Title: Surprises in the theory of quantum channel capacity

Date: Dec 09, 2008 11:50 AM

URL: http://pirsa.org/08120029

Abstract: A quantum channel models a physical process which adds noise to a quantum system by interacting with the environment. Protecting quantum systems from such noise can be viewed as an extension of the classical communication problem introduced by Shannon sixty years ago. A fundamental quantity of interest is the quantum capacity of a given channel. It measures the amount of quantum information that can be transmitted with vanishing error, in the limit of many independent transmissions over that channel. In this talk, I will show that certain pairs of channels, each with a capacity of zero, can have a strictly positive capacity when used together. This unveils a rich structure in the theory of quantum communication that is absent from Shannon\'s classical theory. This is joint work with Graeme Smith (IBM) which was published in the Sept. 26 issue of Science.

Quantum Channel Capacity

more surprises from quantum physics

Jon Yard

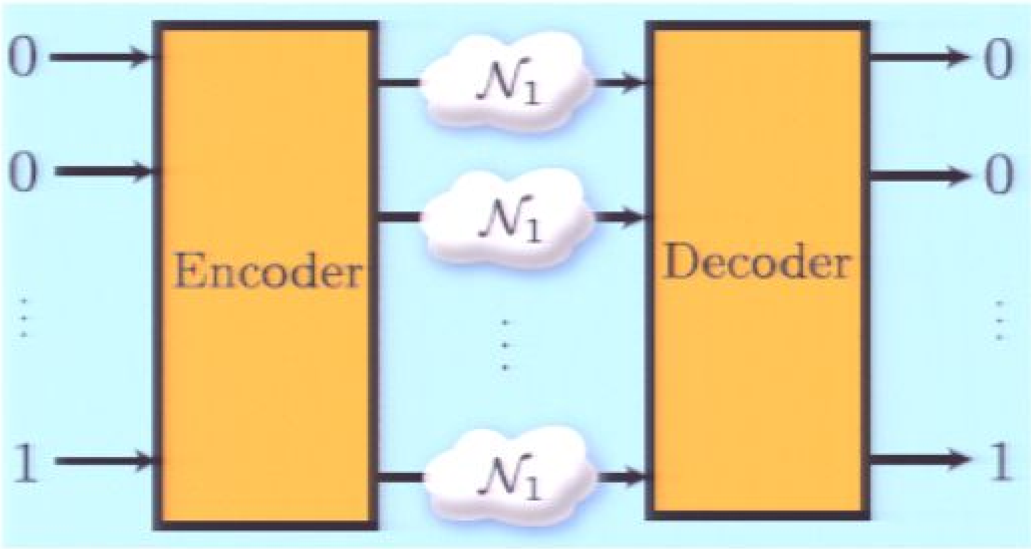
Los Alamos National Laboratory (CNLS/CCS-3)

based on joint with Graeme Smith (IBM) [*Science* '08]

Perimeter Institute YRC

December 9, 2008

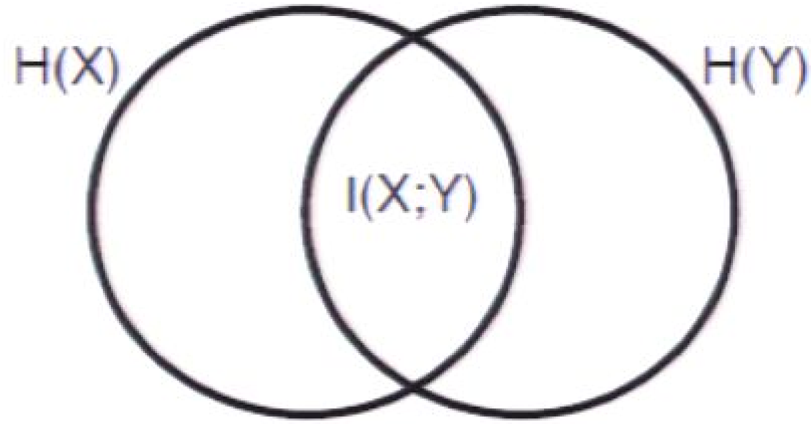
Shannon's capacity



- Conditional probabilities $p(y|x)$
- Capacity $\mathcal{C} = \#$ reliable bits / transmission
- Require error $\to 0$ as $\#$ transmissions $\to \infty$

