathcal{H}_A$$

maximally entangled state (MES)

- **C-J state of a quantum operation** $\Lambda^{A\to B}$ **:**

$$\sigma_{RB} := \left(\mathrm{id}_R \otimes \Lambda^{A\to B}\right)\Phi_{RA} \in \mathcal{P}(\mathcal{H}_R \otimes \mathcal{H}_A)$$

UNIVERSITY OF CAMBRIDGE

Smooth entropies

- *Relative entropies* $D_{\max}(\rho\|\sigma), D_0(\rho\|\sigma), D_{\min}(\rho\|\sigma)$

  -- their smoothed versions $D^{\varepsilon}_{\max}(\rho\|\sigma), D^{\varepsilon}_{H}(\rho\|\sigma)$.....

- *Min-/max- entropies* $H_{\min}(A|B)_\rho, H_0(\rho), H_{\max}(A|B)_\rho$ etc.

  -- their smoothed versions $H^{\varepsilon}_{\min}(A|B)_\rho, H^{\varepsilon}_{\max}(A|B)_\rho$,....

Let's recall their definitions and some properties

UNIVERSITY OF CAMBRIDGE

Entropies

$$H_{\min}(A|B)_\rho := \max_{\sigma_B}\left\{-D_{\max}(\rho_{AB}\,\|\,I_A\otimes\sigma_B)\right\}$$

$$= \max_{\sigma_B}\left\{-\log\lambda_{\max}\left((I_A\otimes\sigma_B^{-1/2})\rho_{AB}(I_A\otimes\sigma_B^{-1/2})\right)\right\}$$

$$H_{\max}(A|B)_\rho := \max_{\sigma_B}\left\{-D_{\min}(\rho_{AB}\,\|\,I_A\otimes\sigma_B)\right\}$$

$$= \max_{\sigma_B}\left\{2\log F(\rho_{AB}, I_A\otimes\sigma_B)\right\}$$

$$H^{\varepsilon}_{\min}(A|B)_\rho := \max_{\bar\rho\in B^{\varepsilon}(\rho)} H_{\min}(A|B)_{\bar\rho};$$

$$H^{\varepsilon}_{\max}(A|B)_\rho := \min_{\bar\rho\in B^{\varepsilon}(\rho)} H_{\max}(A|B)_{\bar\rho};$$

- If $\rho_{RA} = \Phi^m_{RA};$ MES $|\Phi^m_{RA}\rangle = \frac{1}{\sqrt{m}}\sum_{i=1}^{m}|i\rangle|i\rangle$

$$H^{\varepsilon}_{\min}(A|R)_\rho \geq H_{\min}(A|R)_\rho = -\log m = H_{\max}(A|R)_\rho$$

UNIVERSITY OF CAMBRIDGE

Smooth entropies

Duality of smoothed min- and max- entropies: *[Colbeck, Renner Tomamichel]*

For any purification ρ_{ABC} of a bipartite state ρ_{AB}

$$H^{\varepsilon}_{\min}(A|B)_{\rho} = -H^{\varepsilon}_{\max}(A|C)_{\rho}$$

Data-processing inequality:

- e.g. If $\tilde{\omega}_{RA} = (\mathrm{id}_R \otimes \Lambda^{B\to A})\omega_{RB}$

(quantum operation)

$$H^{\varepsilon}_{\max}(R|B)_{\omega} \le H^{\varepsilon}_{\max}(R|A)_{\tilde{\omega}}$$

One-shot to asymptotics

- *Relation between smooth entropies & quantum entropies*

$$\forall \varepsilon > 0: \quad \lim_{n\to\infty} \frac{1}{n} D^{\varepsilon}_{\max}(\rho^{\otimes n} \| \sigma^{\otimes n}) \quad = D(\rho \| \sigma)$$

[Audenaert, Mosonyi, Verstraete ; Tomamichel; ND &Renner]

	$\forall \varepsilon > 0: \lim_{n\to\infty} \frac{1}{n} H^{\varepsilon}_{\min}(A\|B)_{\rho_{AB}^{\otimes n}} = H(A\|B)_{\rho}$
QAEP	$\forall \varepsilon > 0: \lim_{n\to\infty} \frac{1}{n} H^{\varepsilon}_{\max}(A\|B)_{\rho_{AB}^{\otimes n}} = H(A\|B)_{\rho}$

[Colbeck, Renner, Tomamichel; Tomamichel]

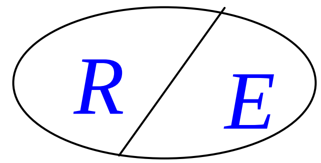
These results allow us to recover the results of the
"asymptotic memoryless setting"
from those of the "one-shot setting"

Mathematical Tools contd.

(II) Decoupling: -- a central concept in quantum info theory

- Has wide-ranging applications:
  - transmission of quantum information
  - other protocols, e.g. state merging, coherent state merging, …...
  - thermodynamics
  - black hole information theory
  - etc.

Mathematical Toolkit contd.



(II) Decoupling:

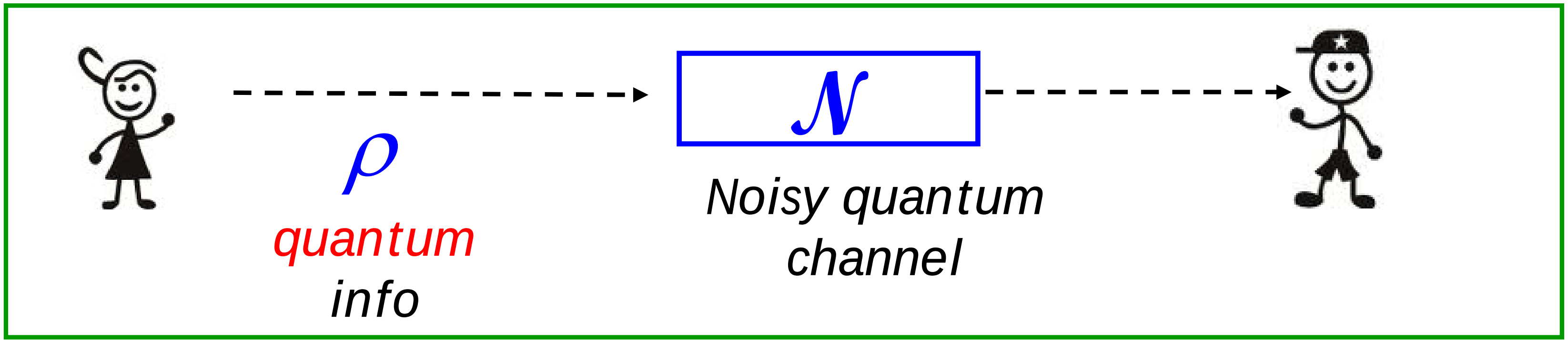
- Consider a composite system RE in a joint state ω_{RE}
- The subsystem R is decoupled (or uncorrelated) from E

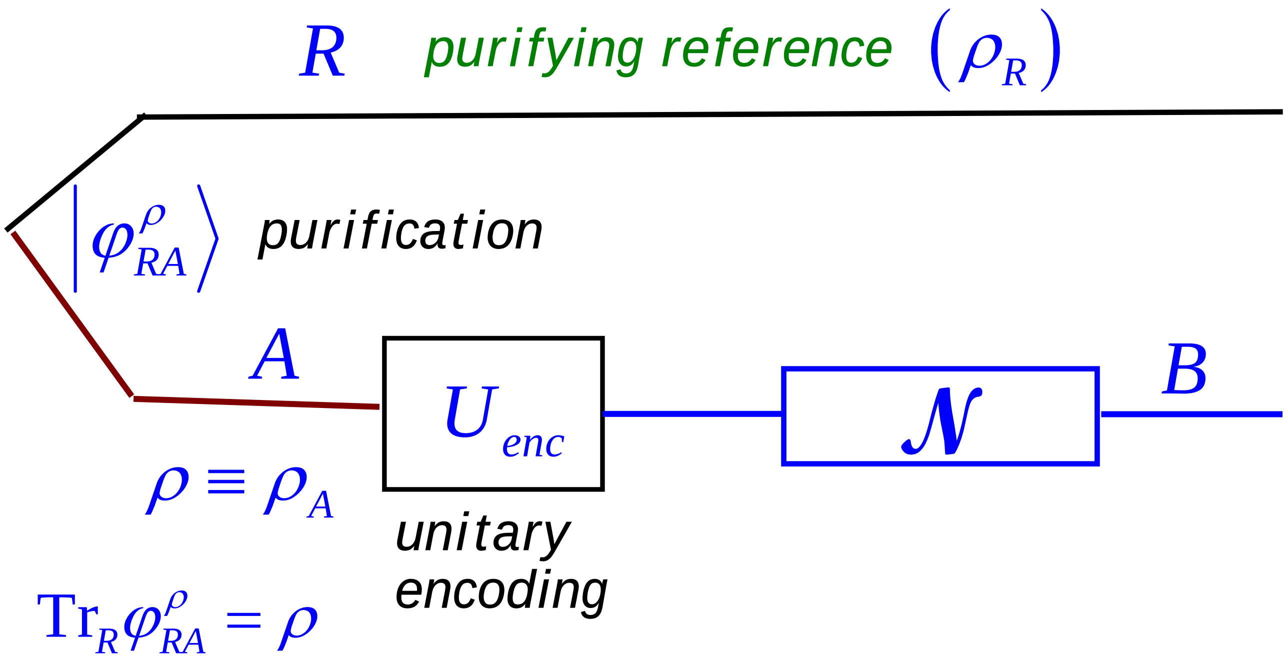
  if:

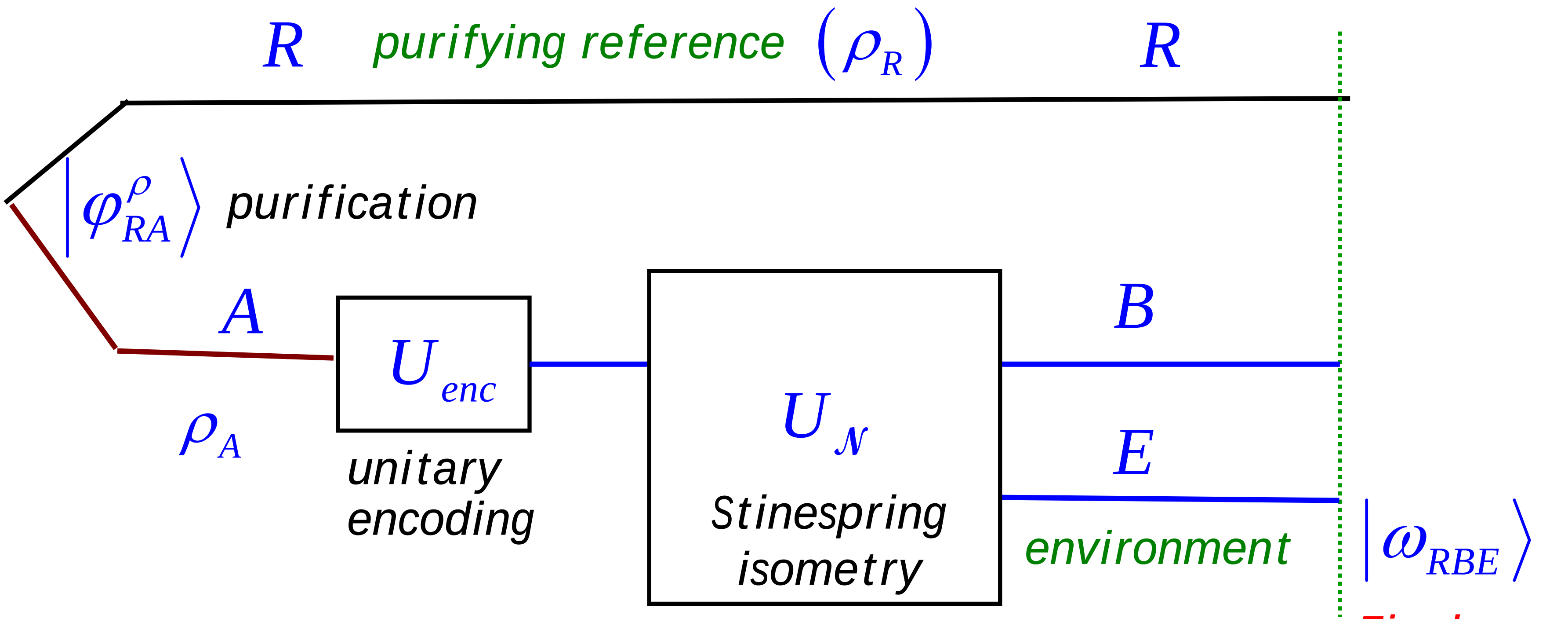
$$\omega_{RE} = \rho_R \otimes \sigma_E$$

- The outcome of any measurement on R is statistically independent of any measurement on E
- The system R does not give any information about system E

