Classical coding via dequantizing

Frédéric Dupuis
Aarhus University

Joint work with
Oleg Szehr *(TU München)*
Marco Tomamichel *(National University of Singapore)*

arXiv:1207.0067

January 8, 2013

Introduction

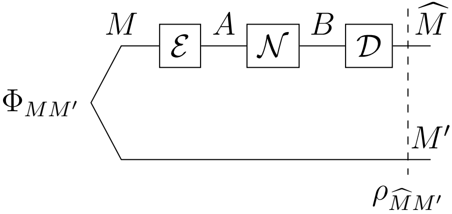
- A purely quantum idea in information theory: Given a pure state $|\rho\rangle_{ABC}$, absence of correlations between A and B means that both A and B are perfectly correlated with C.
- If $\rho_{AB} = \rho_A \otimes \rho_B$, then $|\rho\rangle_{ABC} = |\rho_1\rangle_{AC_A} \otimes |\rho_2\rangle_{BC_B}$.
- Many coding theorems for sending *quantum* information can be proven using this idea (called "decoupling").
- Doesn't seem to work for sending classical information: the information can be present in other systems without affecting the coding scheme.
- Our goal: come up with an analogue of this method for classical information.

Outline

- Coding via decoupling: a crash course
- From decoupling to dequantizing

Decoupling: a crash course

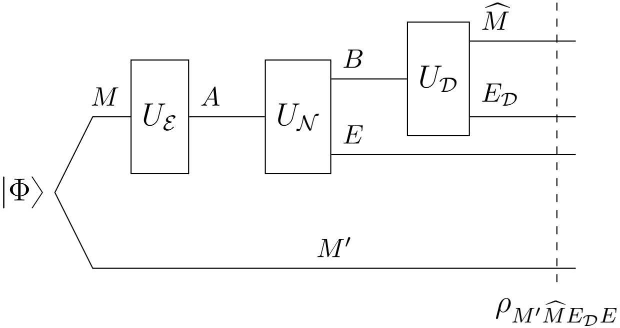
- The problem:



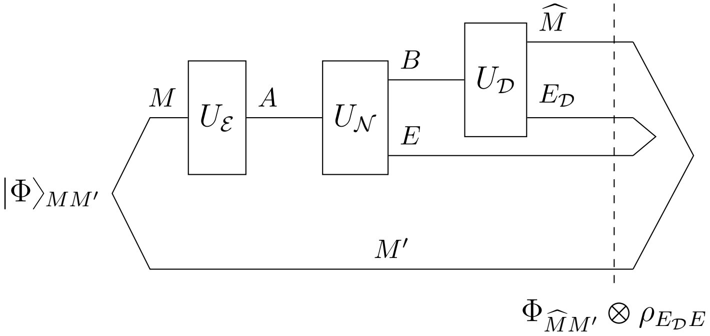
- Here $|\Phi\rangle = \frac{1}{\sqrt{N}} \sum_i |ii\rangle$.
- The hope: $\rho_{\widehat{M}M'} \approx \Phi_{MM'}$.

Decoupling: a crash course

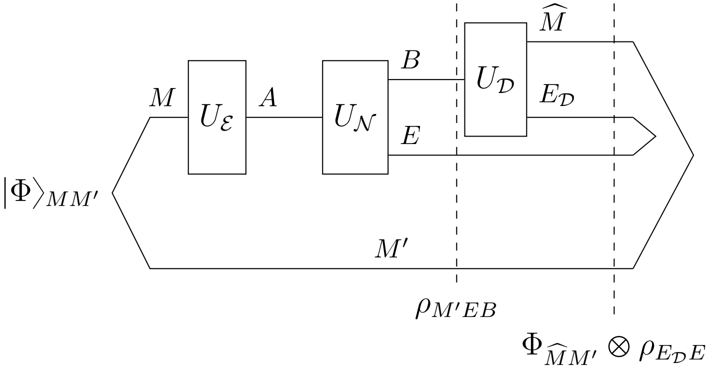
The trick: Purify everything.



We then hope that we obtain:

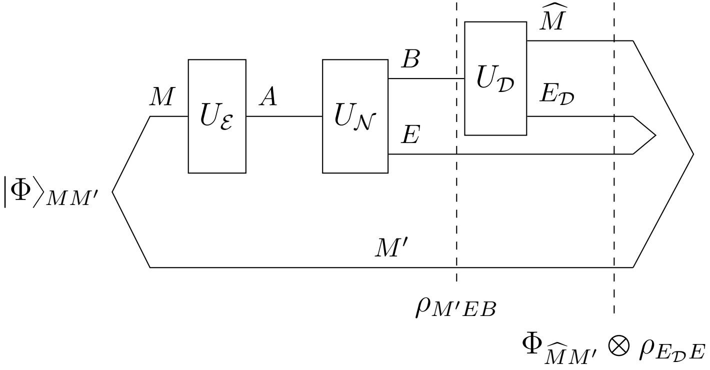


Decoupling: a crash course



- How do we get a decoder? The key: all purifications are equivalent up to a unitary on the purifying system.