Shannon's capacity formula

mutual information



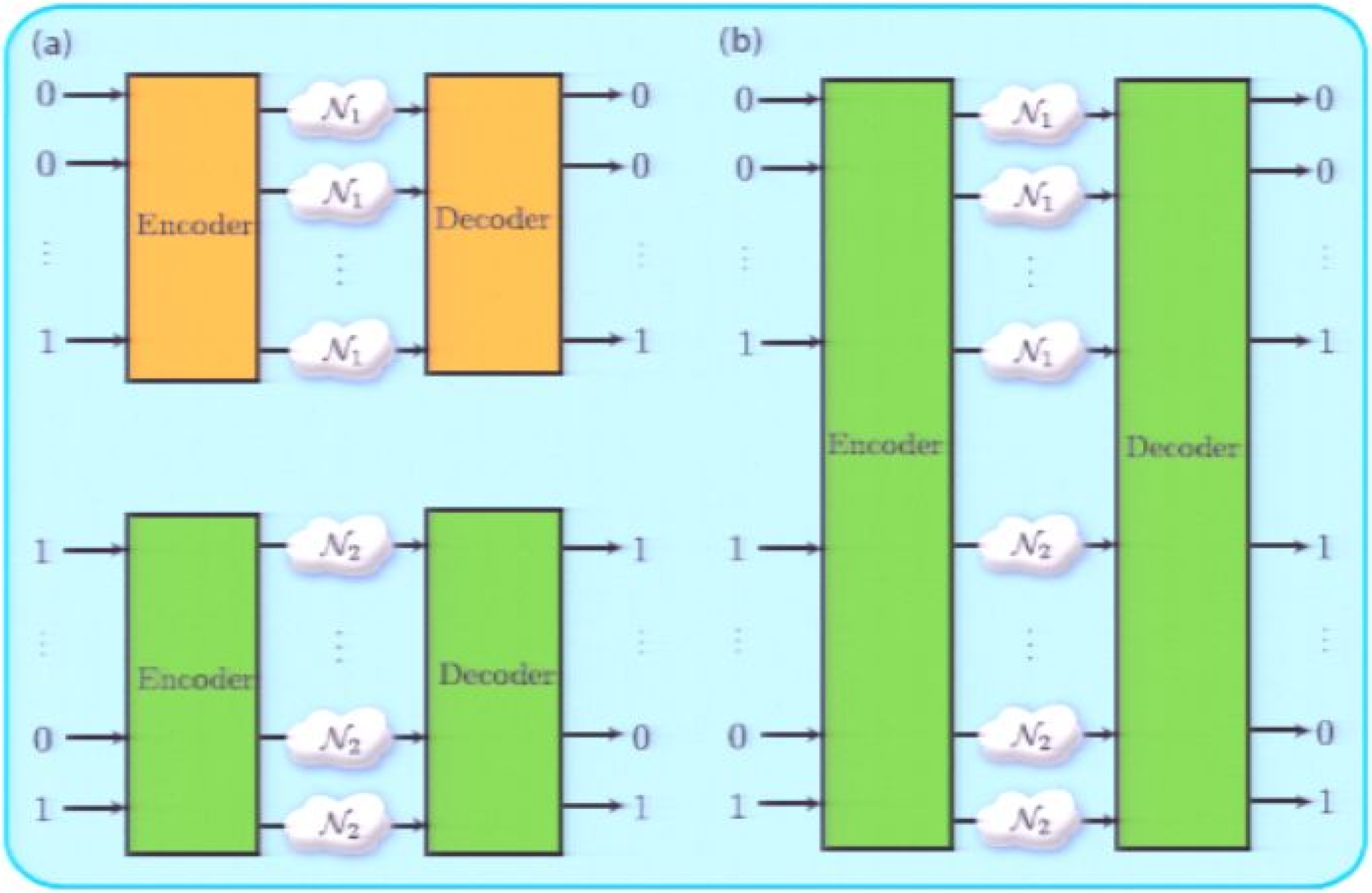
$$I(p) = I(X;Y) = H(X) + H(Y) - H(XY)$$

- Measures correlations ($I = 0 \Leftrightarrow X \perp Y$)
- Entropy $H(X) = -\sum_x p(x) \log_2 p(x)$

$$\mathcal{C} = \max_{p(x)} I(p)$$

- Proof gives matching lower & upper bounds (random coding + converse)