(I) Transmission of quantum information




R purifying reference (ρ_R)
$|\varphi_{RA}^{\rho}\rangle$ purification
A
U_{enc}
$\mathcal{N}$
B
$\rho \equiv \rho_A$
unitary encoding
$\mathrm{Tr}_R \varphi_{RA}^{\rho} = \rho$

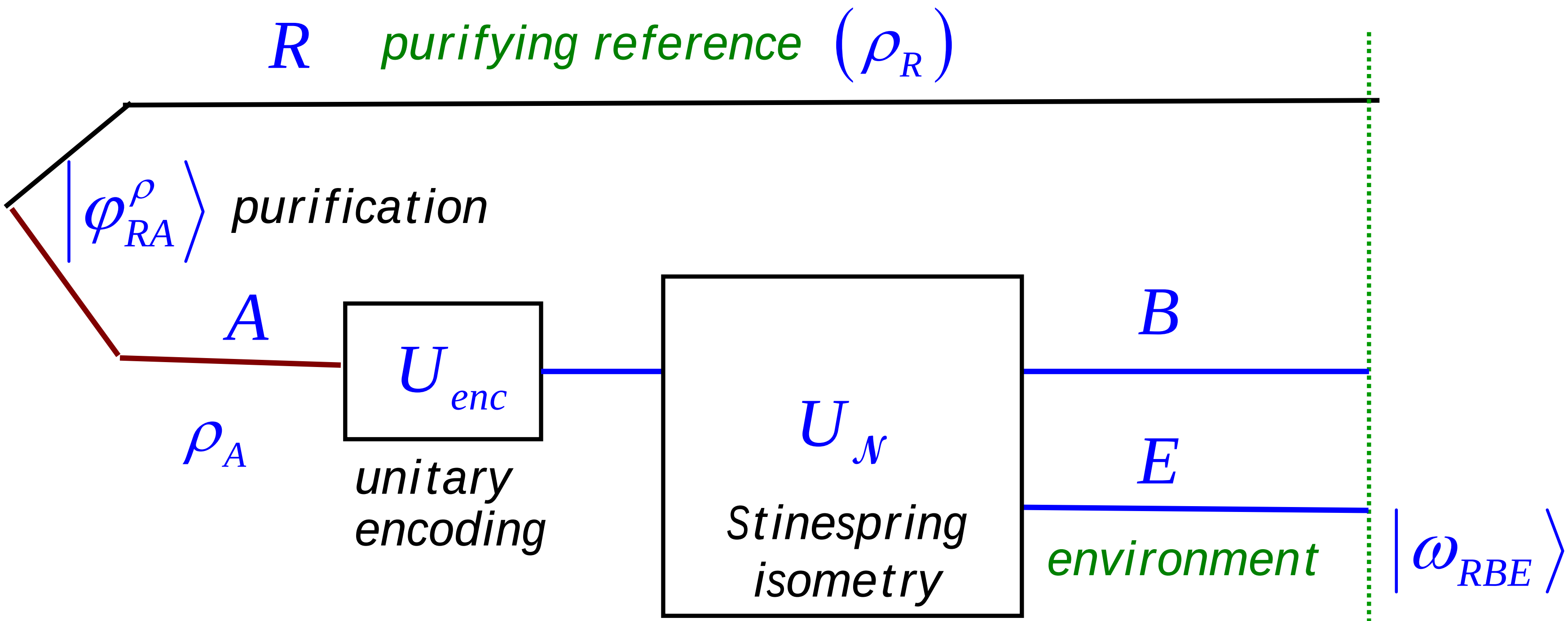


- Let U_{enc} be such that ω_{RE} satisfies:

$$\omega_{RE} = \rho_R \otimes \sigma_E$$

(decoupled)

for some state σ_E



- Let U_{enc} be such that ω_{RBE} satisfies:

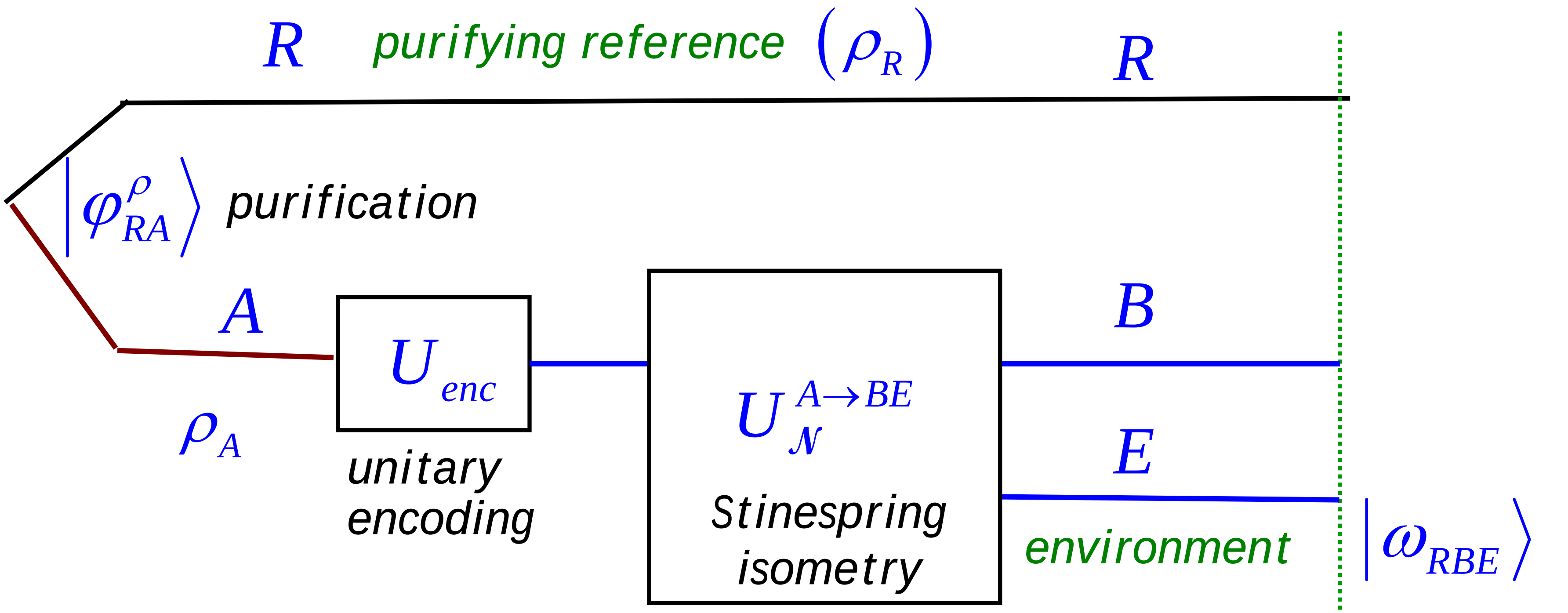
$$\omega_{RE} = \rho_R \otimes \sigma_E$$

(decoupled)

for some state σ_E

purifications

$|\omega_{RBE}\rangle$ — related by a partial isometry — $|\varphi^{\rho}_{RA}\rangle \otimes |\sigma_{EE'}\rangle$:



- *Let* U_{enc} *be such that* ω_{RBE} *satisfies:*

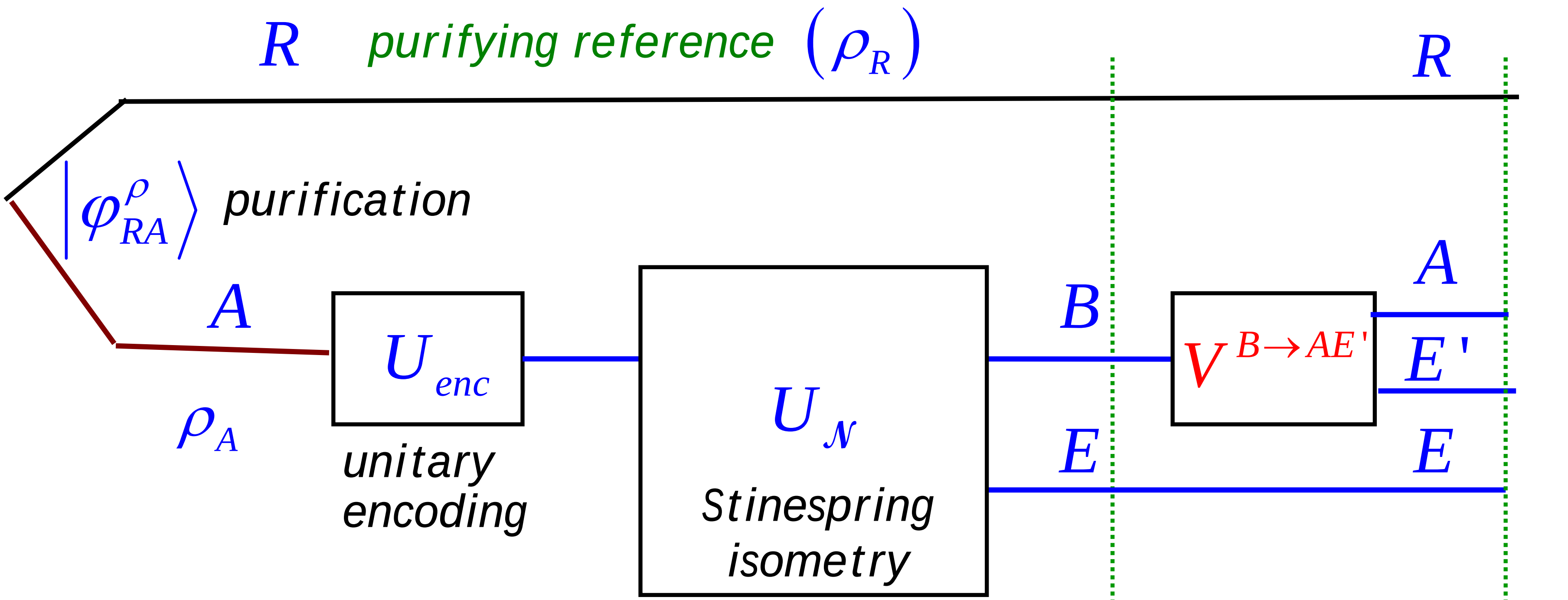
$$\omega_{RE} = \rho_R \otimes \sigma_E$$

(decoupled)

$\exists$ *a partial isometry* $V^{B\to AE'}$ *such that*

$$V^{B\to AE'}|\omega_{RBE}\rangle = |\varphi^{\rho}_{RA}\rangle \otimes |\sigma_{EE'}\rangle$$

This acts as Bob's decoding!

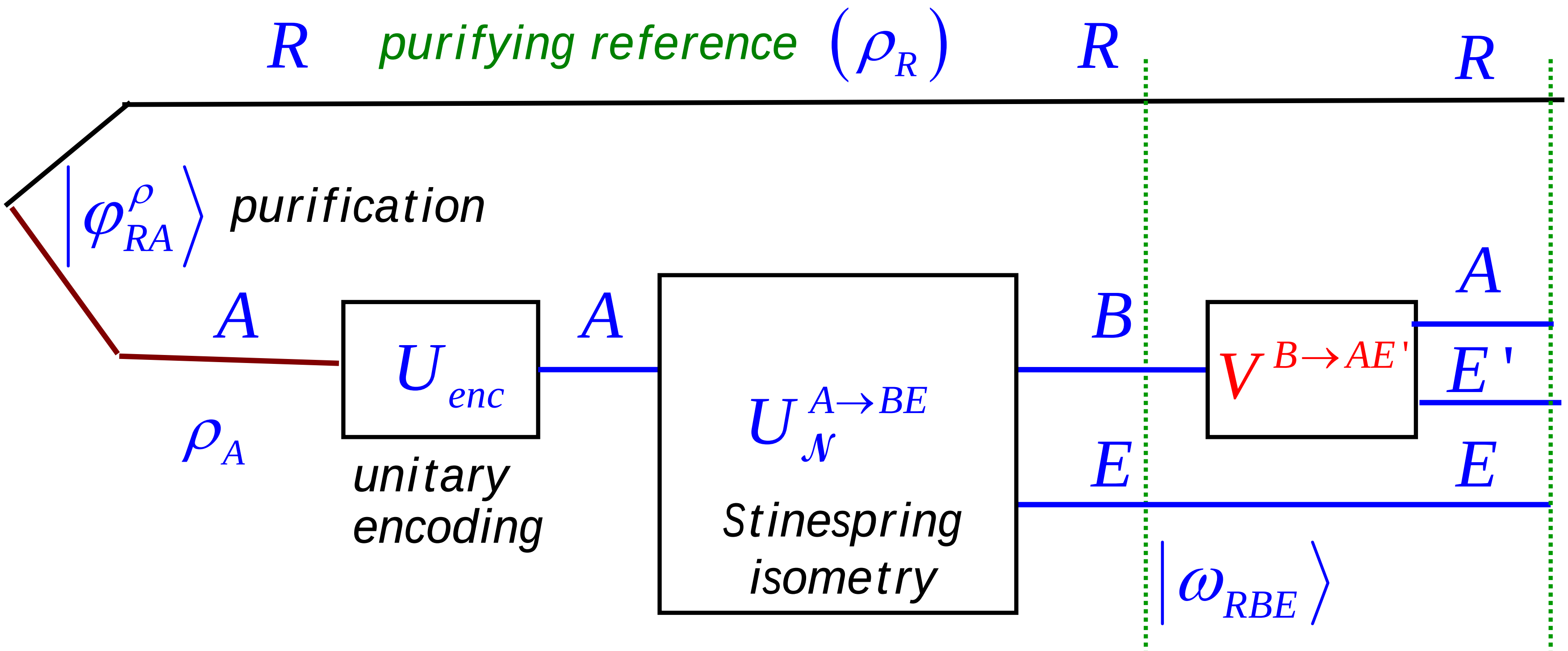


$$V^{B\to AE'}|\omega_{RBE}\rangle = |\varphi_{RA}^{\rho}\rangle \otimes |\sigma_{EE'}\rangle$$

- *Final state in Bob's possession:* $\mathrm{Tr}_{RE}\left(\varphi_{RA}^{\rho} \otimes \sigma_{EE'}\right) = \rho_A \otimes \sigma_{E'}$
- *Bob traces out over the system* E':

$$\mathrm{Tr}_{E'}\left(\rho_A \otimes \sigma_{E'}\right) = \rho_A$$ *to recover Alice's message !*

UNIVERSITY OF CAMBRIDGE



Thus: If U_{enc} *be such that* ω_{RE} *is decoupled:*

$$\omega_{RE} = \rho_R \otimes \sigma_E$$

then Bob can recover Alice's message!