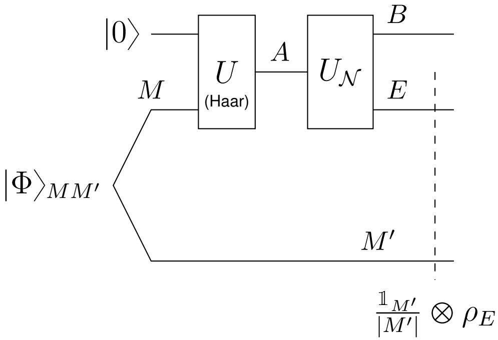
Decoupling: a crash course



- $\Phi_{M'\widehat{M}} \otimes \widehat{\rho}_{E_{\mathcal{D}}E}$ and $\rho_{M'EB}$ are both purifications of $\frac{\mathbb{1}_{M'}}{|M'|} \otimes \rho_E$.
- To get a decoder, we need to get $\frac{\mathbb{1}_{M'}}{|M'|} \otimes \rho_E$ at the output

Decoupling: a crash course

How do we ensure this?



- Encoding: embed M into a larger system, and then apply U chosen uniformly at random (a 2-design works too).
- If we have a product state $\frac{\mathbb{1}_{M'}}{|M'|} \otimes \rho_E$ at the output, then we know that a decoder exists.

Decoupling theorem

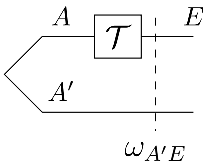
How do we ensure that M' is decoupled from the environment?

Theorem

Let $\mathcal{T}_{A\to E}$ be a channel. Then,

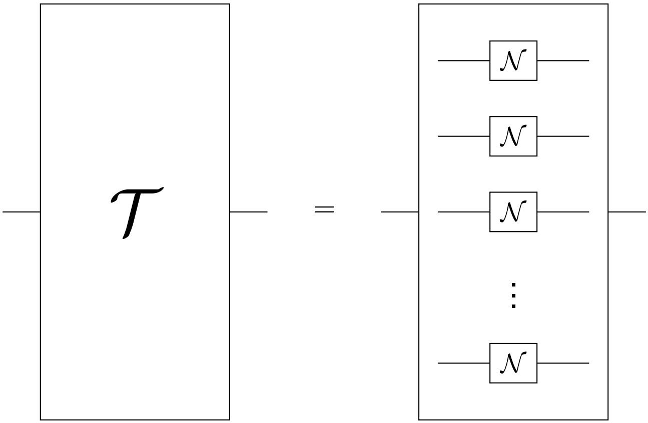
$$\mathbb{E}_{U_A}\left\|\mathcal{T}(U_A\rho_{AM'}U_A^\dagger) - \omega_E \otimes \frac{\mathbb{1}_{M'}}{|M'|}\right\|_1 \leqslant \sqrt{|M'|}2^{-\frac{1}{2}H_{\min}^{\varepsilon}(A'|E)_\omega} + O(\varepsilon).$$

where $\omega_{A'E}$ is a state of the form:



The iid case

One important case: $\mathcal{T} = \mathcal{N}^{\otimes n}$:



The iid case

Theorem

Let $\mathcal{T}_{A\to E}$ be a channel. Then,

$$\mathbb{E}_{U_A} \left\| \mathcal{T}(U_A \rho_{AM'} U_A^\dagger) - \omega_E \otimes \frac{\mathbb{1}_{M'}}{|M'|} \right\|_1 \leqslant \sqrt{|M'|} 2^{-\frac{1}{2} H_{\min}^{\varepsilon}(A'|E)_\omega} + O(\varepsilon).$$

- Fully quantum AEP: $H_{\min}^{\varepsilon}(A'|E)_{\omega^{\otimes n}} \rightsquigarrow nH(A'|E)_\omega = nI(A'\rangle B)_\omega$.
- Hence, need $\log|M'| \lesssim nI(A'\rangle B)_\omega$.
- We therefore recover the Lloyd-Shor-Devetak theorem this way.

The family tree

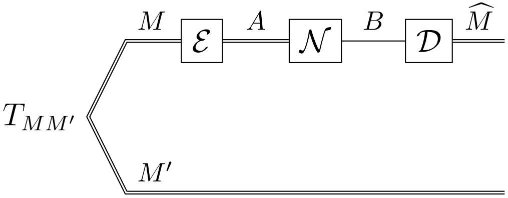
Other coding theorems that can be proven this way:

- Entanglement-assisted quantum (and classical) capacity: start with $|\Phi\rangle_{MM'} \otimes |\Phi\rangle_{\tilde{A}\tilde{B}}$.
- State transfer/"Fully Quantum Slepian-Wolf": Use $\mathcal{T}$ to be a partial trace.
- State merging: Choose $\mathcal{T}$ to be a measurement.
- Coding for quantum broadcast channels
- Etc. . .

