The decoupling approach to quantum information theory

Frédéric Dupuis
Université de Montréal

PhD Defense

Dec 21, 2009

Introduction

What is information theory?

- The study of information processing tasks:
  - Data compression
  - Data transmission through a noisy channel

Quantum information theory? Accomplishing these tasks with *quantum* data or using quantum resources.

Introduction

So what's in this thesis? A general method to solve quantum information theory problems based on removing correlations between quantum systems. More specifically:

- A theorem that says how to remove correlations ("decouple")
- How it can be used to recover many important QIT theorems
- New coding theorems for quantum channels with side information at the transmitter and broadcast channels
- A way to lock classical correlations in quantum states

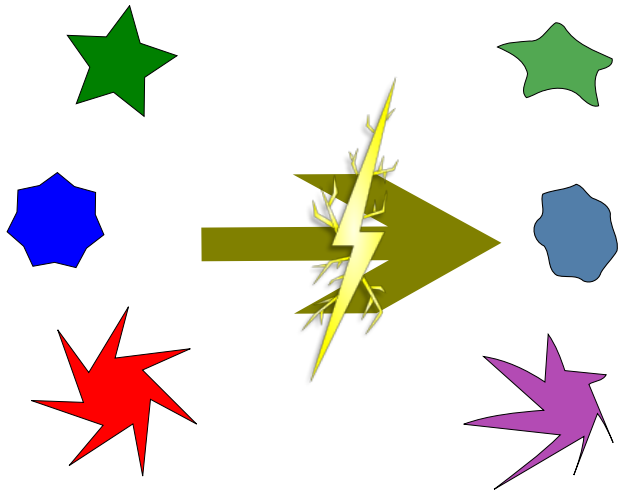
Outline

- Introduction to channels and quantum information
- Coding by destroying correlations
- The decoupling theorem
- Channels with side information at the transmitter
- Locking classical correlations in quantum states

What is a channel?

By “channel”, I mean any physical means by which digital data can be communicated:

- Radio link
- Fibre optics
- Telephone wire
- Etc. . .



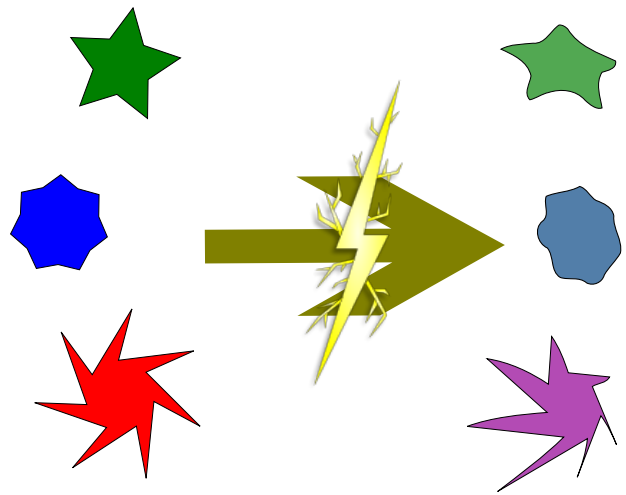
Why can they transmit data?

- Choose an input
- Send it into the channel, which corrupts it
- Try to decipher which input was sent

What is a channel?

How do we model this mathematically?

- Input set $\mathcal{X}$
- Output set $\mathcal{Y}$
- Transition probability $p(y|x)$, $x \in \mathcal{X}, y \in \mathcal{Y}$

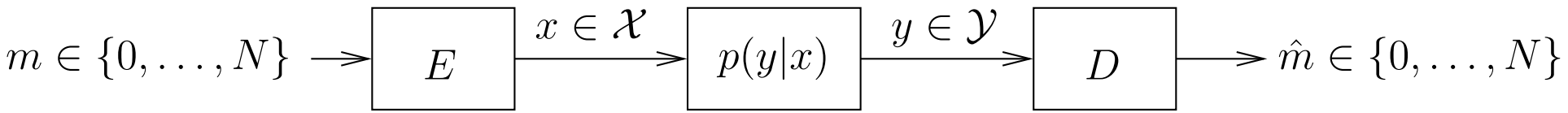


$$x \in \mathcal{X} \longrightarrow \boxed{p(y|x)} \longrightarrow y \in \mathcal{Y}$$

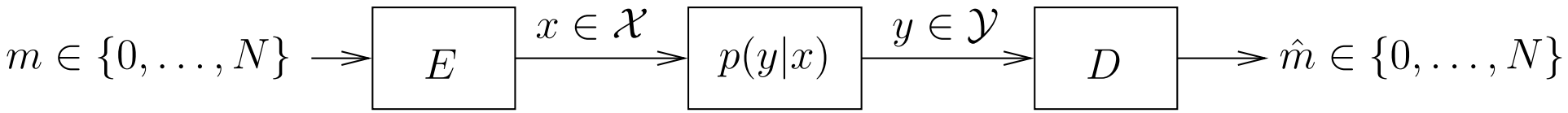
Transmitting data through a channel

Why use a channel? To send data:

- The message m is a number from 1 to N.
- The encoder $E : \{0, \ldots, N\} \to \mathcal{X}$ associates each message to an input symbol from $\mathcal{X}$.
- The decoder $D : \mathcal{Y} \to \{0, \ldots, N\}$ associates each output symbol from $\mathcal{Y}$ with a message estimate.



Transmitting data through a channel



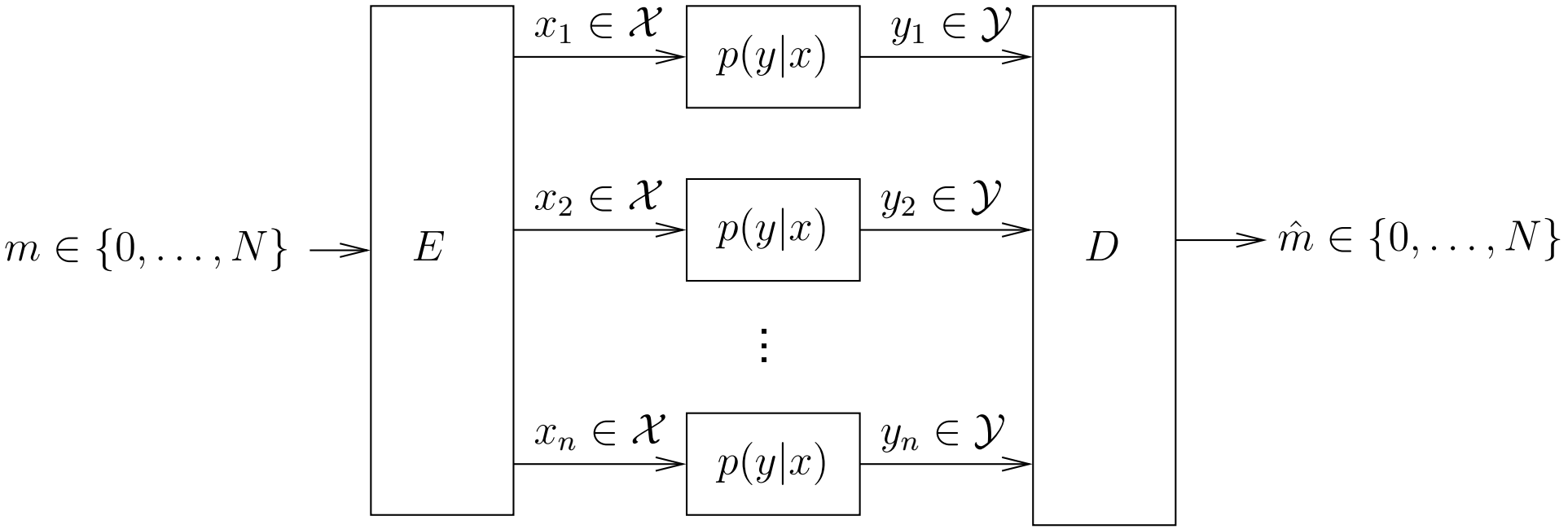
Goals:

- N as high as possible
- $\Pr\{m \neq \hat{m}\}$ as low as possible

The tradeoff between the two depends on the channel.

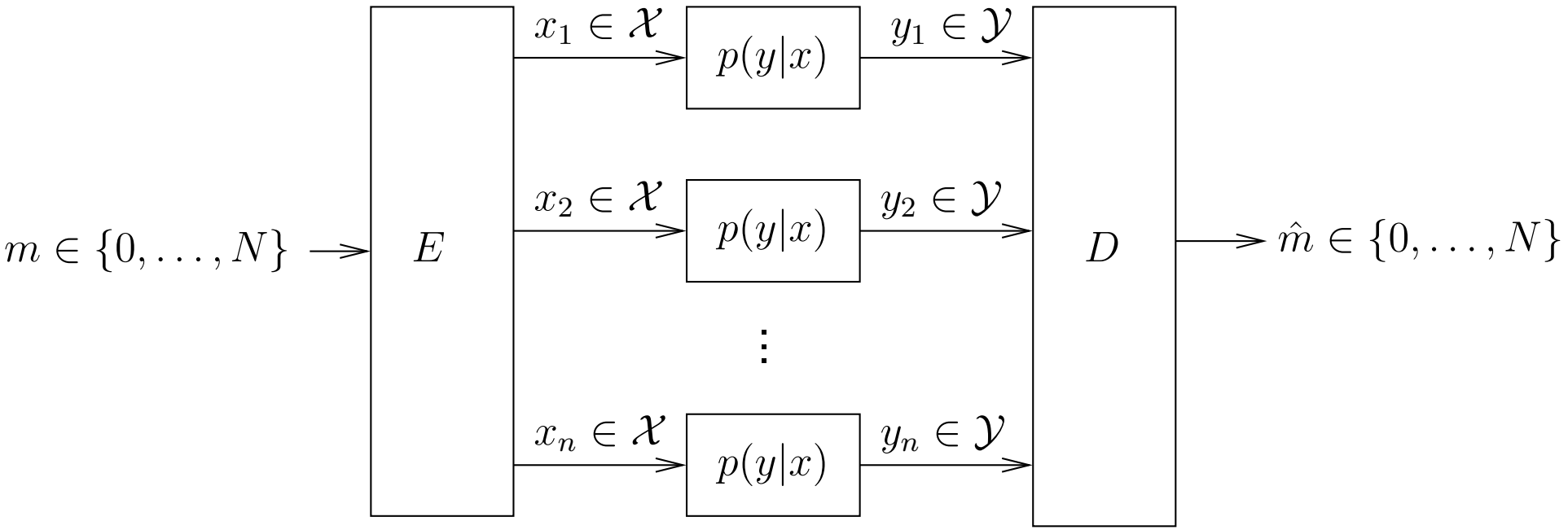
Memoryless channels

An interesting case: memoryless channels



This corresponds to using the same channel n times; a very common occurrence!