UNIVERSITY OF CAMBRIDGE

- In fact, if $\omega_{RE} \overset{\varepsilon}{\approx} \rho_R \otimes \sigma_E$ (approximately decoupled)

  that is, $F\left(\omega_{RE}, \rho_R \otimes \sigma_E\right) \geq 1-\varepsilon$ for some $\varepsilon \geq 0$:

then $\exists$ a decoder such that after decoding Bob has

a state $\overset{\varepsilon}{\approx} \rho_A$ (Alice's message)

- This follows from Uhlmann's theorem:

Let $\rho, \sigma \in \mathcal{D}(\mathcal{H}_A)$, purifications $\left|\varphi^{\rho}_{AR}\right\rangle, \left|\psi^{\sigma}_{AR'}\right\rangle$

$$F\left(\rho, \sigma\right) = \max_{V^{R\to R'}} \left|\left\langle \psi^{\sigma}_{AR'} \right| V^{R\to R'} \left| \varphi^{\rho}_{AR} \right\rangle\right|$$

$$1-\varepsilon \leq F\left(\omega_{RE}, \rho_R \otimes \sigma_E\right) = \max_{V^{B\to AE'}} \left|\left\langle \varphi^{\rho}_{RA} \otimes \sigma_{EE'} \right| V^{B\to AE'} \left| \omega_{RBE} \right\rangle\right|$$

UNIVERSITY OF CAMBRIDGE

$$1-\varepsilon \le F\left(\omega_{RE}, \rho_R \otimes \sigma_E\right) = \max_{V^{B\to AE'}} \left| \left\langle \varphi^{\rho}_{RA} \otimes \sigma_{EE'} \right| V^{B\to AE'} \left| \omega_{RBE} \right\rangle \right|$$

The optimizing partial isometry $V^{B\to AE'}$ *acts as Bob's decoding*

Bob ends up with a state $\overset{\varepsilon}{\approx} \mathrm{Tr}_{RE}\left(\varphi^{\rho}_{RA} \otimes \sigma_{EE'}\right) \overset{\varepsilon}{\approx} \rho_A \otimes \omega_{E'}$

And after doing a partial trace over E', *he ends up with*

a state $\overset{\varepsilon}{\approx} \rho_A$ *(Alice's message)*

i.e., Bob ends up with a state which is ε*-close*

to the quantum state that Alice sent

- *In a nutshell:*

For transmission of quantum information thro' a noisy channel $\mathcal{N}$ in the one-shot setting (up to an error ε), require:

$$\omega_{RE} \overset{\varepsilon}{\approx} \rho_R \otimes \sigma_E$$

(state before decoding)

i.e., the state of the reference system R is (approxly.) decoupled from the state of the environment E of $\mathcal{N}$.

UNIVERSITY OF CAMBRIDGE

History (decoupling)

First explicit use of decoupling in the Q.Info. Theory literature:

- *B. Schumacher & M.D.Westmoreland*

  (quantum error correction)

- *M.Horodecki, J.Oppenheim & A.Winter*

  (state merging)

- *A.Abeysinghe, I.Devetak, P.Hayden, A.Winter*

  (coherent state merging - FQSW)

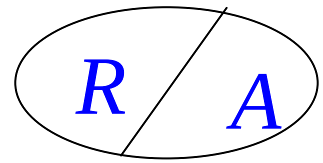
- *P.Hayden, M.Horodecki, J.Yard & A.Winter*

  (quantum info transmission)

"asymptotic memoryless setting"

UNIVERSITY OF CAMBRIDGE

Decoupling Theorem



States conditions under which 2 subsystems of a bipartite system can become almost uncorrelated (decoupled)

Rough idea: *Initially* ρ_{RA} : *possibly correlated*

- *Consider a unitary evolution of system* A *alone:*

$$(I \otimes U)\rho_{RA}(I \otimes U^\dagger)$$

- *Then consider an arbitrary quantum operation on* A

e.g. $\Lambda \equiv \Lambda^{A \to E}$: $\omega_{RE} := (\mathrm{id} \otimes \Lambda)\Big((I \otimes U)\rho_{RA}(I \otimes U^\dagger)\Big)$

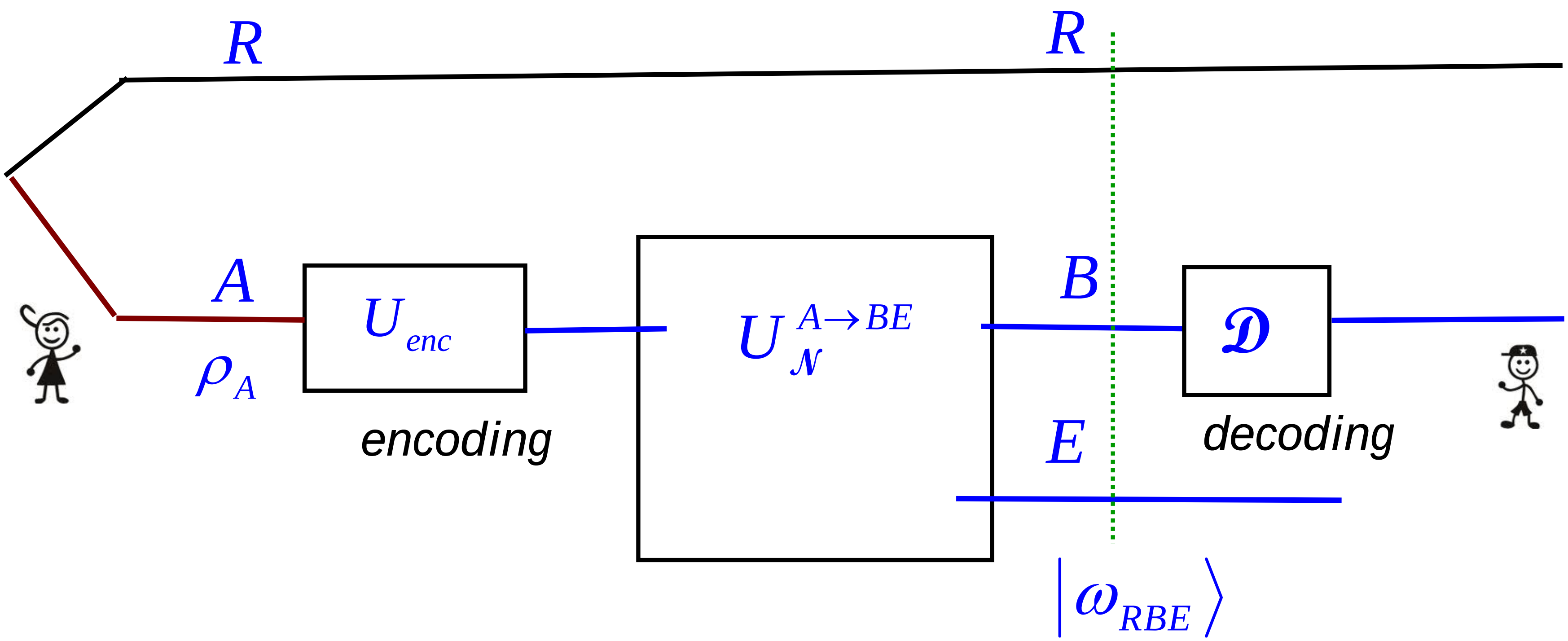
- *Decoupling theorem provides a bound on the distance of a typical resulting state from a decoupled state:*

  i.e., bound on $\| \omega_{RE} - \rho_R \otimes \sigma_E \|_1$

Decoupling Theorem

$$\rho_{RA} \to (I \otimes U)\rho_{RA}(I \otimes U^\dagger) \to (\mathrm{id} \otimes \Lambda)\big((I \otimes U)\rho_{RA}(I \otimes U^\dagger)\big) \equiv \omega_{RE};$$

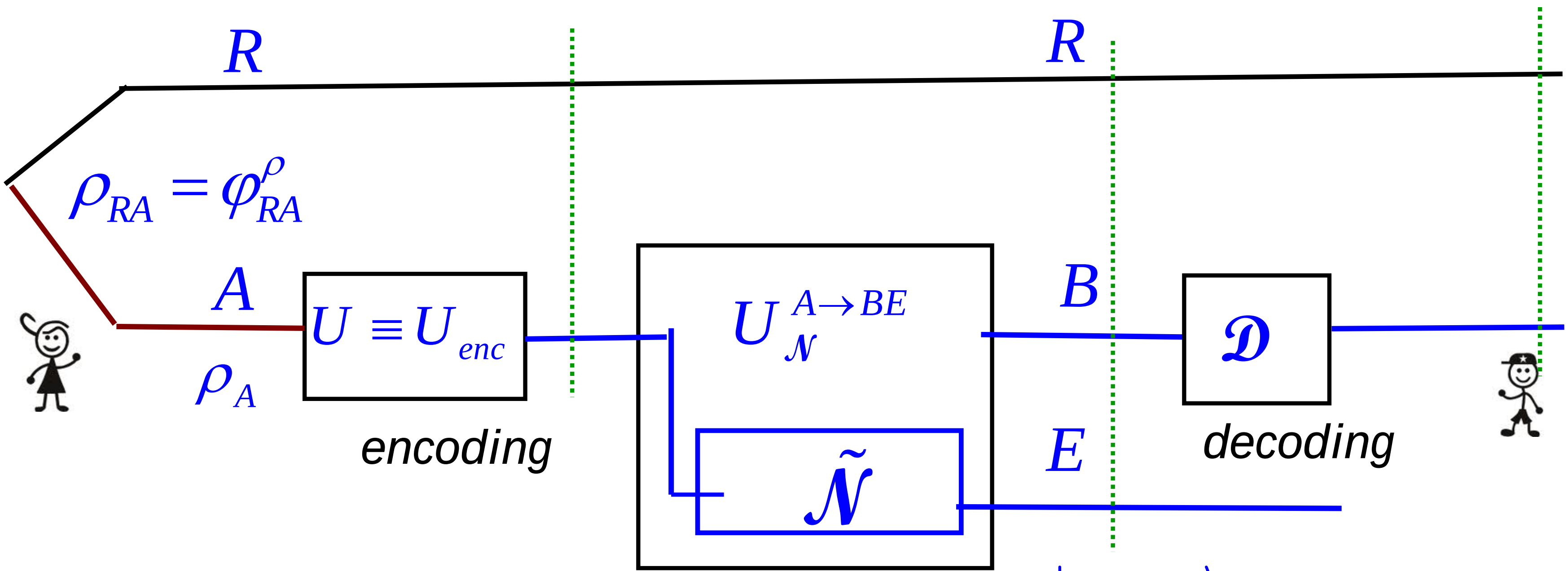
- *For quantum info transmission through a noisy channel:*



Decoupling Theorem

$$\rho_{RA} \to (I \otimes U)\rho_{RA}(I \otimes U^{\dagger}) \to (\mathrm{id} \otimes \Lambda)\big((I \otimes U)\rho_{RA}(I \otimes U^{\dagger})\big) \equiv \omega_{RE};$$

- *For quantum info transmission through a noisy channel:*



$$|\omega_{RBE}\rangle$$

$\Lambda^{A \to E} \equiv \tilde{\mathcal{N}}^{A \to E}$: *complementary channel*

$$\boxed{\omega_{RE} = (\mathrm{id} \otimes \tilde{\mathcal{N}})\big((I \otimes U)\rho_{RA}(I \otimes U^{\dagger})\big)}$$

History (decoupling) contd.