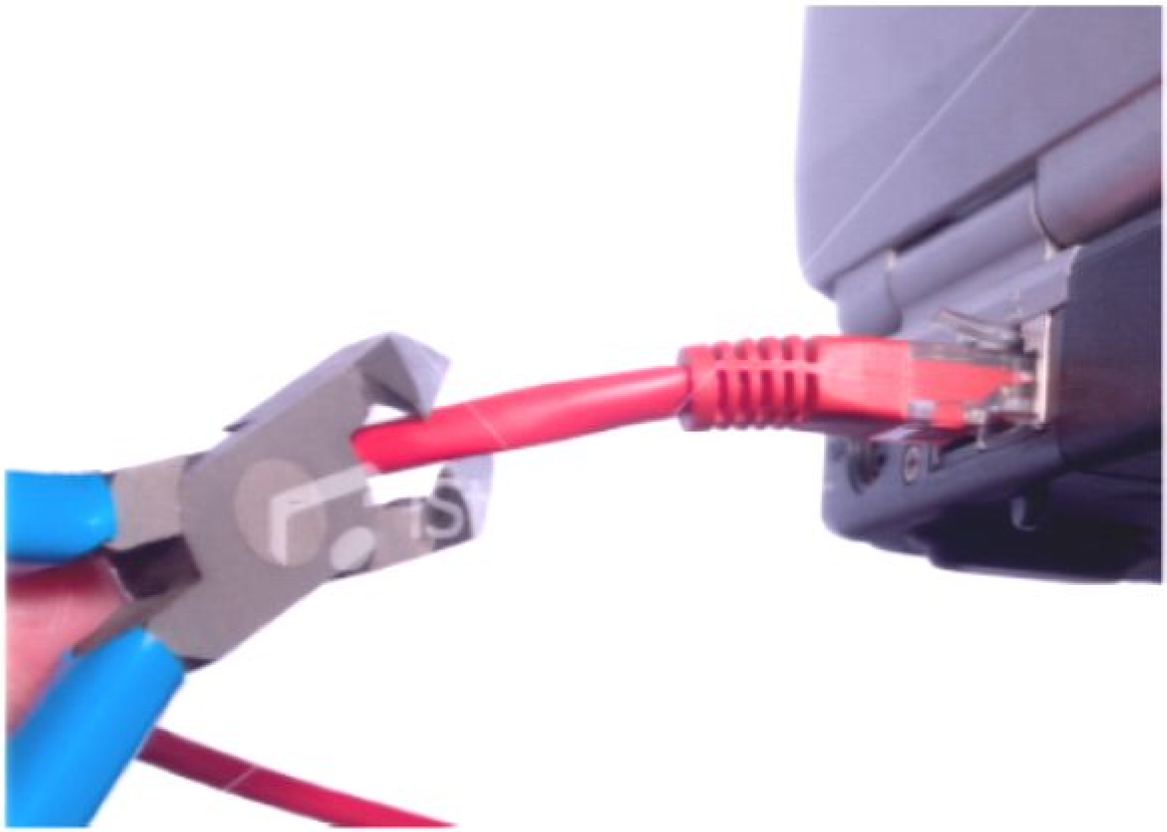
$\mathcal{C}$ is additive



$$\mathcal{C}(\mathcal{N}_1 \otimes \mathcal{N}_2) = \mathcal{C}(\mathcal{N}_1) + \mathcal{C}(\mathcal{N}_2)$$