Memoryless channels



In this case, it is possible to ensure that $\Pr\{m \neq \hat{m}\} \to 0$ as $n \to \infty$ with fixed $(\log N)/n$ [Shannon, 1949]

Quantum channels

Quantum information

But first, a few words about quantum information...

- Physical system that holds information:
  - Classical: Sets $\mathcal{X}$, $\mathcal{Y}$,... Size: log of number of elements in set
  - Quantum: Vector spaces A, B,... Size: log of dimension of vector space
- Possible value of information:
  - Classical: An element x of the set $\mathcal{X}$
  - Quantum: Pure state $|\psi\rangle^A$ in A
- Probabilistic information:
  - Classical: Probability distribution $p(x)$ over $\mathcal{X}$
  - Quantum: (Mixed) state ρ^A: matrix over A.

Quantum information

- Information-preserving transformations:
  - Classical: For each element in $\mathcal{X}$, pick a unique element in $\mathcal{Y}$.
  - Quantum: "Partial isometries" $V^{A\to B}$
- General transformations:
  - Classical: Channels $p(y|x)$
  - Quantum: "CPTP maps" $\mathcal{N}^{A\to B}$

Measuring information

How do we measure the amount of information? Entropies:

- Isolated state ρ^{AB}: $H_2(A|B)_\rho$. Uncertainty about A when we have B. “2-entropy”
- Multiple copies of state ρ^{AB}: $H(A|B)_\rho$. “Shannon entropy”

Purifications

- Given a mixed state ρ^A, there exists pure states $|\psi\rangle^{AB}$ such that $\rho^A = \psi^A$. We call $|\psi\rangle^{AB}$ a *purification* of ρ^A.
- Any two purifications $|\psi\rangle^{AB}$ and $|\varphi\rangle^{AC}$ of ρ^A are related by a partial isometry $V^{B\to C}$:

$$|\varphi\rangle^{AC} = V^{B\to C}|\psi\rangle^{AB}$$

Quantum channels

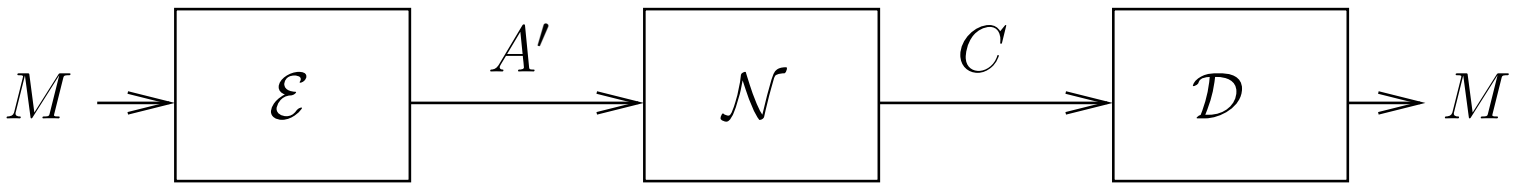
What are quantum channels concretely?

- Fibre optics
- Optical link between Earth and satellites
- Quantum memory
- Etc. . .

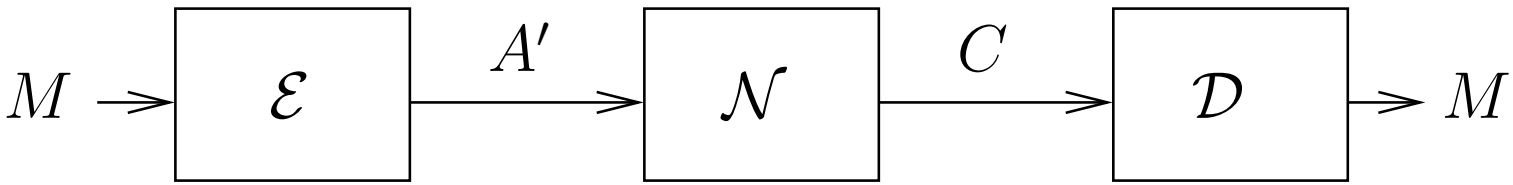
Sending quantum messages

Why use a quantum channel $\mathcal{N}^{A' \to C}$? To send quantum data:

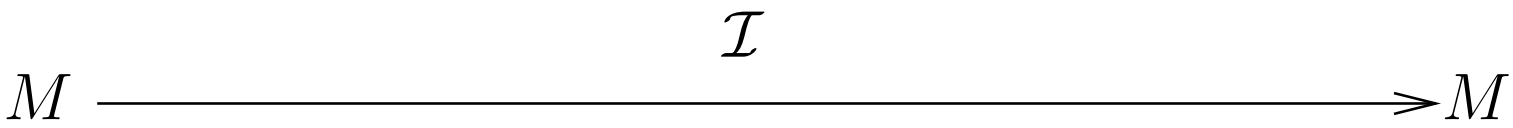
- The message is initially held in quantum system M.
- The encoder $\mathcal{E}^{M \to A'}$ encodes the message into the input to the channel A'.
- The decoder $\mathcal{D}^{C \to M}$ tries to recover the message from the channel output system C.



Sending quantum messages



How to measure the error probability? By comparing the above combination with

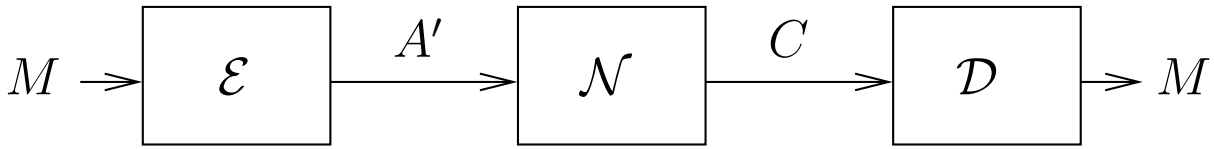


We will want to show that

$$\|\mathcal{D} \circ \mathcal{N} \circ \mathcal{E} - \mathcal{I}\|_\diamond \leqslant \varepsilon$$

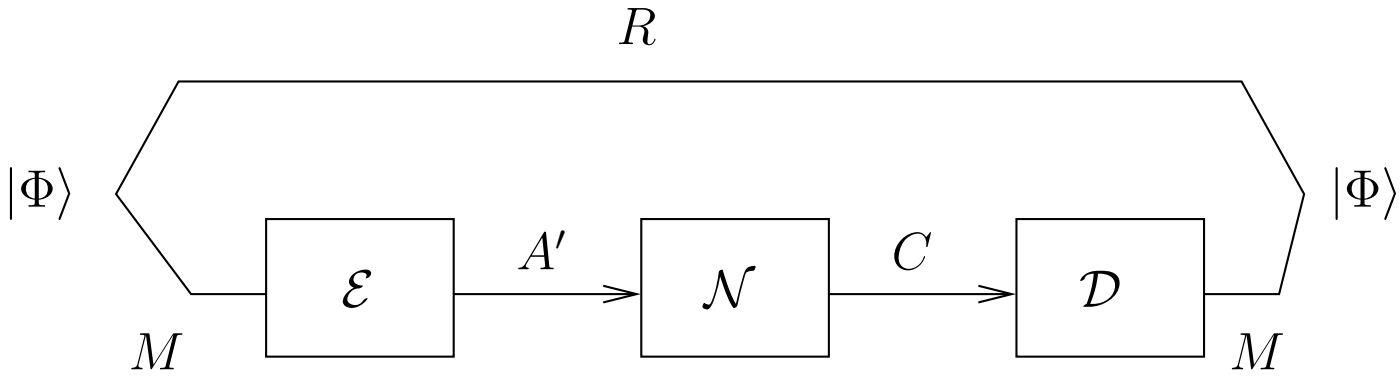
Sending quantum messages

This is difficult to check directly: we would need to check every possible input state. Fortunately, we can only check Φ^{RM}:



$$\|\mathcal{D} \circ \mathcal{N} \circ \mathcal{E} - \mathcal{I}\|_\diamond \leqslant \varepsilon$$

is (essentially) equivalent to

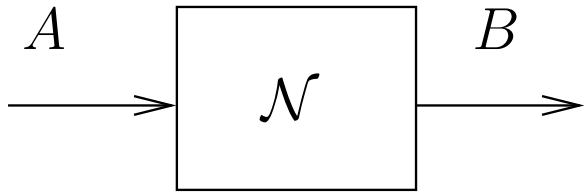


$$\left\|(\mathcal{D} \circ \mathcal{N} \circ \mathcal{E})(\Phi^{RM}) - \Phi^{RM}\right\|_1 \leqslant \varepsilon$$

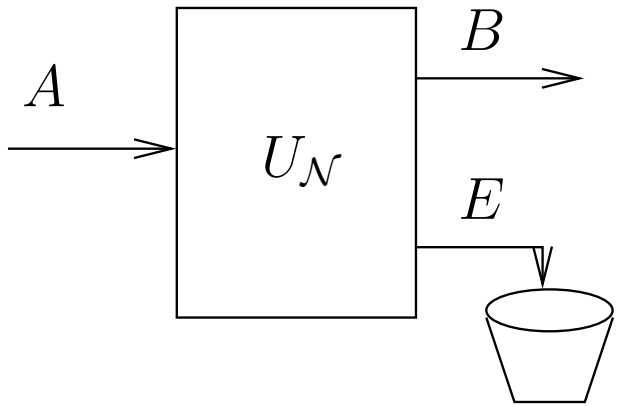
Decoupling

Decoupling

We can also purify CPTP maps: $\mathcal{N}^{A\to B}$ is equivalent to performing a partial isometry $U^{A\to BE}$, and then ignoring part of the output:

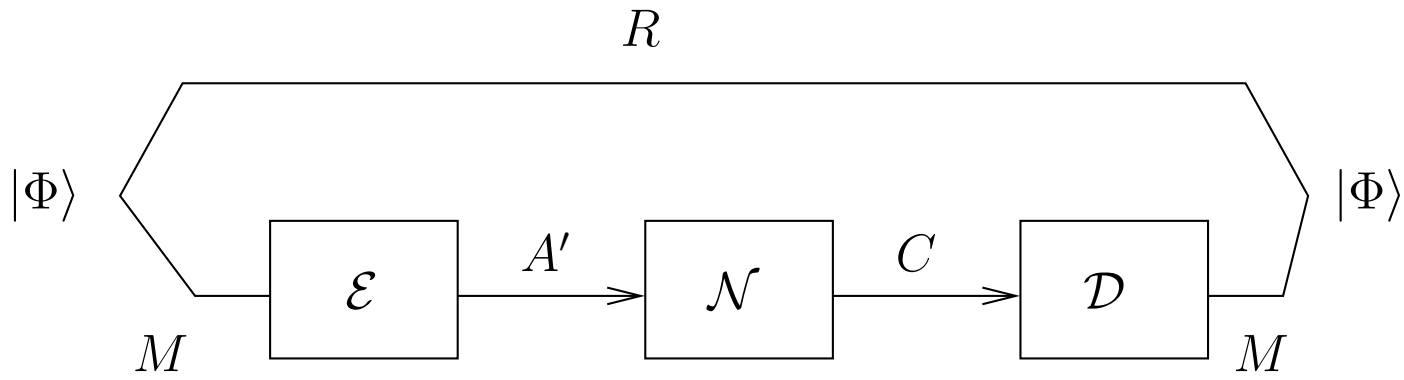


is equivalent to

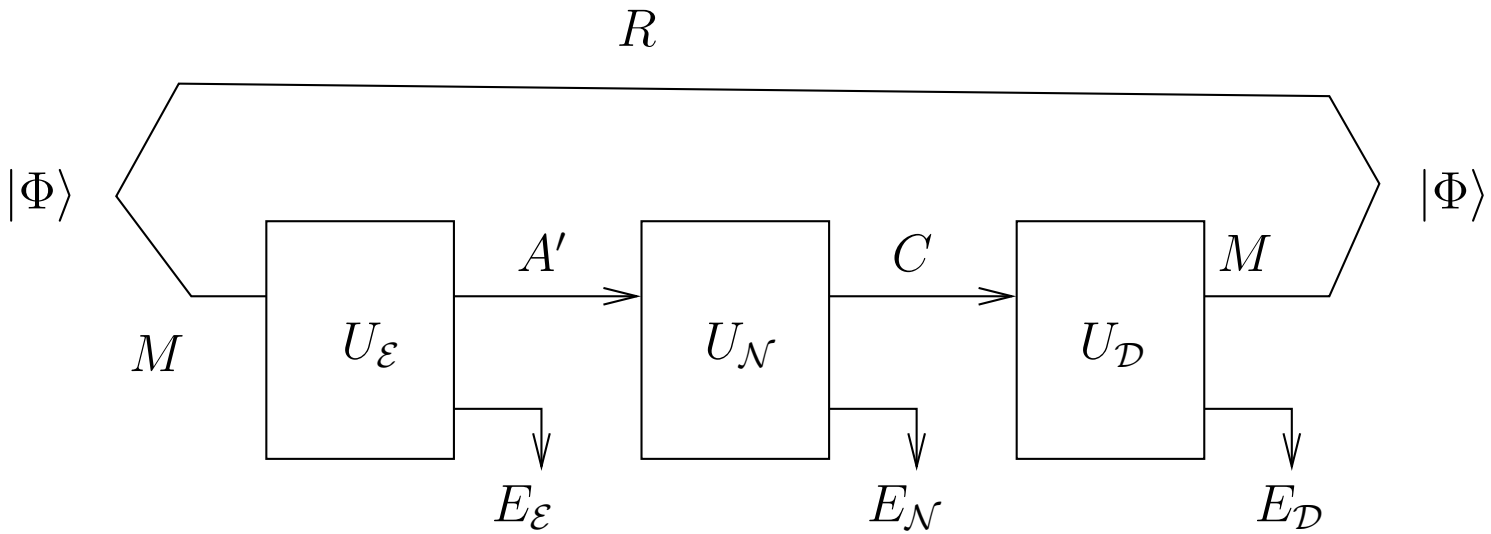


We call E the *environment*.

Decoupling

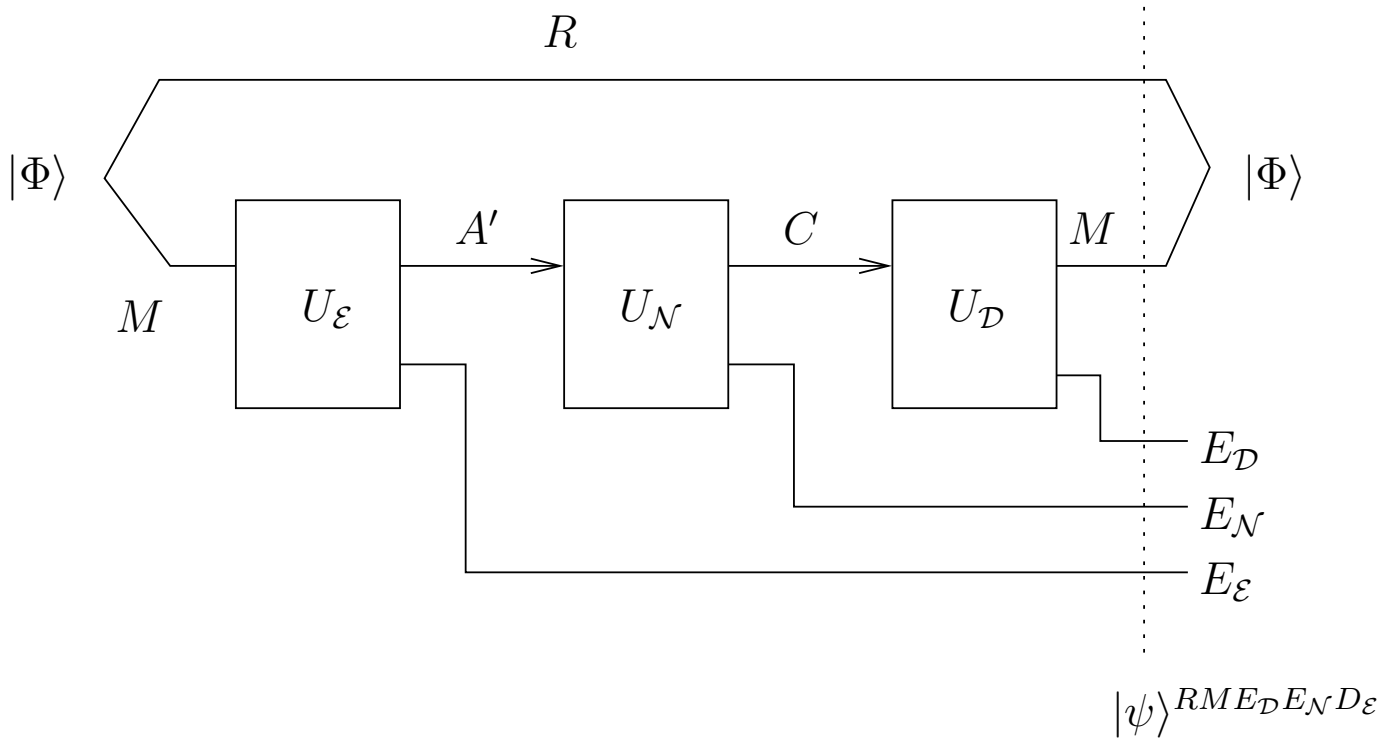


becomes



Decoupling

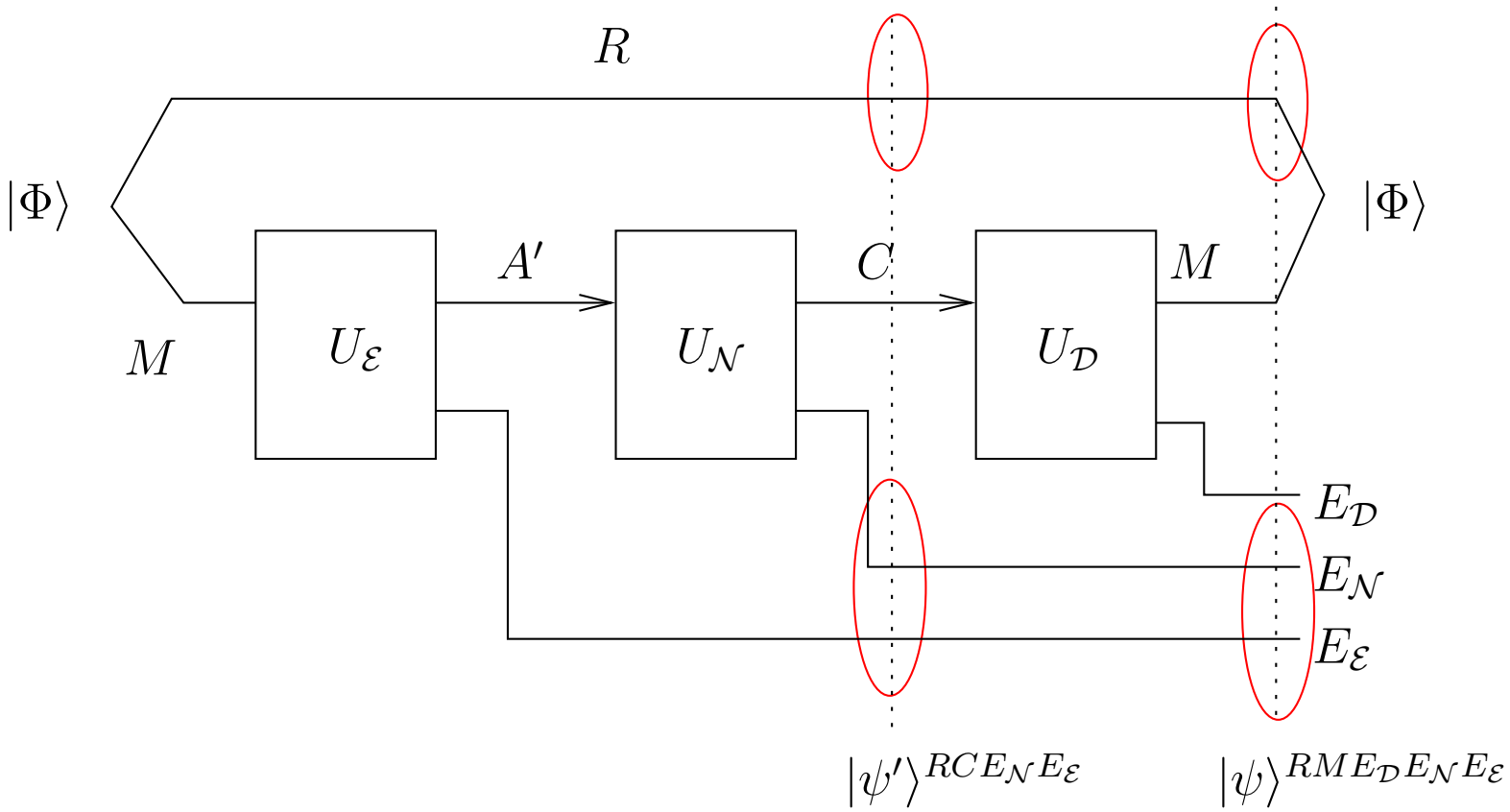
We then get



$$|\psi\rangle^{RME_\mathcal{D}E_\mathcal{N}E_\mathcal{E}} = |\Phi\rangle^{RM} \otimes |?\rangle^{E_\mathcal{D}E_\mathcal{N}E_\mathcal{E}}$$