- *Decoupling theorem provides a bound on*

$$\| \omega_{RE} - \rho_R \otimes \sigma_E \|_1 \qquad \omega_{RE} \equiv \omega_{RE}(U)$$

One-shot setting : decoupling theorems in which the bound on $\| \omega_{RE} - \rho_R \otimes \sigma_E \|_1$ is given in terms of min/max entropies:

- [Berta], [Buscemi &ND], [Berta, Christandl, Renner], [ND, Hsieh]
- [Dupuis];
- [Dupuis, Berta, Wullschleger, Renner]

(decoupling condition expressed in terms of C-J state of the quantum operation)

UNIVERSITY OF CAMBRIDGE

- **One-shot decoupling theorem:** *[Dupuis et al]*

Let $\varepsilon > 0;\quad \Lambda^{A\to E}:$ *(quantum operation)*

$$\sigma_{A'E} = (\mathrm{id}_{A'} \otimes \Lambda)\Phi_{A'A}$$ *C-J state of* Λ

Then for any state ρ_{RA},

$$\int \| (\mathrm{id} \otimes \Lambda)((I \otimes U)\rho_{RA}(I \otimes U^\dagger)) - \rho_R \otimes \sigma_E \|_1 \, dU$$

$$[= \omega_{RE}(U)]$$

$$\overset{\varepsilon}{\leq} 2^{-\frac{1}{2}H_{\min}^{\varepsilon}(A|R)_\rho - \frac{1}{2}H_{\min}^{\varepsilon}(A'|E)_\sigma}$$

$\int \bullet \, dU$: *integral over the Haar measure on the full unitary group over* $\mathcal{H}_A$

$$\sigma_E = \mathrm{Tr}_{A'}\sigma_{A'E}$$

UNIVERSITY OF CAMBRIDGE

- **One-shot decoupling theorem:** *[Dupuis et al]*

Let $\varepsilon > 0; \quad \Lambda^{A \to E} \equiv \tilde{\mathcal{N}}^{A \to E};$ *(quantum operation)*

$$\sigma_{A'E} = (\mathrm{id}_{A'} \otimes \Lambda)\Phi_{A'A}$$ *C-J state of* Λ

Then for any state ρ_{RA},

$$\int \| (\mathrm{id} \otimes \Lambda)((I \otimes U)\rho_{RA}(I \otimes U^{\dagger})) - \rho_R \otimes \sigma_E \|_1 \, dU$$

$$\overset{\varepsilon}{\leq} 2^{-\frac{1}{2}H_{\min}^{\varepsilon}(A|R)_\rho - \frac{1}{2}H_{\min}^{\varepsilon}(A'|E)_\sigma}$$

$\int \bullet \, dU$: *integral over the Haar measure on the full unitary group over* $\mathcal{H}_A$

$$\sigma_E = \mathrm{Tr}_{A'} \sigma_{A'E}$$

UNIVERSITY OF CAMBRIDGE

- **One-shot decoupling theorem:** *[Dupuis et al]*

Let $\varepsilon > 0; \ \tilde{\mathcal{N}}^{A\to E}; \quad \sigma_{A'E} = (\mathrm{id}_{A'} \otimes \tilde{\mathcal{N}})\Phi_{A'A}$

C-J state of $\tilde{\mathcal{N}}$

Then for any state ρ_{RA},

$$\int \|\omega_{RE}(U) - \rho_R \otimes \sigma_E\|_1 \, dU \le 2^{-\frac{1}{2}H_{\min}^{\varepsilon}(A|R)_\rho - \frac{1}{2}H_{\min}^{\varepsilon}(A'|E)_\sigma} \quad \varepsilon$$

$$\omega_{RE}(U) = \omega_{RE} = (\mathrm{id} \otimes \tilde{\mathcal{N}})\big((I \otimes U)\rho_{RA}(I \otimes U^\dagger)\big)$$

$\int \bullet \, dU$: *integral over the Haar measure on the full unitary group over* $\mathcal{H}_A$

$$\sigma_E = \mathrm{Tr}_{A'}\sigma_{A'E}$$

- **One-shot decoupling theorem:** *[Dupuis et al]*

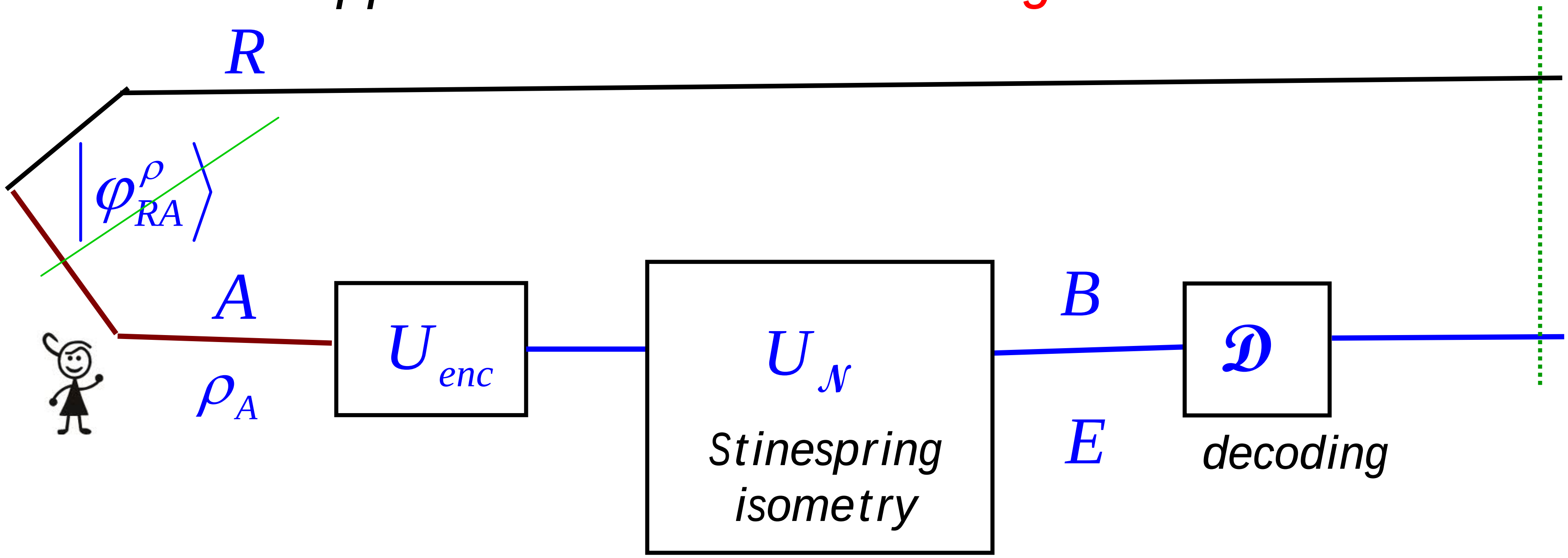
implies that: $\exists U :$

$$\| \omega_{RE}(U) - \rho_R \otimes \sigma_E \|_1 \leq^{\varepsilon} 2^{-\frac{1}{2} H_{\min}^{\varepsilon}(A|R)_\rho - \frac{1}{2} H_{\min}^{\varepsilon}(A'|E)_\sigma}$$

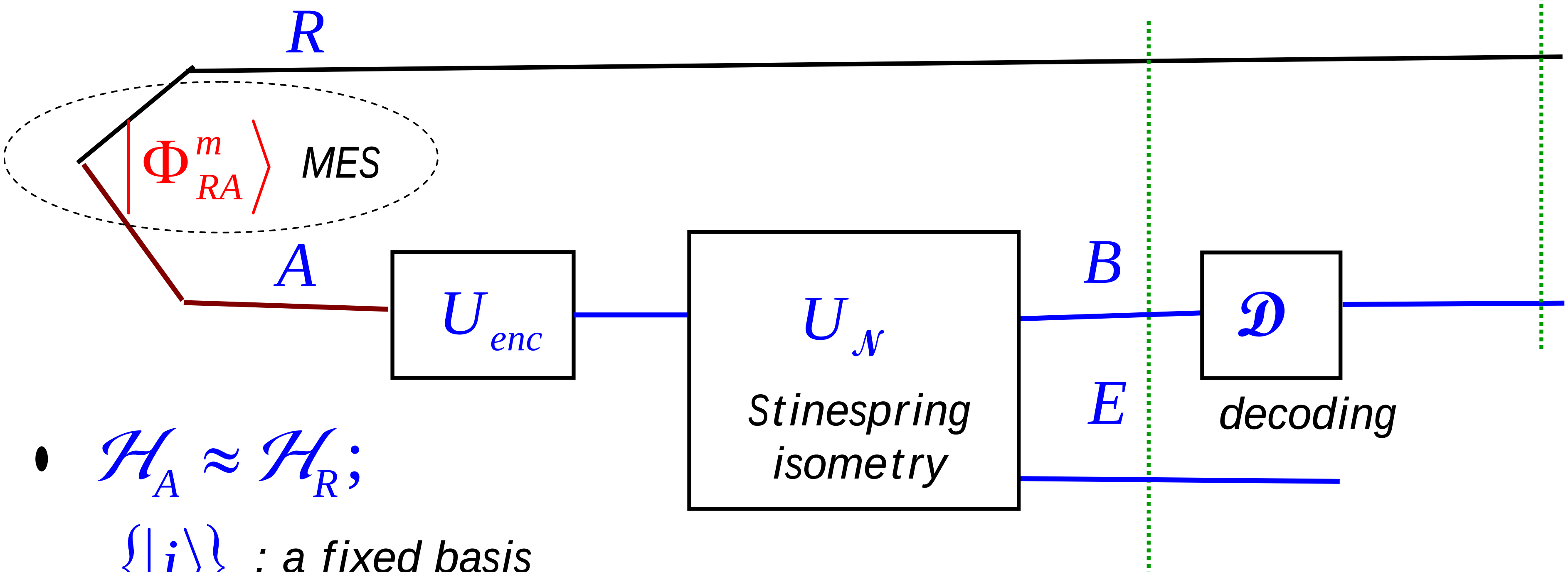
$$\omega_{RE}(U) = \omega_{RE} = (\mathrm{id} \otimes \tilde{\mathcal{N}})\Big((I \otimes U)\rho_{RA}(I \otimes U^\dagger)\Big)$$

$$\sigma_{A'E} = (\mathrm{id}_{A'} \otimes \tilde{\mathcal{N}})\Phi_{A'A}$$ C-J state of $\tilde{\mathcal{N}}$

Application: one-shot entanglement transmission



Application: one-shot entanglement transmission

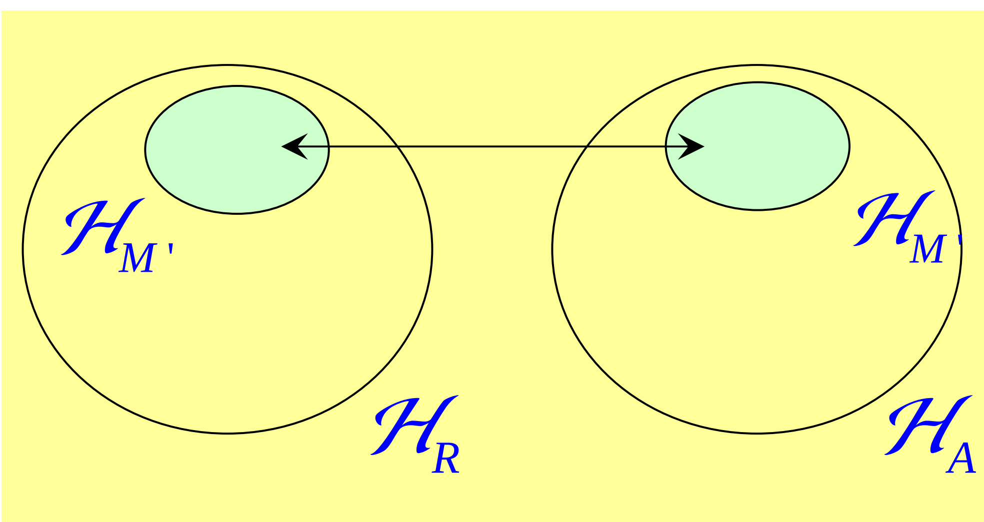


- $\mathcal{H}_A \approx \mathcal{H}_R$;

  $\{|i\rangle\}$: a fixed basis

$$|\Phi^m_{RA}\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle |i\rangle$$