$\mathcal{C}$ = value of channel, independent of other available channels

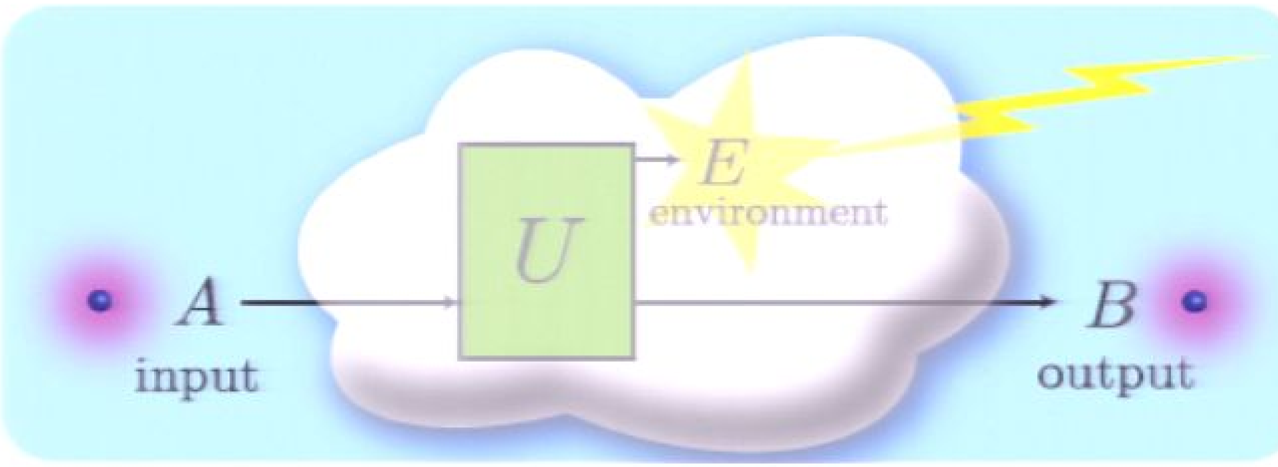
Zero capacity channels



all are easy to make

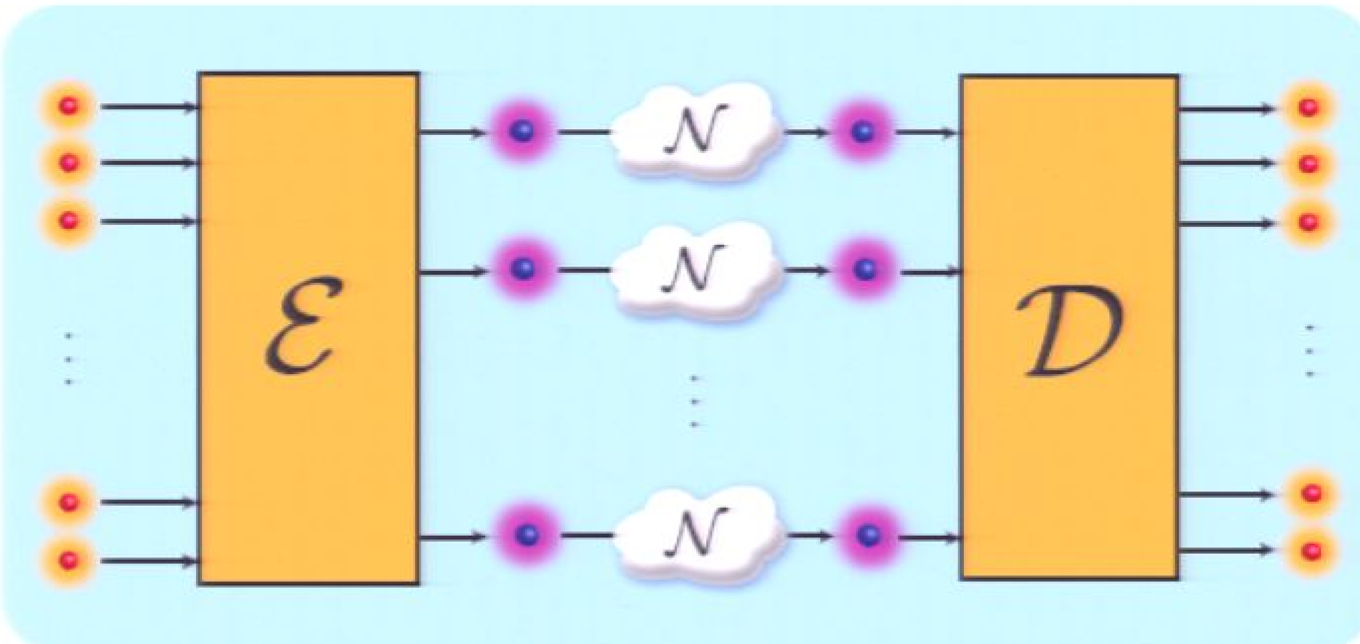
$\mathcal{C} = 0 \Leftrightarrow p(y|x)$ independent of x