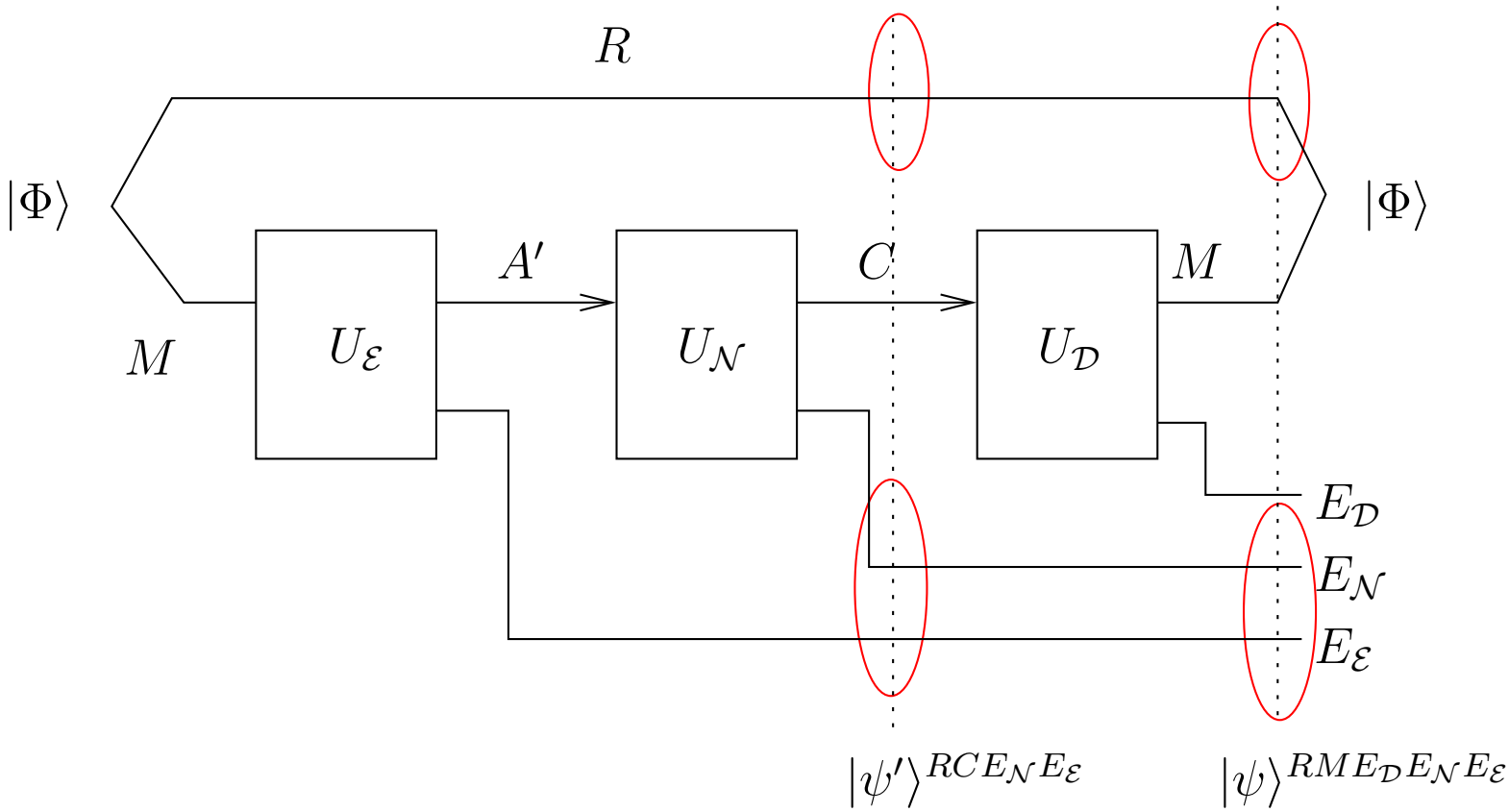
$$\psi^{RE_\mathcal{N}E_\mathcal{E}} = \pi^R \otimes ?^{E_\mathcal{N}E_\mathcal{E}}$$

Decoupling



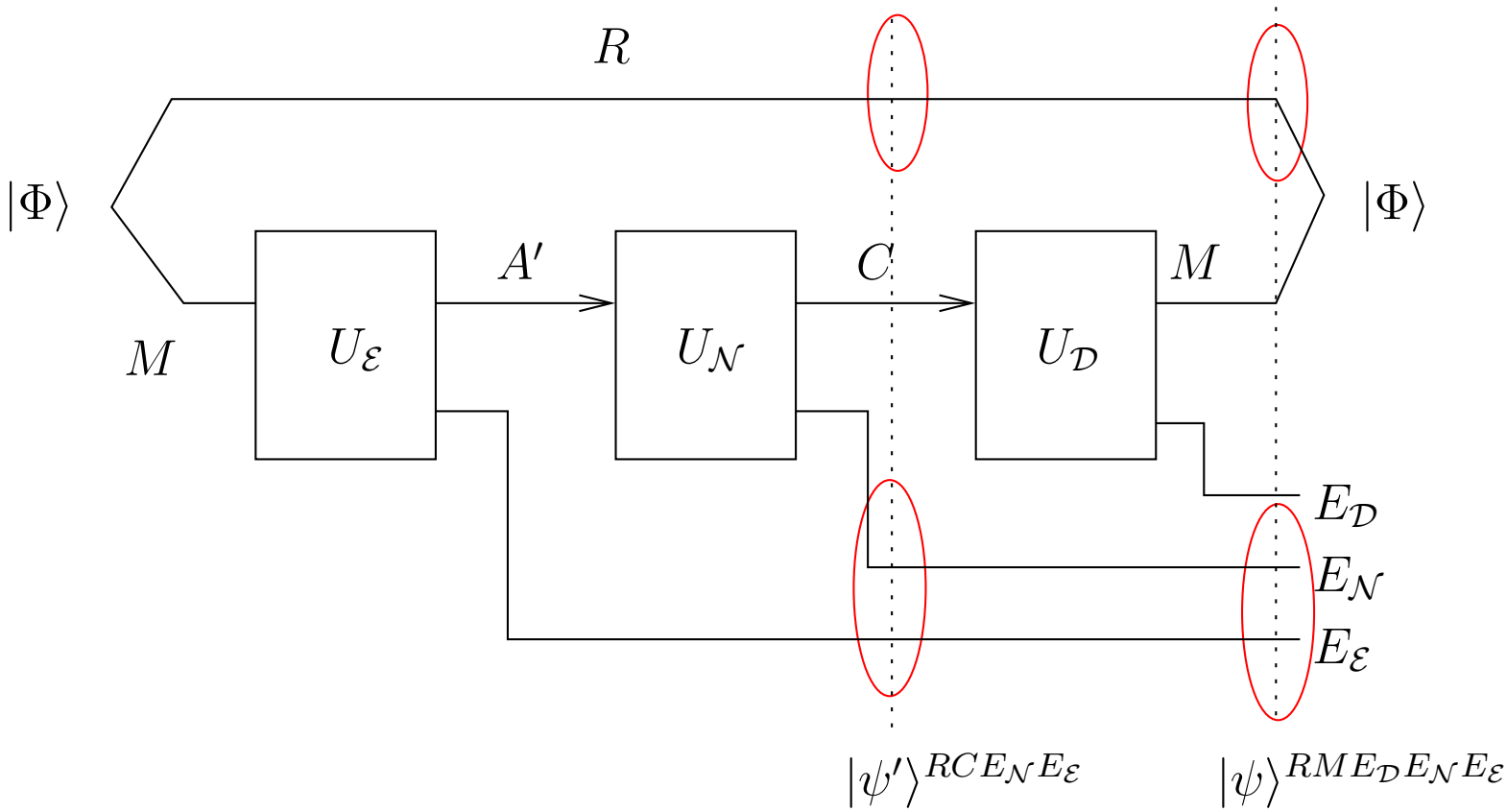
$$\psi'^{RE_{\mathcal{N}}E_{\mathcal{E}}} = \psi^{RE_{\mathcal{N}}E_{\mathcal{E}}} = \pi^{R} \otimes ?^{E_{\mathcal{N}}E_{\mathcal{E}}}$$

Decoupling



Both $|\psi\rangle^{RME_{\mathcal{D}}E_{\mathcal{N}}E_{\mathcal{E}}}$ and $|\psi'\rangle^{RCE_{\mathcal{N}}E_{\mathcal{E}}}$ are purifications of $\pi^R \otimes ?^{E_{\mathcal{N}}E_{\mathcal{E}}} \Rightarrow$ they are related by a partial isometry $U_{\mathcal{D}}^{C\to ME_{\mathcal{D}}}$.