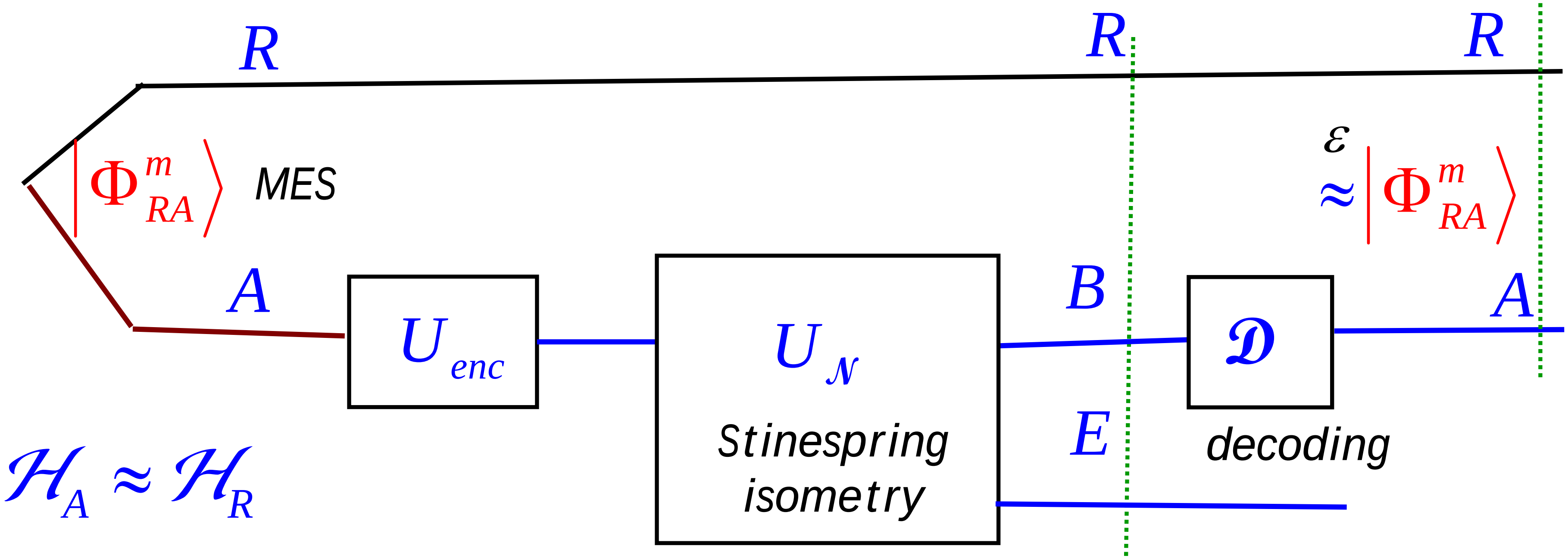
(a MES) $\in \mathcal{H}_{M'} \otimes \mathcal{H}_M$



$\mathcal{H}_M \approx \mathcal{H}_{M'}$;

$m = \dim \mathcal{H}_M$

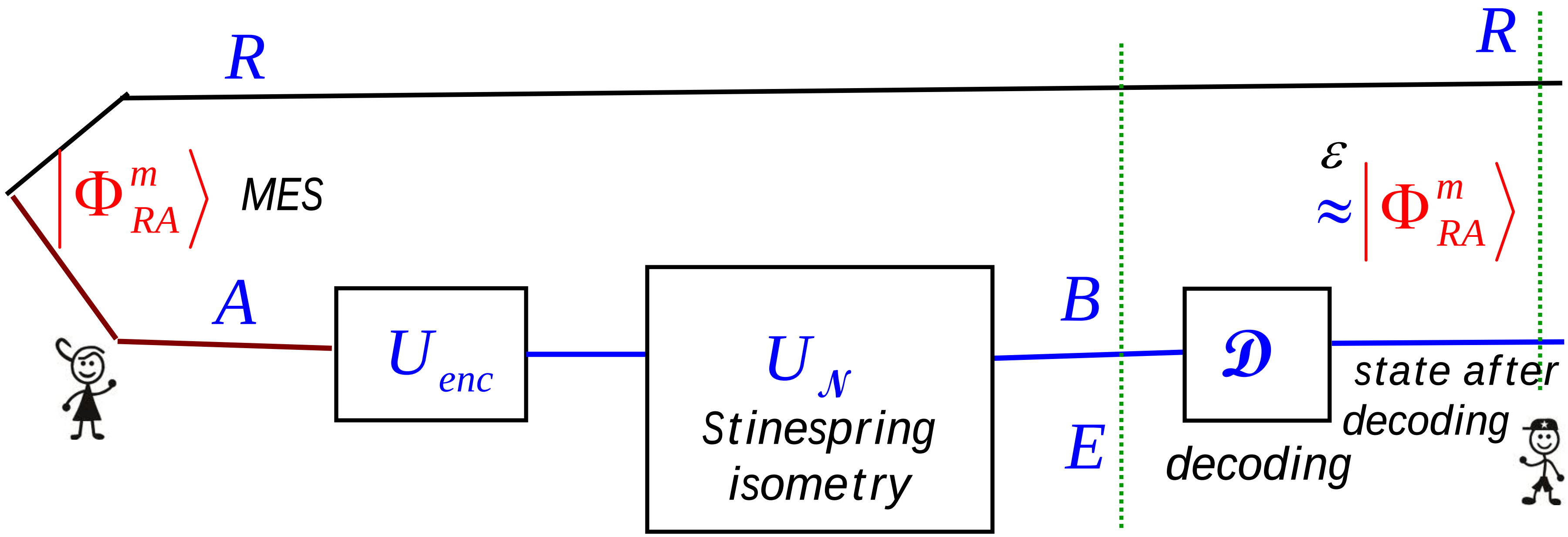
Application: one-shot entanglement transmission



$$|\Phi^m_{RA}\rangle \in \mathcal{H}_{M'} \otimes \mathcal{H}_M \subseteq \mathcal{H}_R \otimes \mathcal{H}_A$$

- Alice shares a MES with the inaccessible reference R
- Aim: to transmit her share of the entanglement to Bob
- such that – after decoding, the state that Bob shares with the reference is $\varepsilon -$ close to $|\Phi^m_{RA}\rangle$

Application: one-shot entanglement transmission

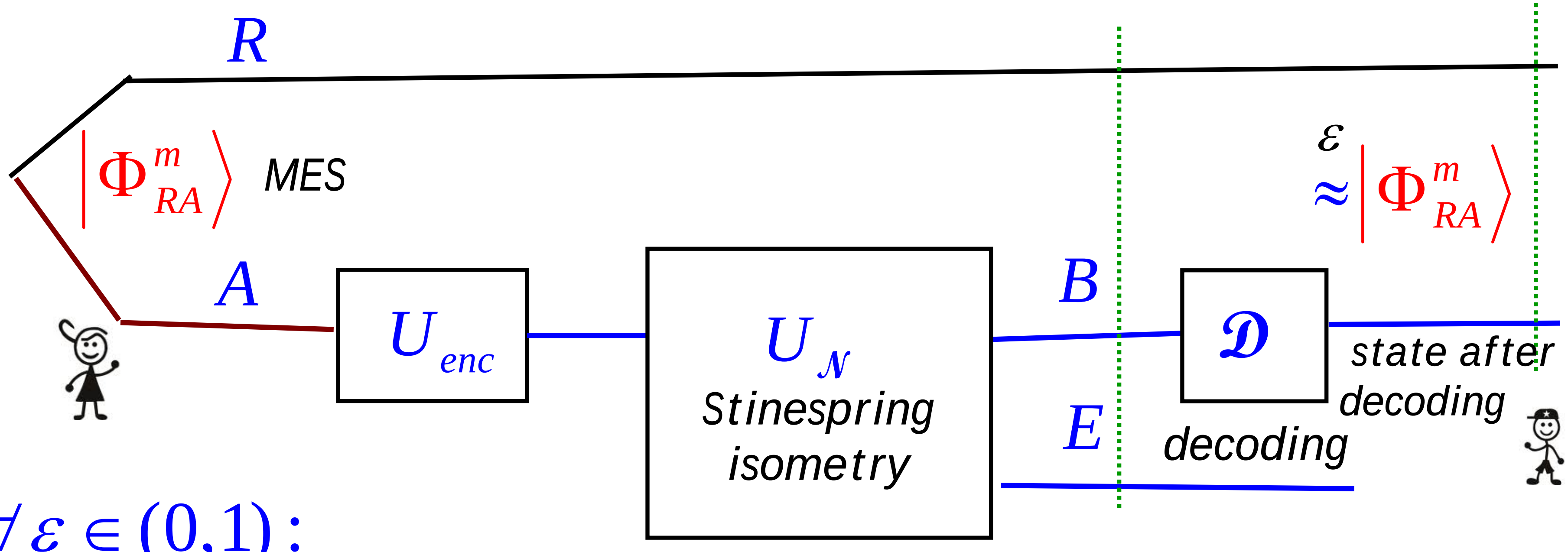


$|\Phi^m_{RA}\rangle$ = MES of Schmidt rank m,

number of ebits transmitted (up to error ε) $= \log m$

- Capacity $:=$ maximum number of ebits transmitted

Application: one-shot entanglement transmission



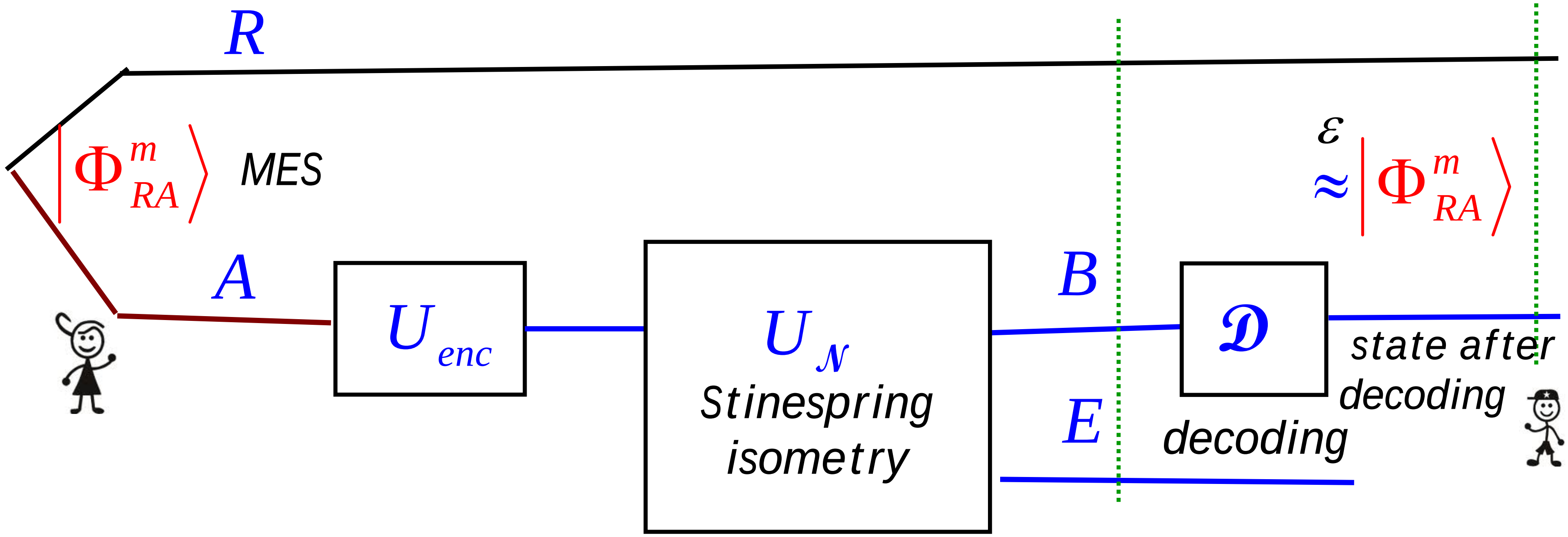
$\forall \varepsilon \in (0,1):$

One-shot $\varepsilon -$ *error entanglement-transmission capacity:*

$$Q^{(1),\varepsilon}_{et}(\mathcal{N}) := \sup\left\{ \log m : \text{ final state } \overset{\varepsilon}{\approx} \Phi^m_{RA} \right\}$$