What about sending classical information?

From decoupling to dequantizing

Sending classical information



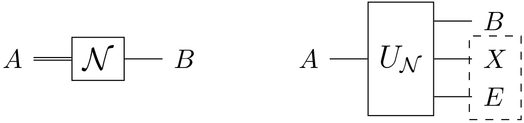
where

- $T_{MM'} := \frac{1}{N}\sum_{i=1}^{N} |ii\rangle\langle ii|_{MM'}$
- $\mathcal{N}$ is a CQ channel: $\mathcal{N}(\xi_A) = \sum_i \mathrm{Tr}[|i\rangle\langle i|\xi_A]\rho_B^i$.

Sending classical information

To use decoupling ideas, we need to purify everything. How do we purify a CQ channel?

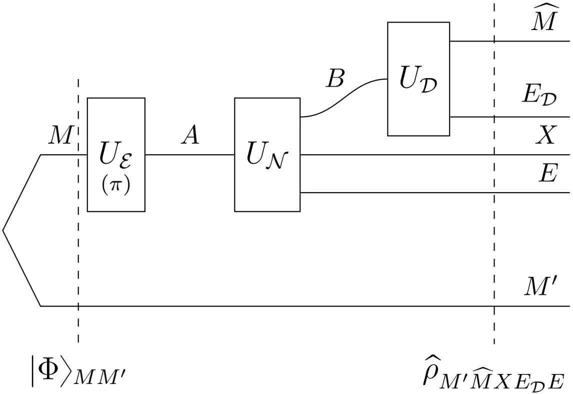
- $\mathcal{N}(\xi_A) = \sum_i \mathrm{Tr}[|i\rangle\langle i|\xi_A]\rho_B^i$.
- $U_{\mathcal{N}}|i\rangle_A = |i\rangle_X \otimes |\rho^i\rangle_{BE}$.



- The environment of the channel is now XE.

Sending classical information

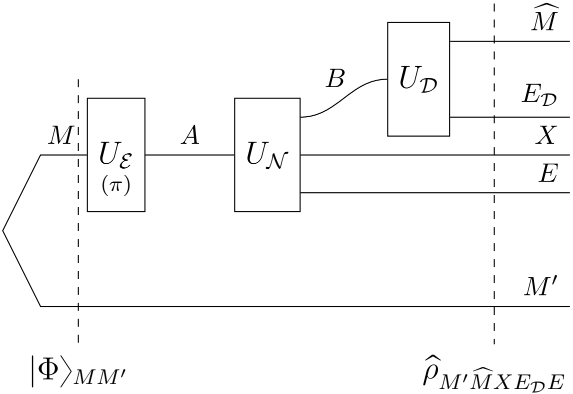
If we purify the entire process, we then get:



- Note that since the encoder $\mathcal{E}$ is classical, $U_{\mathcal{E}}$ is just a permutation π of the basis elements.

Sending classical information

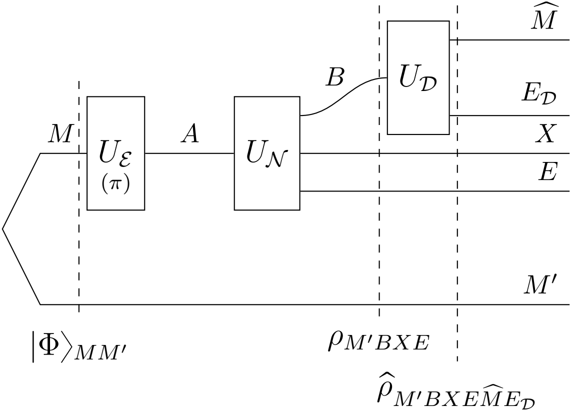
If we purify the entire process, we then get:



- Note that since the encoder $\mathcal{E}$ is classical, $U_{\mathcal{E}}$ is just a permutation π of the basis elements.
- In the end, we want to ensure that $\widehat{\rho}_{M'\widehat{M}} = \frac{1}{N}\sum_i |ii\rangle\langle ii|$.