Decoupling

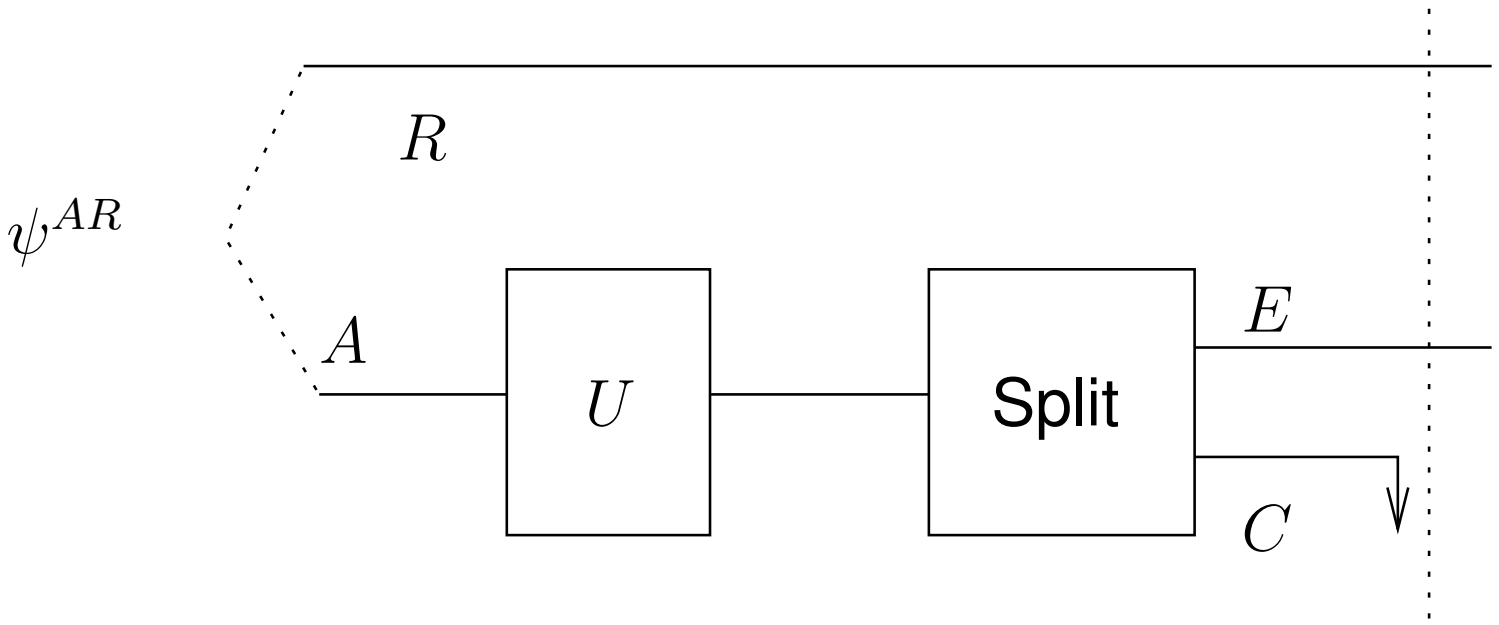


To make sure a decoder exists, we only need to make sure that $\psi'^{RE_{\mathcal{N}}E_{\mathcal{E}}} \approx \pi^R \otimes ?^{E_{\mathcal{N}}E_{\mathcal{E}}}$.

Decoupling theorems

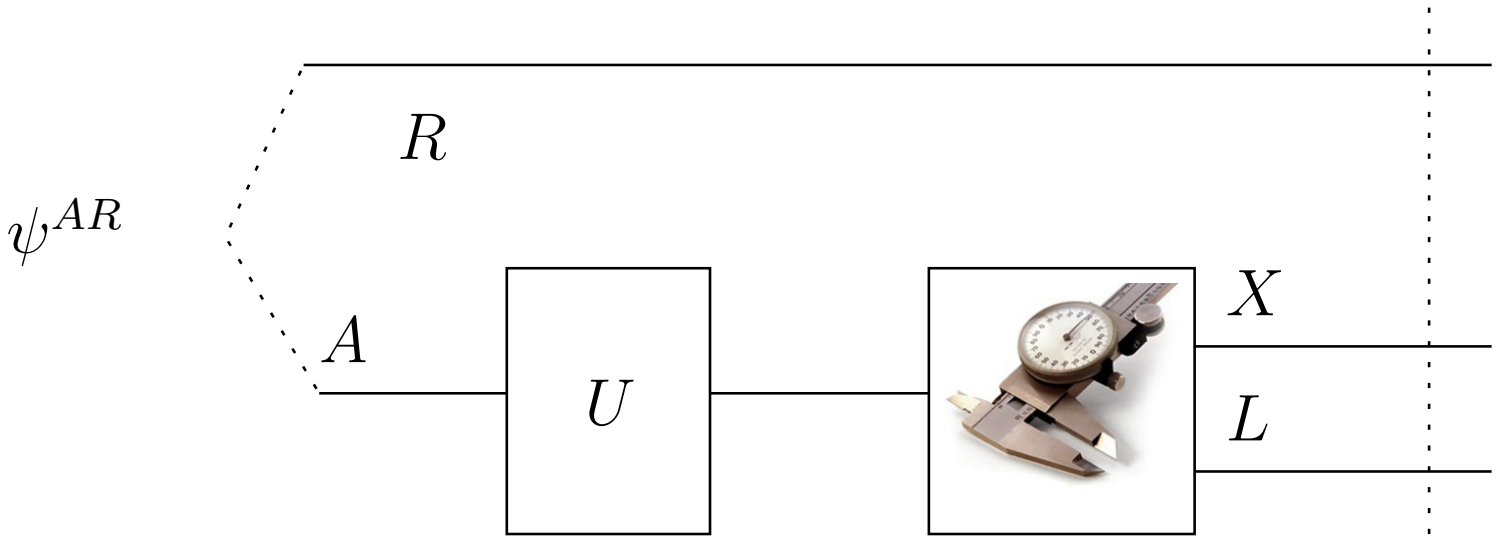
- The same logic applies in many different information theory settings.
- We need a way to ensure that two quantum systems are decoupled.
- Two main methods used:
  - Fully Quantum Slepian-Wolf (Abeyesinghe, Devetak, Hayden, Winter 2006)
  - State merging (Horodecki, Oppenheim, Winter 2005)
- Common pattern: Apply random unitary, then do "something". Should be good on average.

Fully Quantum Slepian-Wolf



$$\mathbb{E}_U \left\| \mathrm{Tr}_E[U \cdot \psi^{AR}] - \pi^E \otimes \psi^R \right\|_1 \leqslant \sqrt{\frac{|E|}{|C|} 2^{-H_2(A|R)_\psi}}$$

State merging



X: Measurement result

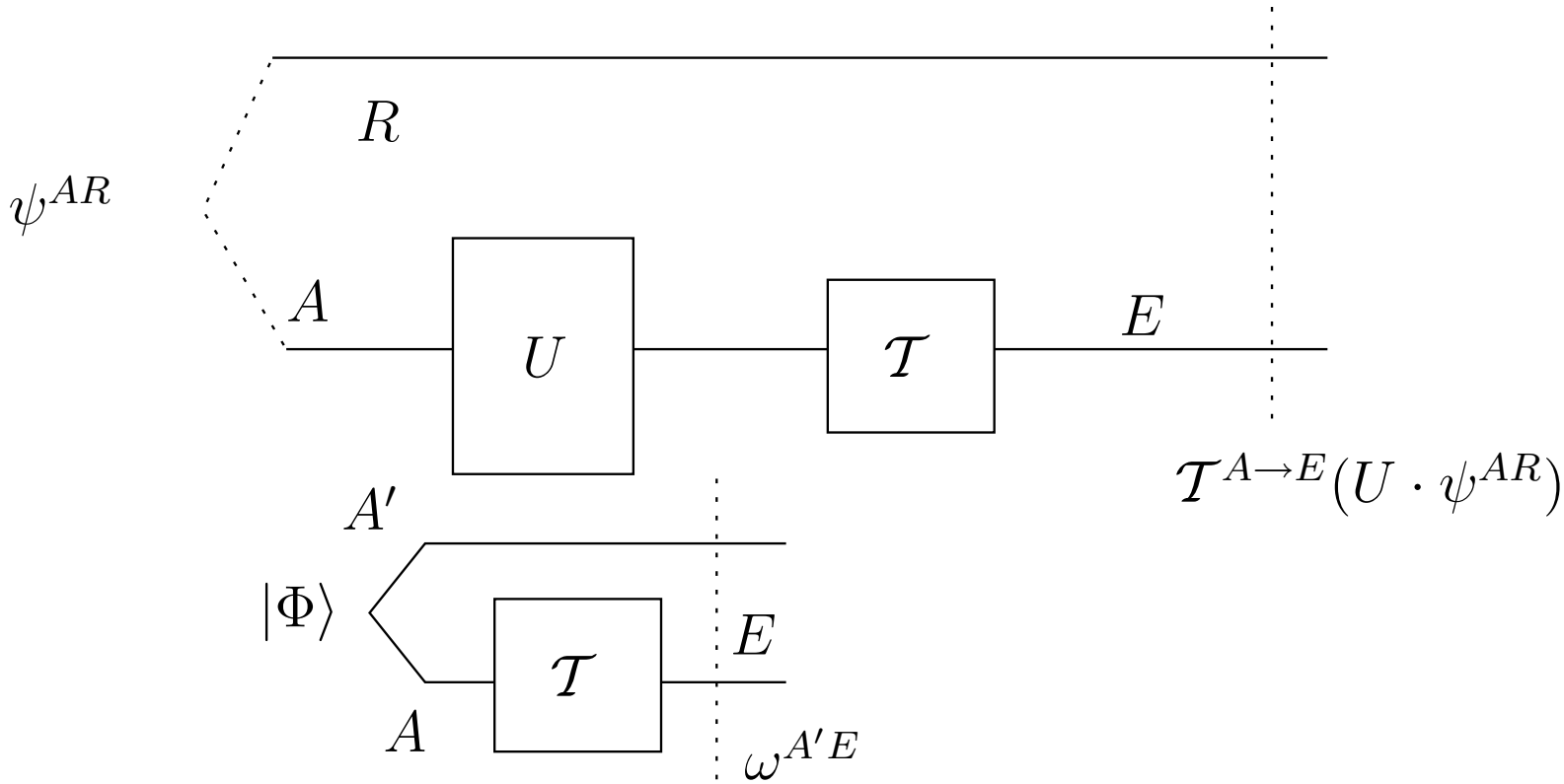
L: Quantum leftover

$$\mathcal{M}^{A\to XL}(U\cdot\psi^{AR})$$

$$\mathbb{E}_U \left\|\mathcal{M}^{A\to XL}(\psi^{AR}) - \pi^{XL}\otimes\psi^R\right\|_1 \leqslant \sqrt{|L|2^{-H_2(A|R)_\psi}}$$