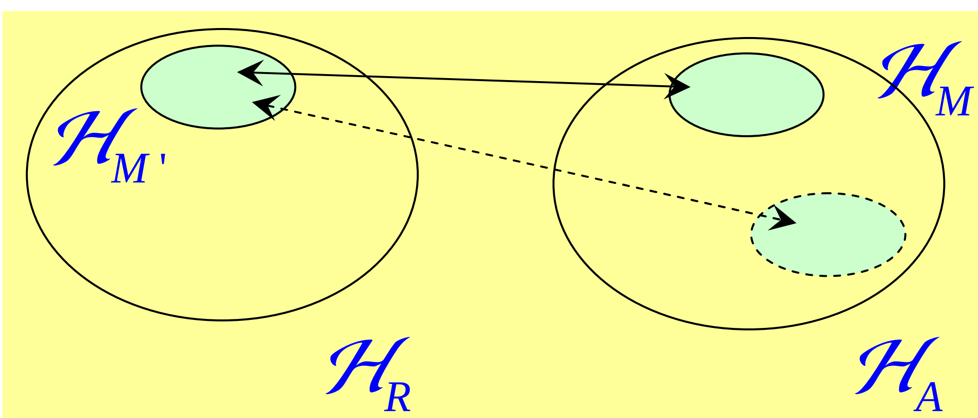
UNIVERSITY OF CAMBRIDGE

Application: one-shot entanglement transmission



Role of the encoding map: U_{enc}

To select a suitable coding subspace which is almost error-free



Application: one-shot entanglement transmission

- *Theorem: [ND, M-H.Hsieh; F.Buscemi & ND]*

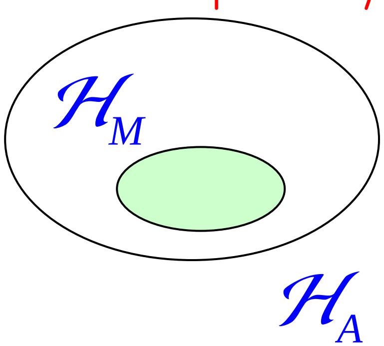
One-shot $\varepsilon -$ *error entanglement-transmission capacity,*

$\forall \varepsilon \in (0,1):$

$$Q_{et}^{(1),\varepsilon}(\mathcal{N}) \approx \max_{\mathcal{H}_M \subseteq \mathcal{H}_A} \left\{ -H_{\max}^{\varepsilon}(R|B)_{\sigma} \right\}$$

$$\sigma_{RB} = (\mathrm{id}_R \otimes \mathcal{N}^{A \to B}) \Phi_{RA}^m;$$

Since $|\Phi_{RA}^m\rangle \in \mathcal{H}_{M'} \otimes \mathcal{H}_M$, *action of* $\mathcal{N}$ *restricted to* $\mathcal{H}_M$



- σ_{RB} *depends on the choice of* $\mathcal{H}_M$
- *hence maximise over all* $\mathcal{H}_M \subseteq \mathcal{H}_A$

Application: one-shot entanglement transmission

- *Theorem: [ND, M-H.Hsieh; F.Buscemi & ND]*

One-shot $\varepsilon -$ *error entanglement-transmission capacity,*
$\forall \varepsilon \in (0,1):$

$$Q_{et}^{(1),\varepsilon}(\mathcal{N}) \approx \max_{\mathcal{H}_M \subseteq \mathcal{H}_A} \left\{ -H_{\max}^{\varepsilon}(R|B)_{\sigma} \right\}$$

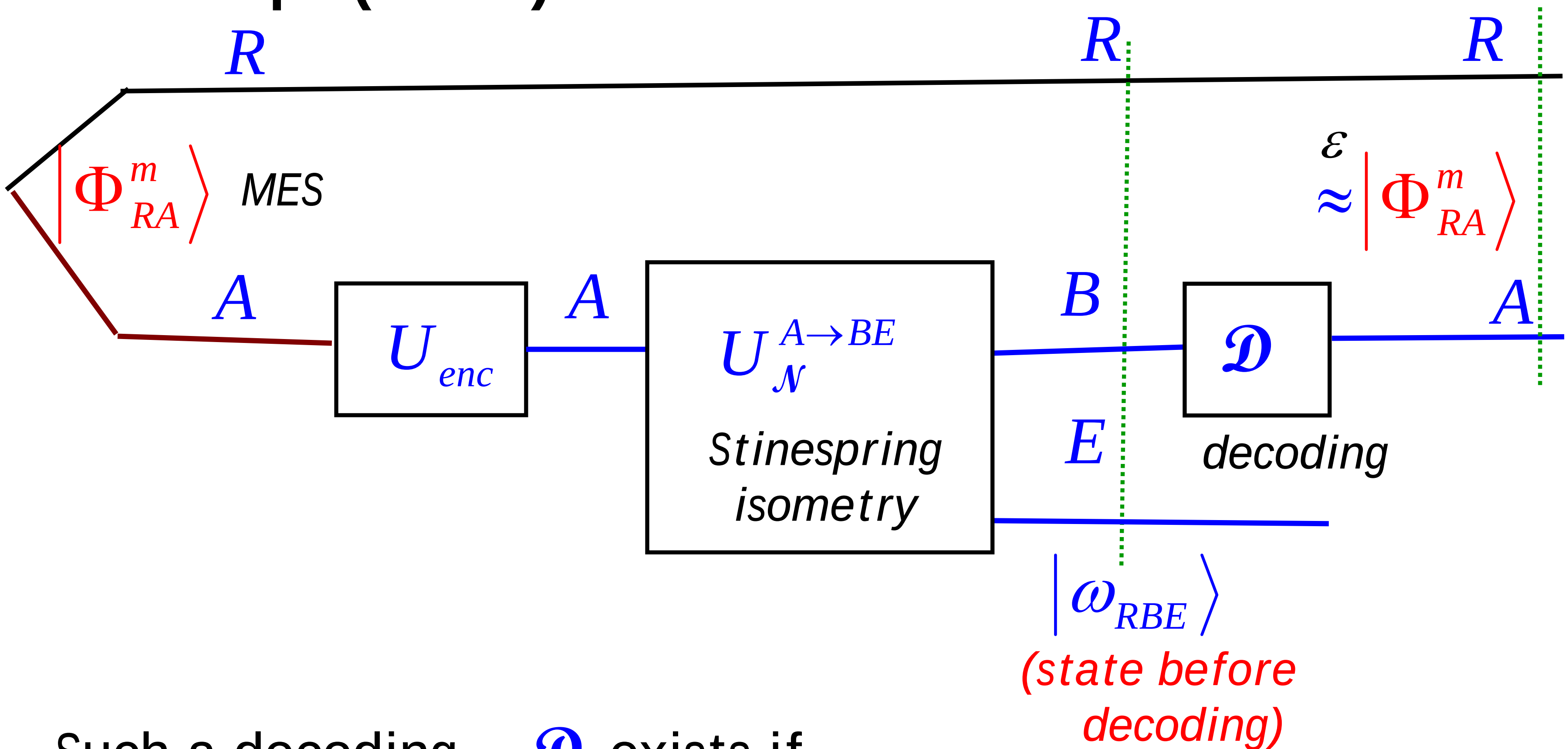
$$\max_{\mathcal{H}_M \subset \mathcal{H}_A} \left\{ -H_{\max}^{\varepsilon}(R|B)_{\sigma} \right\} + f(\varepsilon) \leq Q_{et}^{(1),\varepsilon}(\mathcal{N})$$

$$\leq \max_{\mathcal{H}_M \subset \mathcal{H}_A} \left\{ -H_{\max}^{\varepsilon}(R|B)_{\sigma} \right\}$$

- **Proof:** **Step I (Achievability) ;** *lower bound* **Step II (Converse)** *upper bound*

Application: one-shot entanglement transmission

- **Proof: Step I (Direct)** *lower bound*



- Such a decoding $\mathcal{D}$ exists if

$$\omega_{RE} \stackrel{\varepsilon}{\approx} \rho_R \otimes \sigma_E; \qquad \rho_R = \frac{I}{m}$$

(completely mixed state)

- Use one-shot decoupling theorem

- **One-shot decoupling theorem:** *[Dupuis et al]*

implies that: $\exists U:$

$$\| \omega_{RE}(U) - \rho_R \otimes \sigma_E \|_1 \leq^{\varepsilon} 2^{-\frac{1}{2} H_{\min}^{\varepsilon}(A|R)_{\Phi^m} - \frac{1}{2} H_{\min}^{\varepsilon}(R|E)_{\sigma}}$$

$$\omega_{RE}(U) = \omega_{RE} = (\mathrm{id} \otimes \tilde{\mathcal{N}})\Big((I \otimes U)\Phi_{RA}^m (I \otimes U^\dagger)\Big)$$

$$\sigma_{RE} = (\mathrm{id}_R \otimes \tilde{\mathcal{N}})\Phi_{RA}^m; \quad \text{C-J state of } \tilde{\mathcal{N}}$$

$$\because \rho_{RA} = \Phi_{RA}^m$$

- *since action of* $\mathcal{N}\,(\&\ \therefore \tilde{\mathcal{N}})$ *restricted to* $\mathcal{H}_M \subseteq \mathcal{H}_A$
- *and* Φ_{RA}^m *is a MES in* $\mathcal{H}_{M'} \otimes \mathcal{H}_M$

- **One-shot decoupling theorem:** *[Dupuis et al]*

implies that: $\exists U:$

$$\| \omega_{RE}(U) - \rho_R \otimes \sigma_E \|_1 \stackrel{\varepsilon}{\leq} 2^{-\frac{1}{2} H_{\min}^{\varepsilon}(A|R)_{\Phi^m} - \frac{1}{2} H_{\min}^{\varepsilon}(R|E)_{\sigma}} \quad ......(a)$$

$$\omega_{RE}(U) = \omega_{RE} = \; = (\mathrm{id} \otimes \tilde{\mathcal{N}})\Big((I \otimes U)\Phi_{RA}^m (I \otimes U^\dagger)\Big)$$

$$\sigma_{RE} = (\mathrm{id}_R \otimes \tilde{\mathcal{N}})\Phi_{RA}^m; \qquad \because \rho_{RA} = \Phi_{RA}^m$$

- Require : **RHS** of (a) to be small

$$\Rightarrow \; \| \omega_{RE} - \rho_R \otimes \sigma_E \|_1 \stackrel{\varepsilon}{\approx} 0 \; \Rightarrow \omega_{RE} \stackrel{\varepsilon}{\approx} \rho_R \otimes \sigma_E$$

(approx.) **decoupling!**

UNIVERSITY OF CAMBRIDGE

- **One-shot decoupling theorem:** *[Dupuis et al]*

implies that: $\exists U :$

$$\| \omega_{RE}(U) - \rho_R \otimes \sigma_E \|_1 \leq \varepsilon \, 2^{-\frac{1}{2} H^{\varepsilon}_{\min}(A|R)_{\Phi^m} - \frac{1}{2} H^{\varepsilon}_{\min}(R|E)_{\sigma}} \quad \text{......(a)}$$

Note: $H^{\varepsilon}_{\min}(A|R)_{\Phi^m} \geq -\log m$

$$\sigma_{RE} = (\mathrm{id}_R \otimes \tilde{\mathcal{N}})\Phi^m_{RA};$$

Purification: $|\sigma_{RBE}\rangle = (\mathrm{id}_R \otimes U^{A\to BE}_{\mathcal{N}})\Phi^m_{RA}$

Duality of smoothed min- and max- entropies: $H^{\varepsilon}_{\min}(R|E)_{\sigma} = -H^{\varepsilon}_{\max}(R|B)_{\sigma}$

$$\| \omega_{RE} - \rho_R \otimes \sigma_E \|_1 \overset{\varepsilon}{\leq} 2^{-\frac{1}{2}H^{\varepsilon}_{\min}(A|R)_{\Phi^m} - \frac{1}{2}H^{\varepsilon}_{\min}(R|E)_{\sigma}}$$

$$\| \omega_{RE} - \rho_R \otimes \sigma_E \|_1 \overset{\varepsilon}{\leq} 2^{\frac{1}{2}\log m + \frac{1}{2}H^{\varepsilon}_{\max}(R|B)_{\sigma}} \quad \text{.....(a)}$$

- **Decoupling occurs if:** RHS of (a) is small :

$$\log m = -H^{\varepsilon}_{\max}(R\,|\,B)_{\sigma} + f(\varepsilon);$$

- **One-shot entanglement transmission capacity:**

$$Q^{(1),\varepsilon}_{et}(\mathcal{N}) \geq \max_{\mathcal{H}_M \subseteq \mathcal{H}_A} \left\{ -H^{\varepsilon}_{\max}(R\,|\,B)_{\sigma} \right\} + f(\varepsilon)$$