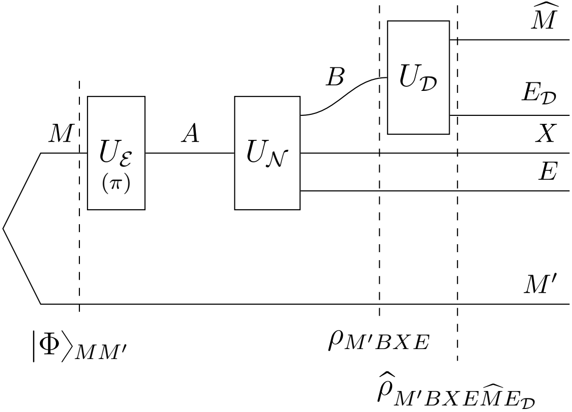
Sending classical information

What does that entail for the environment?



- We have that $|\widehat{\rho}\rangle = \frac{1}{\sqrt{N}} \sum_i |i i \pi(i)\rangle_{\widehat{M}M'X} \otimes |\xi^i\rangle_{EE_{\mathcal{D}}}$.
- This means that $\widehat{\rho}_{M'XE} = \frac{1}{N} \sum_i |i\pi(i)\rangle\langle i\pi(i)|_{M'X} \otimes \xi^i_E$.

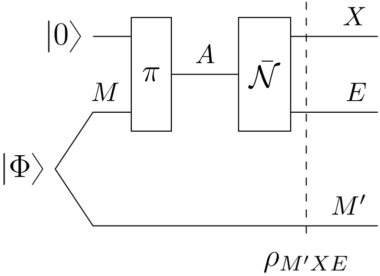
Sending classical information



- Only classical correlations between M' and environment XE.
- So, we need $\rho_{M'XE} = \frac{1}{N}\sum_i |i\pi(i)\rangle\langle i\pi(i)|_{M'X} \otimes \xi_E^i$.

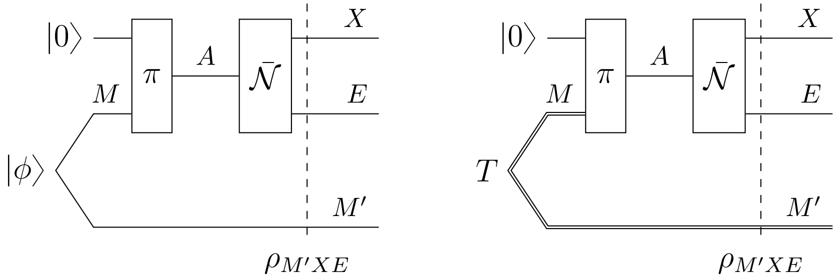
“Dequantizing” theorem

How can we enforce this?



- Encoder π is a permutation over all computation basis elements $|i\rangle$, chosen uniformly over the symmetric group.

“Dequantizing” theorem



- Encoder π is a permutation over all computation basis elements $|i\rangle$, chosen uniformly over the symmetric group.
- Look at the difference between left and right diagrams.

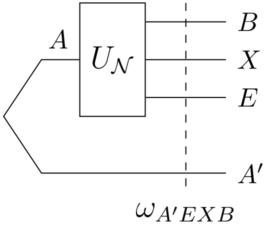
"Dequantizing" theorem

Theorem

Let $\bar{\mathcal{N}}_{A\to XE}$ be a complementary CQ channel. Then,

$$\mathbb{E}_\pi \left\| \bar{\mathcal{N}} \left(\pi_A (\Phi_{M'A} - T_{M'A}) \pi_A^\dagger \right) \right\|_1 \leqslant \sqrt{\frac{|M'|}{|A|}} 2^{-\frac{1}{2} H_{\min}^\varepsilon (A'|EX)_\omega} + O(\varepsilon).$$

where $\omega_{A'EXB}$ is a state of the form



HSW via dequantizing theorem

Theorem

Let $\bar{\mathcal{N}}_{A\to XE}$ be a complementary CQ channel. Then,

$$\mathbb{E}_{\pi_A \in \mathcal{P}(A)} \left\| \bar{\mathcal{N}} \left(\pi_A (\Phi_{M'A} - T_{M'A}) \pi_A^\dagger \right) \right\|_1 \leqslant \sqrt{\frac{|M'|}{|A'|}} 2^{-\frac{1}{2} H_{\min}(A'|EX)_\omega}.$$

- Suppose we apply this theorem to an iid channel.
- Choose typical subspace: $\log |A'| \rightsquigarrow nH(A')$.
- Quantum AEP:
  $H_{\min}^{\varepsilon}(A'|EX)_\omega \rightsquigarrow nH(A'|EX) = -nH(A'|B)$.
- Hence, $\log |A'| + H_{\min}^{\varepsilon}(A'|EX) \rightsquigarrow nI(A'; B)$.
- Need $\log |M'| \lesssim nI(A'; B)$

Conclusion

- We have a "decoupling-like" proof of the HSW theorem.
- Can this method be fruitfully applied to other problems?
- Can we get cleaner proofs of "mixed" problems (classical and quantum messages at the same time)?

Thank you!