Decoupling theorem

We can generalize these:



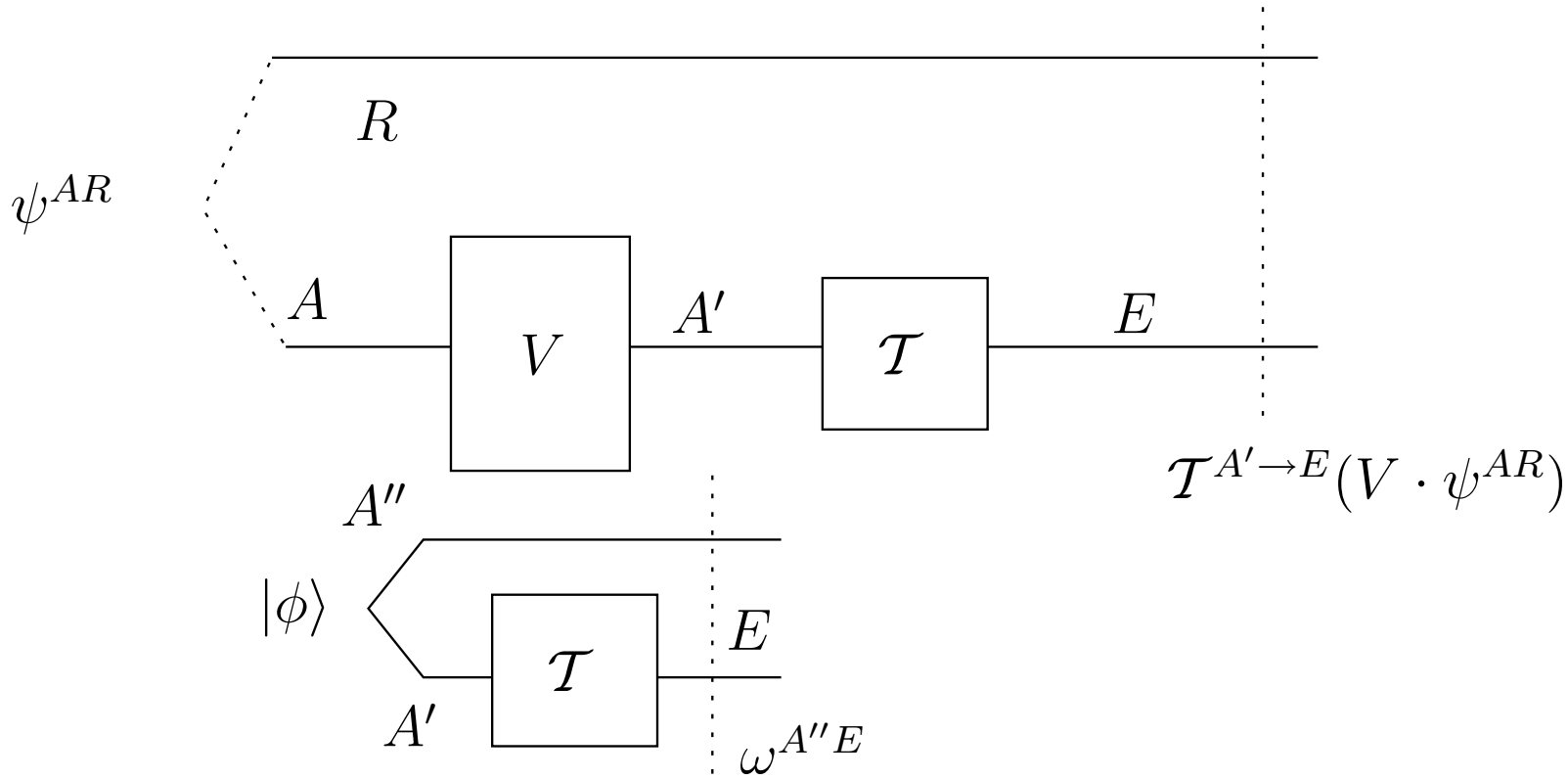
$$\mathbb{E}_U \left\| \mathcal{T}^{A\to E}(\psi^{AR}) - \mathcal{T}(\pi^A)\otimes\psi^R \right\|_1 \leqslant \sqrt{2^{-H_2(A'|E)_\omega - H_2(A|R)_\psi}}$$

Decoupling theorem

- We recover FQSW and state merging (just use the $\mathcal{T}$ that corresponds to them)
- Much more general and flexible

Decoupling theorem

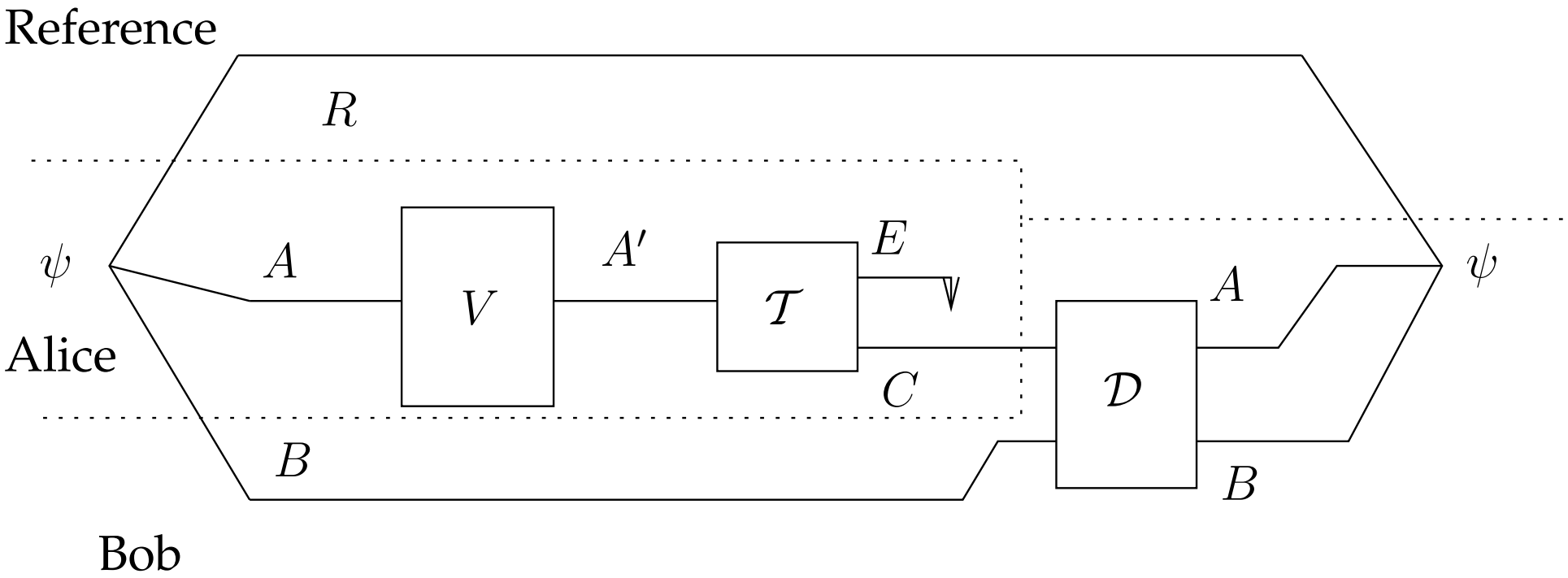
An even more general version: there exists a $V^{A\to A'}$ such that



$$\left\|\mathcal{T}^{A'\to E}(U\cdot\psi^{AR})-\mathcal{T}(\pi^A)\otimes\psi^R\right\|_1$$
$$\lesssim\sqrt{2^{-H_2^\varepsilon(A''|E)_\omega-H_2^\varepsilon(A|R)_\psi}}+\sqrt{2^{H_{\max}^\varepsilon(A)_\psi-H_2^\varepsilon(A'')_\omega}}$$