■

UNIVERSITY OF CAMBRIDGE

In summary

- *We established the lower bound:*

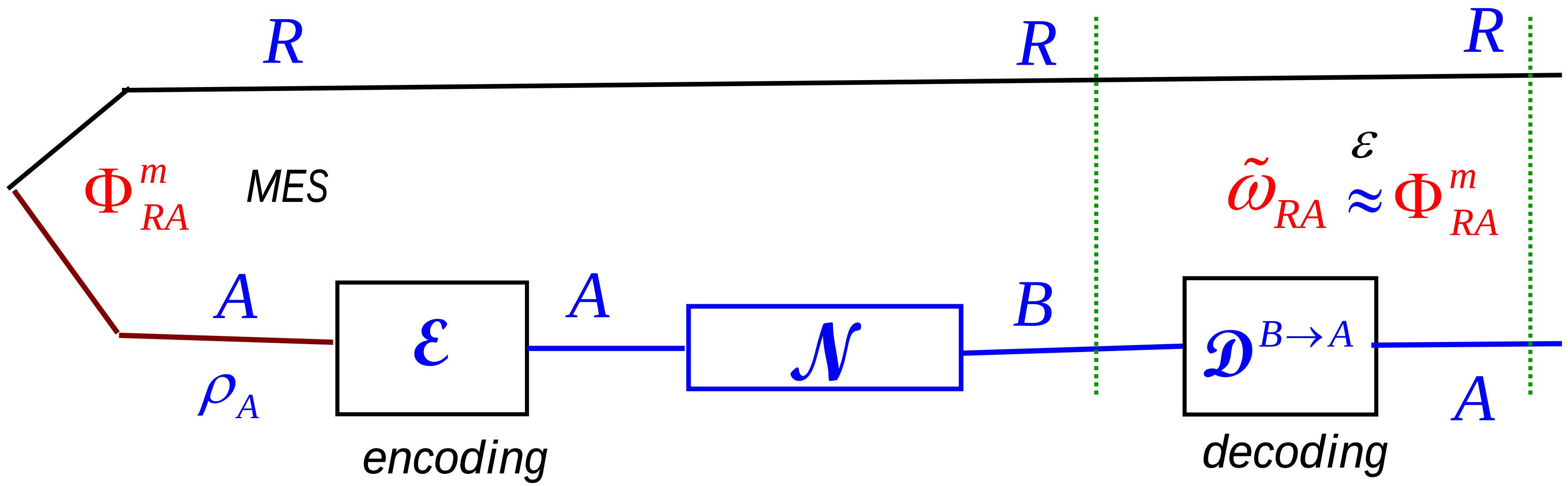
$$Q_{et}^{(1),\varepsilon}(\mathcal{N}) \geq \max_{\mathcal{H}_M \subseteq \mathcal{H}_A} \left\{ -H_{\max}^{\varepsilon}(R \mid B)_{\sigma} \right\} + f(\varepsilon)$$

- *Used the fact: decoupling* $\Rightarrow \exists$ *a decoder*

- *Condition for decoupling* → *lower bound*

Converse: $Q_{et}^{(1),\varepsilon}(\mathcal{N}) \leq \max_{\mathcal{H}_M \subseteq \mathcal{H}_A} \left\{-H_{\max}^{\varepsilon}(R|B)_\sigma\right\}$

- **Proof:**
  - Assume that $\exists$ an encoding $\mathcal{E}$ & a decoding $\mathcal{D}$ such that



$\log m \leq ?$

$\Rightarrow Q_{et}^{(1),\varepsilon}(\mathcal{N}) \leq ?$

UNIVERSITY OF CAMBRIDGE

- **Converse:** $Q_{et}^{(1),\varepsilon}(\mathcal{N}) \leq \max_{\mathcal{H}_M \subseteq \mathcal{H}_A} \left\{ -H_{\max}^{\varepsilon}(R|B)_{\sigma} \right\}$

$$\log m = -H_{\max}(R|A)_{\Phi_{RA}^m}$$

$$\leq \max_{\tau_{RA} \in B^{\varepsilon}(\tilde{\omega}_{RA})} \left\{ -H_{\max}(R|A)_{\tau} \right\}$$

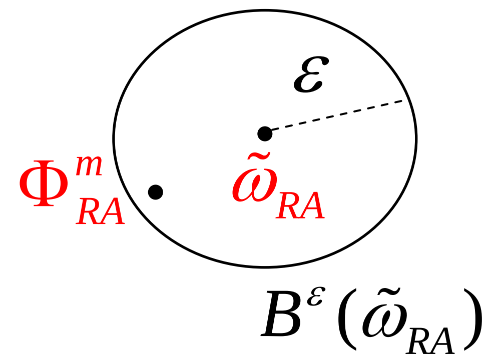
$$= - \min_{\tau_{RA} \in B^{\varepsilon}(\tilde{\omega}_{RA})} \left\{ H_{\max}(R|A)_{\tau} \right\}$$

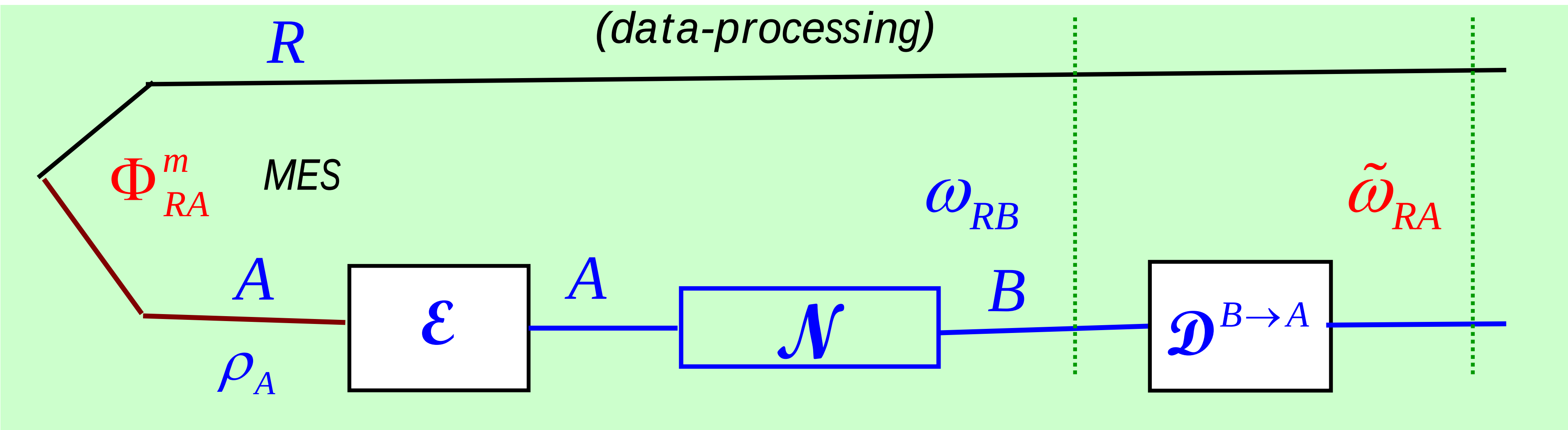
$$= - H_{\max}^{\varepsilon}(R|A)_{\tilde{\omega}} \leq -H_{\max}^{\varepsilon}(R|B)_{\omega} \quad \because \mathcal{D}^{B\to A}$$

(data-processing)

State after decoding :

$$\tilde{\omega}_{RA} \overset{\varepsilon}{\approx} \Phi_{RA}^m$$





UNIVERSITY OF CAMBRIDGE

- **Converse:** $Q_{et}^{(1),\varepsilon}(\mathcal{N}) \leq \max_{\mathcal{H}_M \subseteq \mathcal{H}_A} \left\{ -H_{\max}^{\varepsilon}(R|B)_\sigma \right\}$

Thus:

$$\log m \leq -H_{\max}^{\varepsilon}(R|B)_\omega$$

where

$$\omega_{RB} = (\mathrm{id}_R \otimes \mathcal{N}^{A\to B} \circ \mathcal{E})\Phi_{RA}^m;$$

*

$$\leq -H_{\max}^{\varepsilon}(R|B)_\sigma$$

where

$$\sigma_{RB} = (\mathrm{id}_R \otimes \mathcal{N}^{A\to B})\Phi_{RA}^m;$$

Main ingredients of * :

- *Ricochet:* $(I \otimes U)|\Phi\rangle = (U^T \otimes I)|\Phi\rangle$

- *Invariance of smooth conditional max-entropy under local unitaries*

$$H_{\max}^{\varepsilon}(R|B)_\omega = H_{\max}^{\varepsilon}(R|B)_\sigma \quad \text{if} \quad \omega_{RB} \overset{U}{\leftrightarrow} \sigma_{RB}$$

$$\Rightarrow \log m \leq -H_{\max}^{\varepsilon}(R|B)_\sigma$$

UNIVERSITY OF CAMBRIDGE

- **Converse:** $Q_{et}^{(1),\varepsilon}(\mathcal{N}) \leq \max_{\mathcal{H}_M \subseteq \mathcal{H}_A} \left\{ -H_{\max}^{\varepsilon}(R|B)_{\sigma} \right\}$

$$\log m \leq -H_{\max}^{\varepsilon}(R|B)_{\omega}$$

$$\sigma_{RB} = (\mathrm{id}_R \otimes \mathcal{N}^{A\to B})\Phi_{RA}^{m};$$

$$\omega_{RB} = (\mathrm{id}_R \otimes \mathcal{N}^{A\to B} \circ \mathcal{E})\Phi_{RA}^{m};$$

$$= (\mathrm{id}_R \otimes \mathcal{N}^{A\to B} \circ U_{\varepsilon})\Phi_{RA}^{m};$$

(Unitary encoding suffices)

$$= (\mathrm{id}_R \otimes \mathcal{N}^{A\to B})(\mathrm{id}_R \otimes U_{\varepsilon})\Phi_{RA}^{m};$$

$$= (\mathrm{id}_R \otimes \mathcal{N}^{A\to B})(U_{\varepsilon}^{T} \otimes \mathrm{id}_A)\Phi_{RA}^{m};$$

$$= (U_{\varepsilon}^{T} \otimes \mathrm{id}_A)(\mathrm{id}_R \otimes \mathcal{N}^{A\to B})\Phi_{RA}^{m};$$

$$= (U_{\varepsilon}^{T} \otimes \mathrm{id}_A)\left((\mathrm{id}_R \otimes \mathcal{N}^{A\to B})\Phi_{RA}^{m}\right);$$

$$= (U_{\varepsilon}^{T} \otimes \mathrm{id}_A)\sigma_{RB}$$

(Unitarily equivalent)

$$H_{\max}^{\varepsilon}(R|B)_{\omega} = H_{\max}^{\varepsilon}(R|B)_{\sigma}$$

$$\log m \leq -H_{\max}^{\varepsilon}(R|B)_{\omega}$$

$$\Rightarrow \log m \leq -H^{\varepsilon}_{\max}(R|B)_{\sigma}$$

$$Q^{(1),\varepsilon}_{et}(\mathcal{N}) \leq \max_{\mathcal{H}_M \subseteq \mathcal{H}_A} \left\{ -H^{\varepsilon}_{\max}(R|B)_{\sigma} \right\}$$

■

In summary

- *We established the upper bound (converse) by starting with the assumption that :*

  $\exists$ *an encoding* $\mathcal{E}$ *& a decoding* $\mathcal{D}$ *such that*

  decoded state is $\overset{\varepsilon}{\approx} \Phi^m_{RA}$

- *Going from* $\log m = -H_{\max}(R|A)_{\Phi^m_{RA}}$ → *smooth conditional max-entropy*
- *using the fact that a unitary encoding suffices*
- *& invariance of smooth conditional max-entropy under unitaries*

UNIVERSITY OF CAMBRIDGE

One-shot $\varepsilon-$ error entanglement-transmission capacity:

$$Q_{et}^{(1),\varepsilon}(\mathcal{N}) \approx \max_{\mathcal{H}_M \subseteq \mathcal{H}_A} \left\{ -H_{\max}^{\varepsilon}(R\,|\,B)_{\sigma} \right\}$$

UNIVERSITY OF CAMBRIDGE

One-shot setting → **Asymptotic memoryless setting**

Asymptotic capacity

$$Q_{et}(\mathcal{N}) = \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}Q_{et}^{(1),\varepsilon}(\mathcal{N}^{\otimes n})$$

One-shot result:

$$Q_{et}^{(1),\varepsilon}(\mathcal{N}) \approx \max_{\mathcal{H}_M\subseteq\mathcal{H}_A}\left\{-H_{\max}^{\varepsilon}(R|B)_\sigma\right\}$$

$$.... \leq Q_{et}^{(1),\varepsilon}(\mathcal{N}^{\otimes n}) \leq ....$$

UNIVERSITY OF CAMBRIDGE

One-shot setting → Asymptotic memoryless setting

Asymptotic capacity

$$Q_{et}(\mathcal{N}) = \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}Q_{et}^{(1),\varepsilon}(\mathcal{N}^{\otimes n})$$

One-shot result:

$$Q_{et}^{(1),\varepsilon}(\mathcal{N}) \approx \max_{\mathcal{H}_M\subseteq\mathcal{H}_A}\left\{-H_{\max}^{\varepsilon}(R\,|\,B)_{\sigma}\right\}$$

$$\ldots\leq Q_{et}^{(1),\varepsilon}(\mathcal{N}^{\otimes n}) \leq \max_{\mathcal{H}_{M_n}\subseteq\mathcal{H}_A^{\otimes n}}\left\{-H_{\max}^{\varepsilon}(R\,|\,B)_{\sigma_n}\right\}$$

$n\to\infty$

$$Q_{et}(\mathcal{N}) = \lim_{n\to\infty}\frac{1}{n}\max_{\mathcal{H}_{M_n}\subseteq\mathcal{H}_A^{\otimes n}}\left\{-H(R\,|\,B)_{\sigma_n}\right\}$$

$$\sigma_n = \sigma_{R_nB_n} = (\mathrm{id}_{R_n}\otimes\mathcal{N}^{\otimes n})\Phi_{R_nA_n}^{m_n}$$

UNIVERSITY OF CAMBRIDGE

One-shot setting → **Asymptotic memoryless setting**

$$Q_{et}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \max_{\mathcal{H}_{M_n} \subset \mathcal{H}_A^{\otimes n}} \left\{ -H(R|B)_{\sigma_n} \right\}$$

$$I_{\sigma_n}^{R>B} = -H(R|B)_{\sigma_n}$$

coherent information

Entanglement transmission capacity (in asymptotic, memoryless setting)

$$Q_{et}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \max_{\mathcal{H}_{M_n} \subset \mathcal{H}_A^{\otimes n}} I_{\sigma_n}^{R_n > B_n}$$

[Lloyd, Shor, Devetak]

regularized coherent information

UNIVERSITY OF CAMBRIDGE

Summary

- Quantum information transmission through a noisy quantum channel $\mathcal{N}$ in the one-shot setting

- Decoupling → existence of a decoder:

  such that Bob can recover the quantum state sent by Alice up to an error ε

- One-shot entanglement transmission through a quantum channel : bounds on the capacity

  -- given in terms of the smooth conditional max-entropy

UNIVERSITY OF CAMBRIDGE

Summary contd.

- One-shot entanglement transmission capacity

$$Q_{et}^{(1),\varepsilon}(\mathcal{N}) \approx \max_{\mathcal{H}_M \subseteq \mathcal{H}_A} \left\{ -H_{\max}^{\varepsilon}(R|B)_\sigma \right\}$$

- This yields bounds on the one-shot quantum capacity of $\mathcal{N}$

since

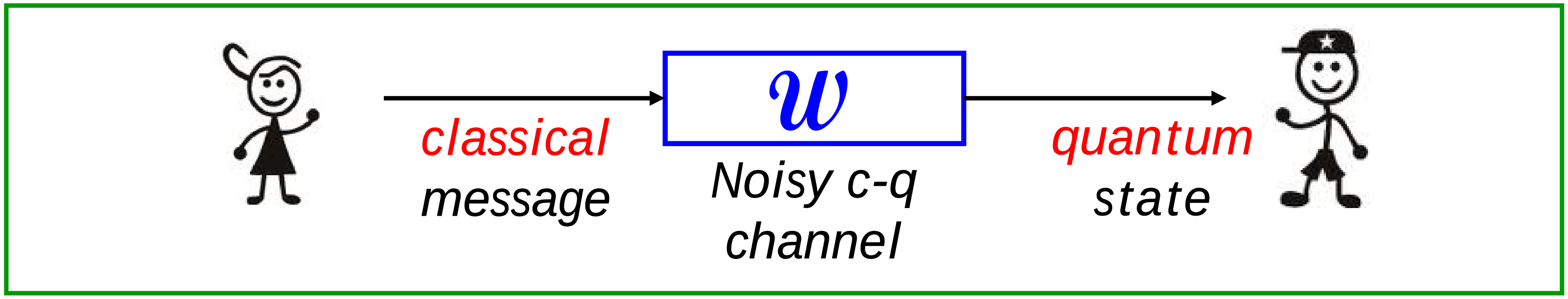
$$Q_{et}^{(1),\frac{\varepsilon}{2}}(\mathcal{N}) \le Q^{(1),\varepsilon}(\mathcal{N}) \le Q_{et}^{(1),\varepsilon}(\mathcal{N})$$

one-shot quantum capacity

- Retrieve known asymptotic result of Lloyd, Shor & Devetak:

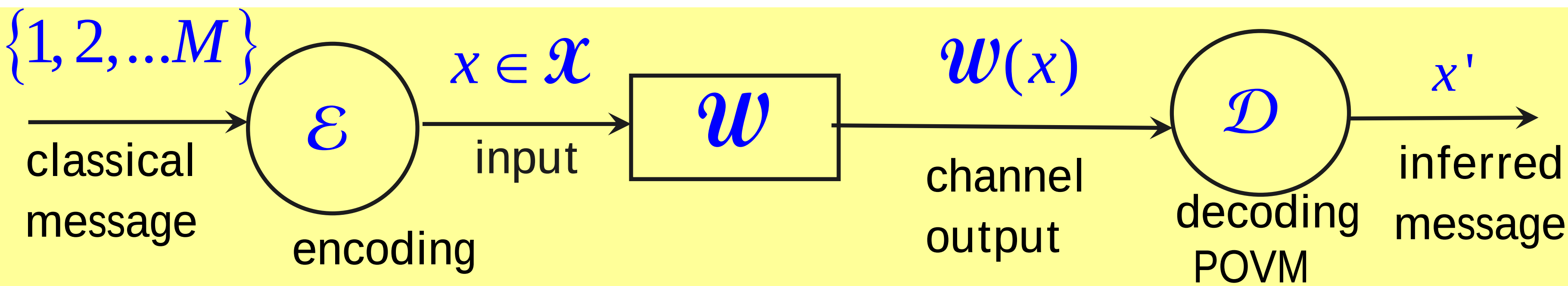
-- given in terms of the regularized coherent information

(II) Transmission of classical information through a classical-quantum (c-q) channel:



$\mathcal{W} : \mathcal{X} \mapsto \mathcal{D}(\mathcal{H})$; $\mathcal{X}$: input alphabet $\mathcal{H}$: output Hilbert space

One-shot setting



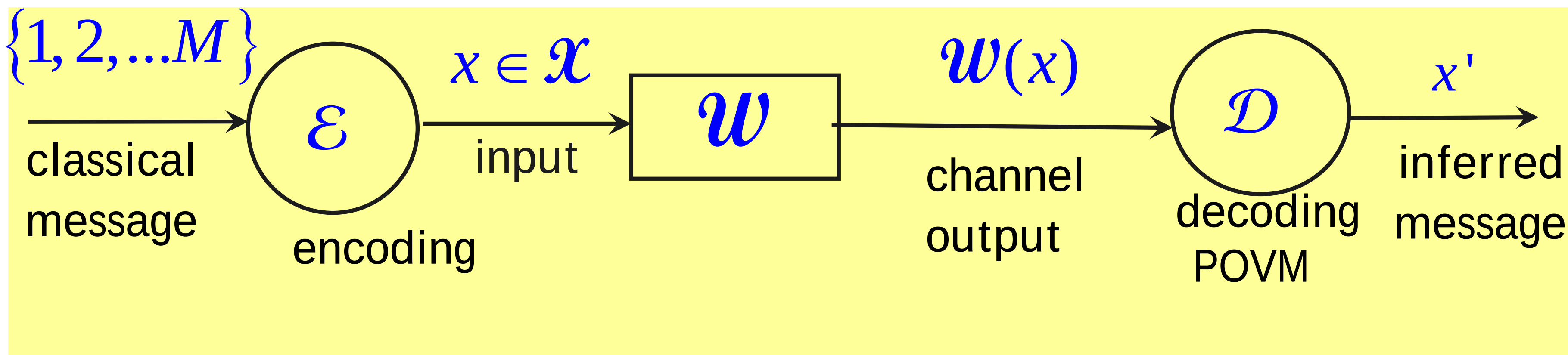
$C := (\mathcal{E}, \mathcal{D}, M)$: Error-correcting code

$\log M$: No. of bits of message sent

UNIVERSITY OF CAMBRIDGE

(II) Transmission of classical information through a classical-quantum (c-q) channel:

One-shot setting



$\forall \varepsilon > o,$ *One-shot* $\varepsilon -$ *error capacity of* $\mathcal{W}$:

$$C_{\varepsilon}^{(1)}(\mathcal{W}) := \sup \{ \log M : p_e \leq \varepsilon \}$$

(prob. of error)

UNIVERSITY OF CAMBRIDGE

"asymptotic memoryless setting"

$$p_e^{(n)} \to 0 \text{ as } n \to \infty$$

- **HSW Theorem:**

$$C(\mathcal{W}) = \chi^*(\mathcal{W}) \qquad \textit{(Holevo Capacity)}$$

$$= \max_{p_{\mathcal{X}}} \left\{ H\left(\sum_{x \in \mathcal{X}} p(x)\mathcal{W}(x)\right) - \sum_{x \in \mathcal{X}} p(x) H(\mathcal{W}(x)) \right\}$$

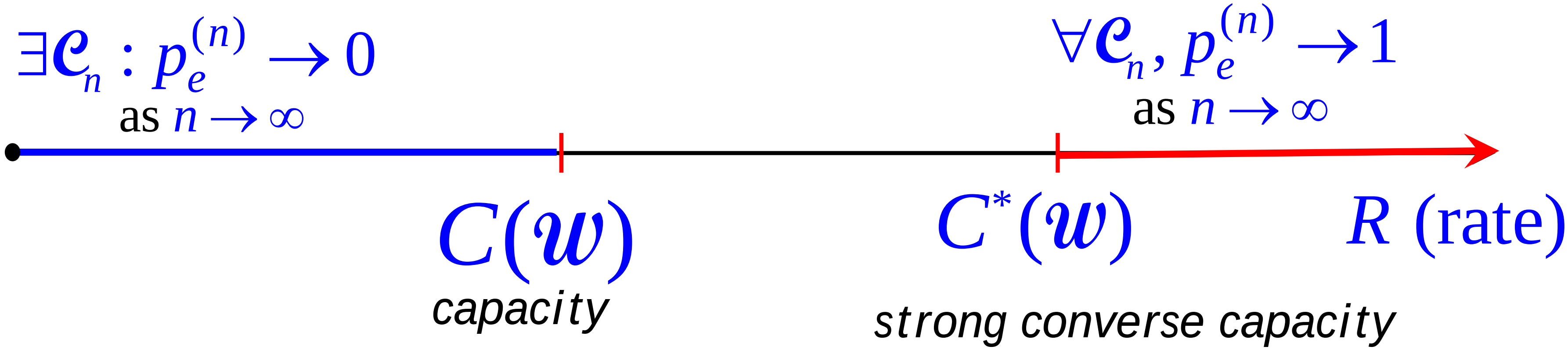
$$C(\mathcal{W}) = \max_{p_{\mathcal{X}}} \min_{\sigma_B} D\left(\rho_{XB} \,\|\, \rho_X \otimes \sigma_B\right)$$

[quantum relative entropy]

where, $\rho_{XB} = \sum_x p_x |x\rangle\langle x| \otimes \mathcal{W}(\rho_x);$

"*asymptotic, memoryless setting*"

- *2 characteristic quantities for* $\mathcal{W}$



- The capacity satisfies the strong converse property **:**

$$C(\mathcal{W}) = C^*(\mathcal{W}) = \chi^*(\mathcal{W})$$

[Ogawa & Nagaoka; Winter]

- *Aim of one-shot analysis:*
  - *Obtain bounds on* $C_{\varepsilon}^{(1)}(\mathcal{W});$
  - *Retrieve the HSW theorem* $C(\mathcal{W}) = \chi^{*}(\mathcal{W})$
  - *Retrieve the strong converse property*

$$C(\mathcal{W}) = C^{*}(\mathcal{W}) = \chi^{*}(\mathcal{W})$$

UNIVERSITY OF CAMBRIDGE

One-shot Results

$\forall \varepsilon \in (0,1):$

- **Our result:** *(ND, M.Mosonyi, M-H-Hsieh, F.Brandao: [D,M,H,B])*

$$C_\varepsilon^{(1)}(\mathcal{W}) \approx \max_{p_x} \min_{\sigma_B} D_{\max}^{\varepsilon'}\left(\rho_{XB} \,\|\, \rho_X \otimes \sigma_B\right)$$

(smoothed max-relative entropy)

(HSW Theorem)

$$C(\mathcal{W}) = \max_{p_x} \min_{\sigma_B} D\left(\rho_{XB} \,\|\, \rho_X \otimes \sigma_B\right)$$

[quantum relative entropy]

where, $\rho_{XB} = \sum_x p_x |x\rangle\langle x| \otimes \mathcal{W}(\rho_x);$

- **Another result:** *(L.Wang,R.Renner: [W,R])*

$$C_\varepsilon^{(1)}(\mathcal{W}) \approx \max_{p_x} D_H^{\varepsilon}\left(\rho_{XB} \,\|\, \rho_X \otimes \rho_B\right)$$

(hypothesis testing relative entropy)

- *also [W.Matthews & S.Wehner]*

UNIVERSITY OF CAMBRIDGE

Comparison of results *of [D,M,H,B] and [W,R]*

HSW theorem

$$C(w) = \chi^*(w)$$

- *[D,M,H,B]*

[W,R]

Strong converse property

$$C(w) = C^*(w) = \chi^*(w)$$

The strong converse property cannot be deduced from *[W,R]*

UNIVERSITY OF CAMBRIDGE

Thank you!

- *Thanks also to:*

F.Buscemi, F.Brandao, M-H.Hsieh and M.Mosonyi