One-shot quantum channel coding

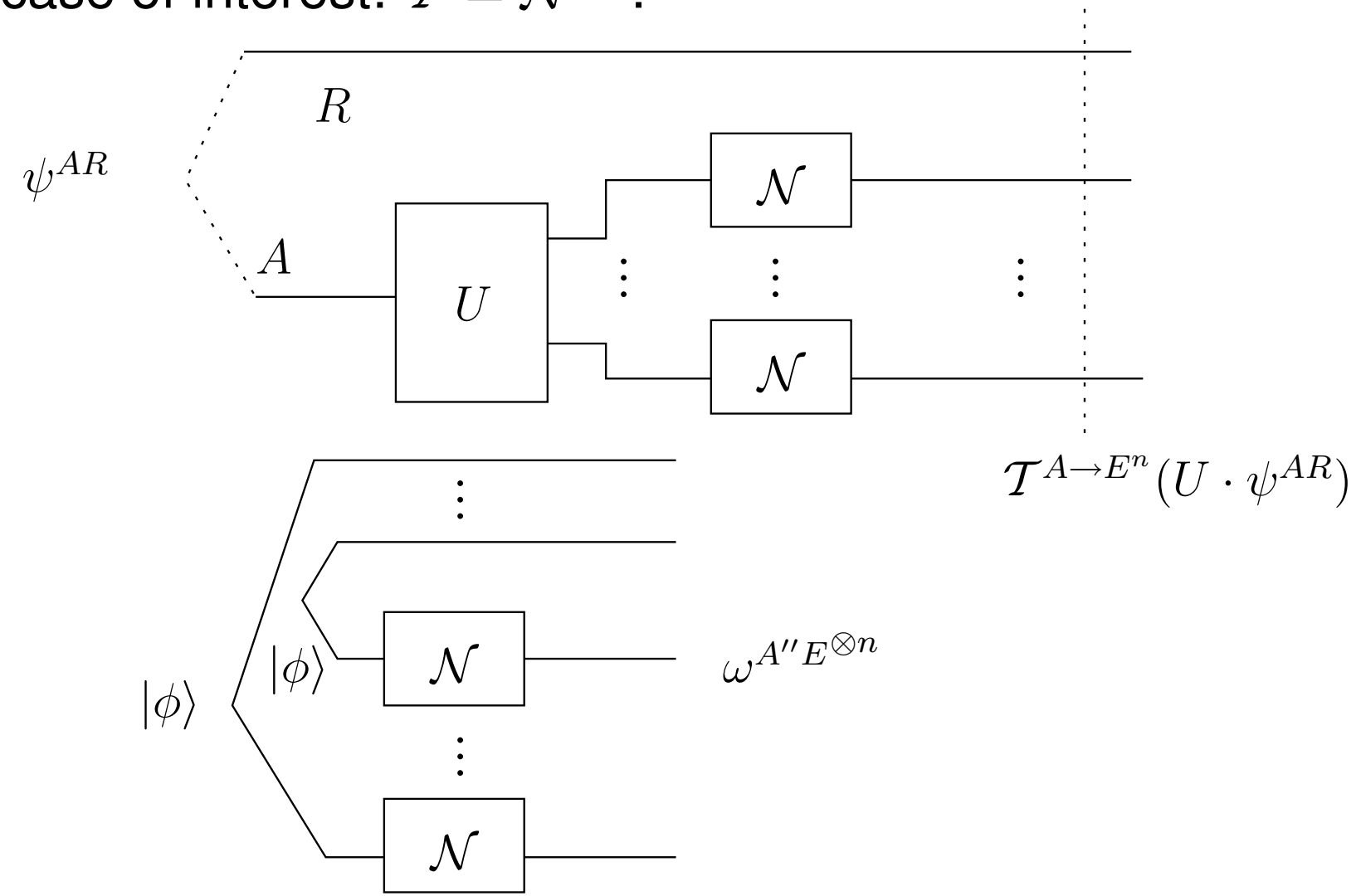
By purifying this, we get a channel coding theorem:



Similar to Buscemi and Datta (2009), but with quantum side-information at Bob.

Quantum channel coding

Special case of interest: $\mathcal{T} = \mathcal{N}^{\otimes n}$:



Quantum channel coding

Recall that:

$$\left\|\mathcal{T}^{A'\to E}(U\cdot\psi^{AR})-\mathcal{T}(\pi^A)\otimes\psi^R\right\|_1 \lesssim \sqrt{2^{-H_2^\varepsilon(A''|E)_\omega-H_2^\varepsilon(A|R)_\psi}}+\sqrt{2^{H_{\max}^\varepsilon(A)_\psi-H_2^\varepsilon(A'')_\omega}}$$

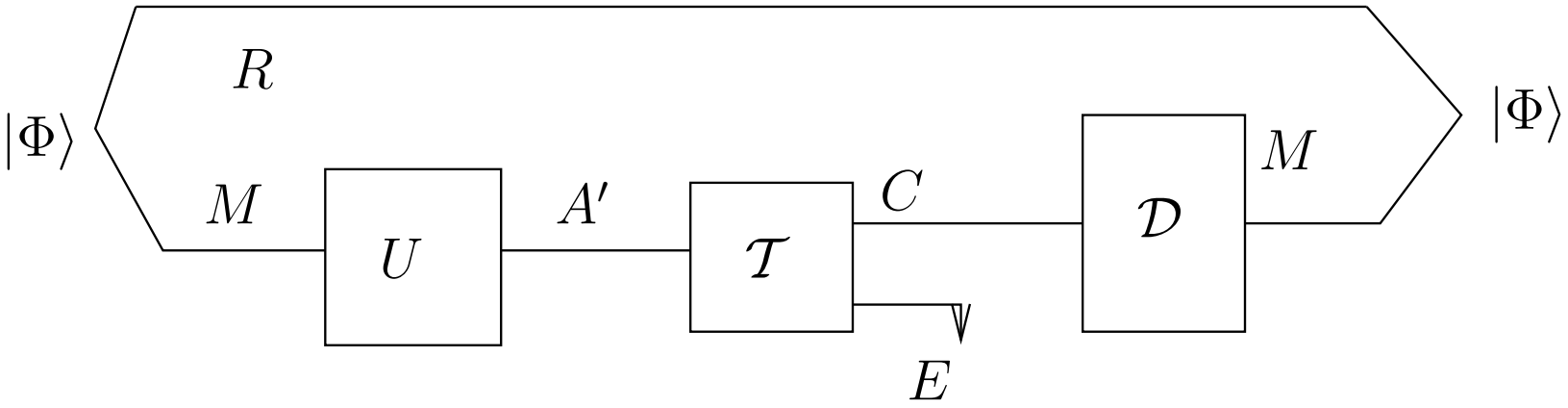
But when $\mathcal{T}=\mathcal{N}^{\otimes n}$,

$$H_2^\varepsilon(A''^n|E^n)_{\omega^{\otimes n}}\to nH(A''|E)_\omega$$
$$H_2^\varepsilon(A''^n)_{\omega^{\otimes n}}\to nH(A'')_\omega$$

[Tomamichel, Colbeck, Renner 2008]. Hence,

$$\left\|\mathcal{N}^{\otimes n}(U\cdot\psi^{AR})-\mathcal{N}^{\otimes n}(\pi^A)\otimes\psi^R\right\|_1 \lesssim \sqrt{2^{-nH(A''|E)_\omega-H_2^\varepsilon(A|R)_\psi}}+\sqrt{2^{H_{\max}^\varepsilon(A)_\psi-nH(A'')_\omega}}$$

Quantum channel coding



$$\log |M| < -H(A''|E)_\omega$$

[Lloyd, Shor, Devetak]

Channels with side information at the transmitter

Channels with side information at the transmitter

What is a (classical) channel with side information at the transmitter?

- $p_{Y|XS}(y|x,s)$
  - Input $x \in \mathcal{X}$
  - Output $y \in \mathcal{Y}$
  - State $s \in \mathcal{S}$
  - Probability distribution over S fixed by channel: $p_S(s)$
- s is known to the transmitter ahead of time.

Channels with side information at the transmitter

Consider an n-bit memory device, where each bit can be in one of 3 states:

- Stuck at 0: No matter what we write, we get 0. Happens with probability $\varepsilon/2$.
- Stuck at 1. Happens with probability $\varepsilon/2$.
- Works perfectly. Happens with probability $1-\varepsilon$.

We can test the memory before writing to it, but not when reading from it.

Quantum channels with side information at the transmitter

A quantum version of this makes sense. For example, an n-qubit quantum memory device, with each qubit either

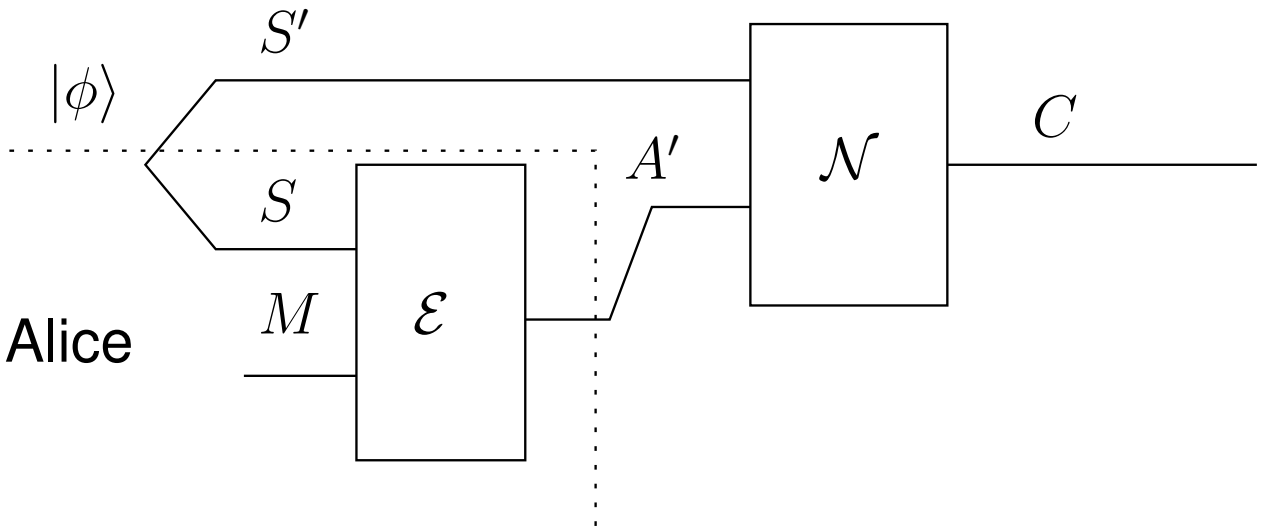
- Stuck at 0: No matter what we write, we get $|0\rangle$. Happens with probability $\varepsilon/2$.
- Stuck at 1. Happens with probability $\varepsilon/2$.
- Functioning perfectly. Happens with probability $1-\varepsilon$.

We can test the memory before writing to it, but not when reading from it.

Quantum channels with side information at the transmitter

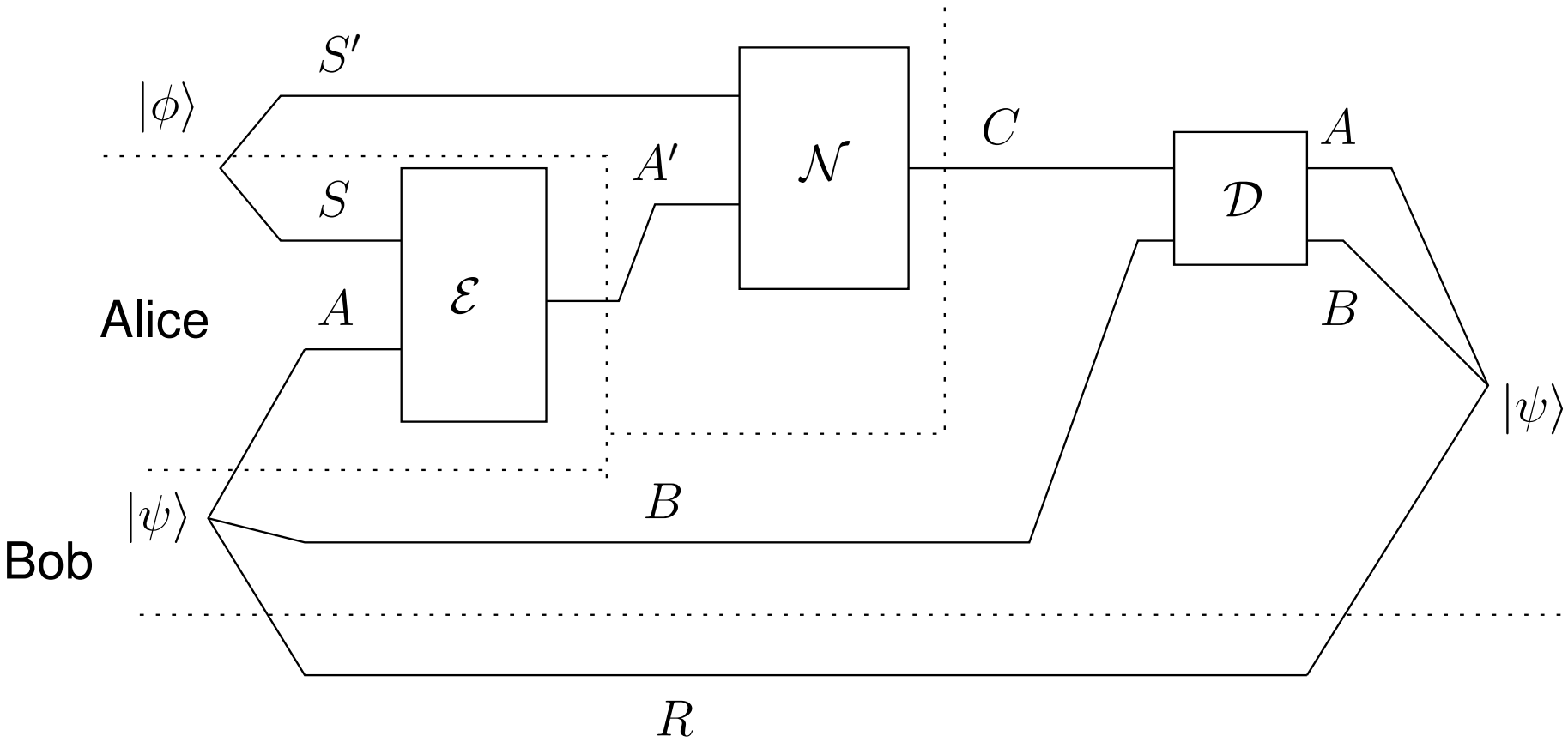
General quantum case:

- Alice has a quantum system S in her hands which is correlated with what the channel will do.



Coding theorem

We can use the decoupling theorem to get a coding theorem for these channels:



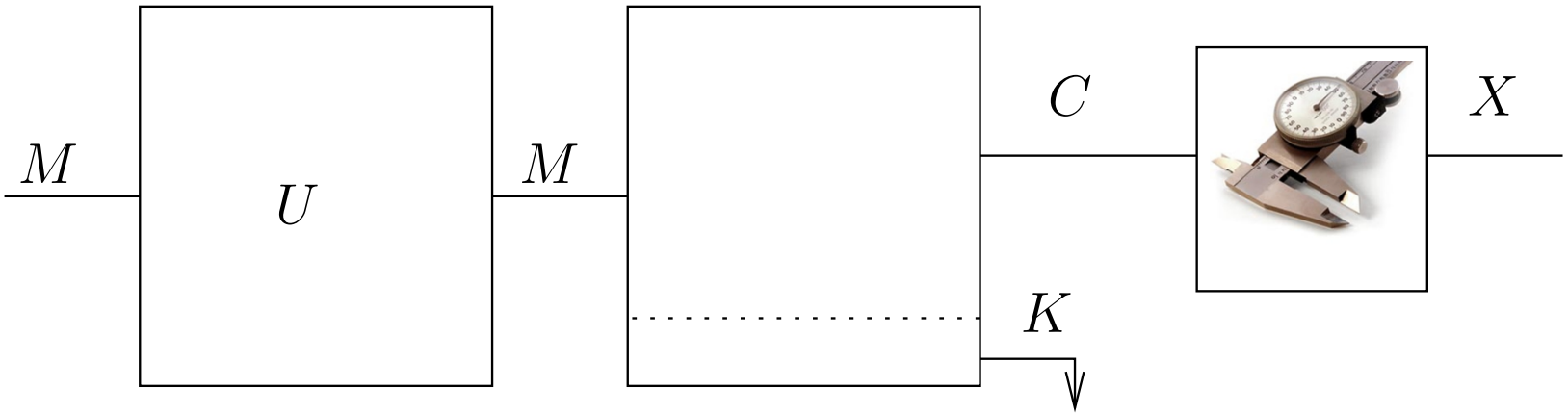
Locking classical information in quantum states

Joint work with Patrick Hayden and Debbie Leung

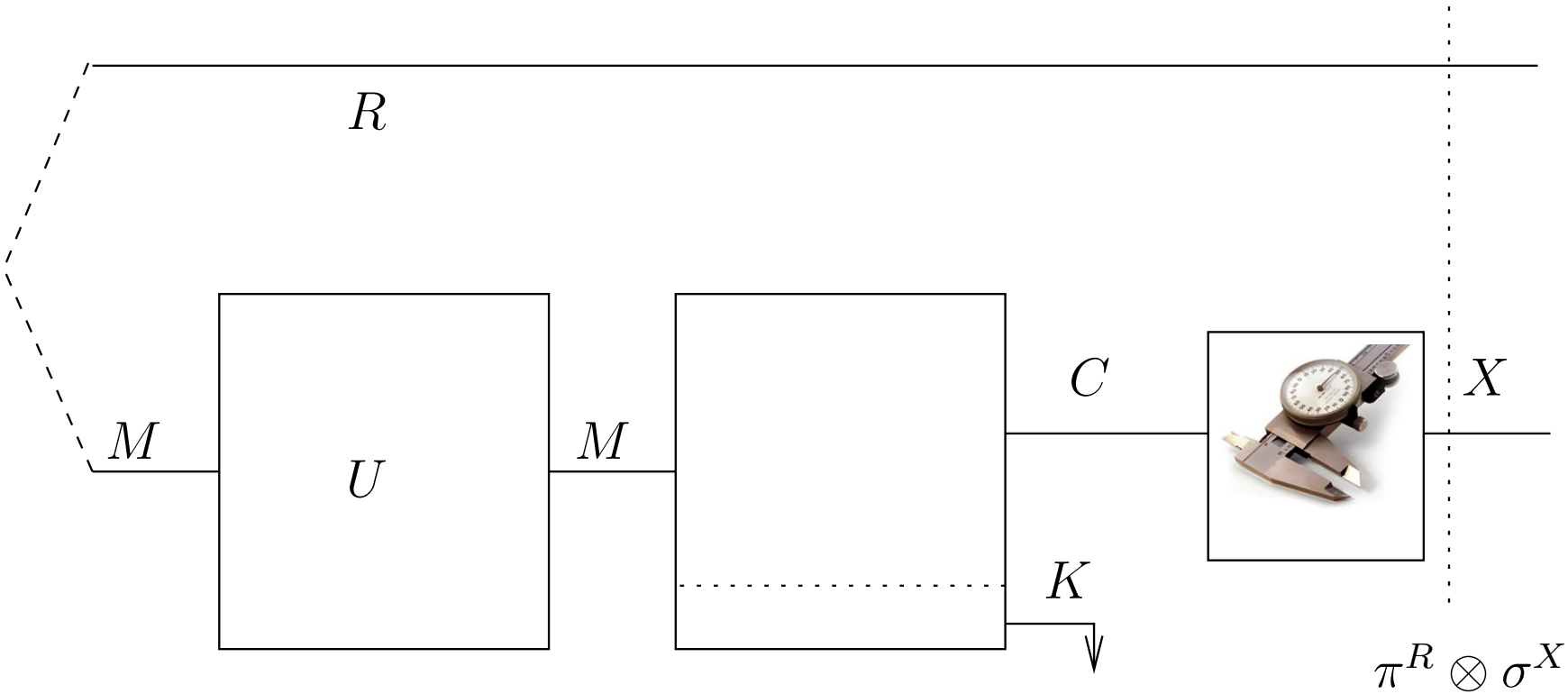
Locking classical information in quantum states

- We can encode n classical bits into n qubits.
- We can also "lock" n classical bits into quantum states as follows:
  - Perform a unitary on the message
  - Split the message into a big part C and a tiny "key" K
  - Any measurement result on C is uncorrelated with the message

Locking classical information in quantum states



Locking classical information in quantum states



Just like encryption?

Not surprised? Isn't that what we do when we encrypt a file?
Not quite...

- Message: A number from 1 to 10
- Key: a single bit
- Given a classical C, I can always narrow down the message to two possibilities out of 10. Hence, C is very correlated with the message.
- To prevent correlations, the key must be as big as the message.

Quantumly: an n-bit message with a $\mathrm{polylog}(n)$ key is possible.

Proof sketch

- For any fixed measurement, we can use the decoupling theorem to show that, when we select U at random, on average the final state is decoupled.
- We can also show that this is true with very high probability, so the probability of bad decoupling for a given measurement is very low.
- So low that:

$$(\text{Prob of bad measurement}) \times (\#\text{ of possible measurements}) < 1$$

- So there exists a U that gives good decoupling for *every* measurement.
- How to count possible measurements? Somewhat complicated. . .

Previous work on locking

Pick random U, key = choice of U:

- DiVincenzo, Horodecki, Leung, Smolin, Terhal 2004
- Hayden, Leung, Shor, Winter 2004

This work:

- Quantum key
- Success criterion: trace distance from decoupled state instead of accessible information

Conclusion

- Showed a general decoupling theorem
- Can be used in very diverse problems in quantum information theory and unifies them
- Showed coding theorems for channels with side information at the transmitter
- Showed (in the thesis!) coding theorems for broadcast channels
- Showed how to lock classical correlations into quantum states

What about the future?

- We have not used the decoupling theorem to its full potential yet
- Could be used to show protocols for channels with memory
- Other types of channels
- Optimality?
- Explicit protocols (with high concentration)

The End

Thank you!