Quantum channels



- Physical process adding noise to quantum states
- linear CPTP map on density matrices (general operation)
- Reversible interaction with inaccessible environment
- Trivial classification of $\mathcal{C} = 0$ channels, $0 + 0 = 0$

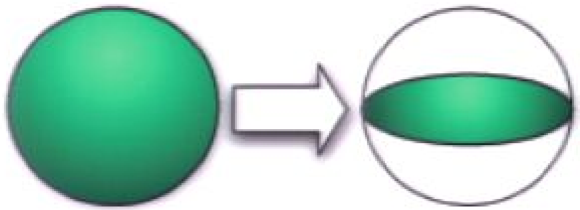
Quantum capacity $\mathcal{Q}$



- $\mathcal{Q} = \#$ qubits that can be reliably sent / transmission
- $\mathcal{Q} = \#$ ebits that can be reliably generated / transmission
- Questions characterize 'information conveying properties'
- Bounds on quantum error correction (independent noise)
- Not understood as well as Shannon's capacity

Examples

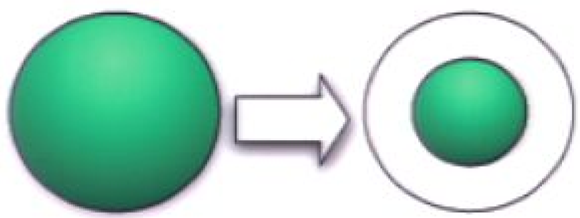
- Qubit flip



$$\rho \mapsto (1-p)\rho + pZ\rho Z$$

$$\mathcal{Q} = 1 - H(p)$$

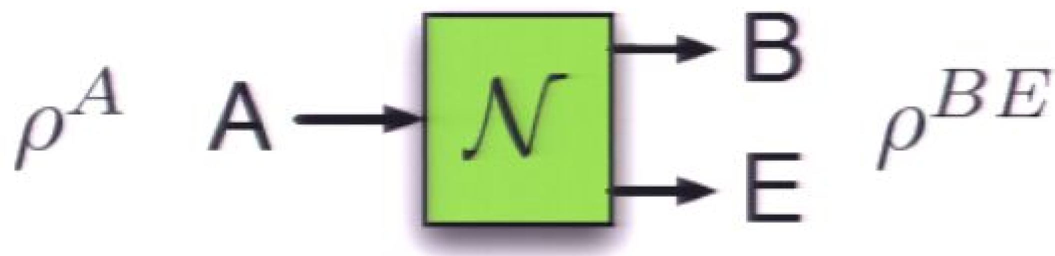
- Depolarizing



$$\rho \mapsto (1-p)\rho + pI/2$$

$$\mathcal{Q} > 0 \text{ for } p < p^* \text{ with } .2552 \leq p^* \leq .3333$$

General formula for $\mathcal{Q}$?

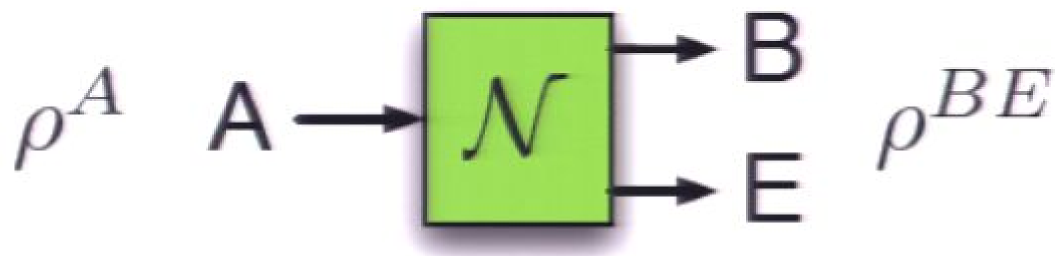


- Random codes [L,S,D,HHWY]

$$\mathcal{Q}(\mathcal{N}) \geq \mathcal{Q}^{(1)}(\mathcal{N}) = \max_{\rho^A} I_C(\rho^A)$$

- Coherent information $I_C(\rho^A) = H(B) - H(E)$
- Lower bound tight for 'degradable channels' [DS]

General formula for $\mathcal{Q}$?



- Random codes [L,S,D,HHWY]

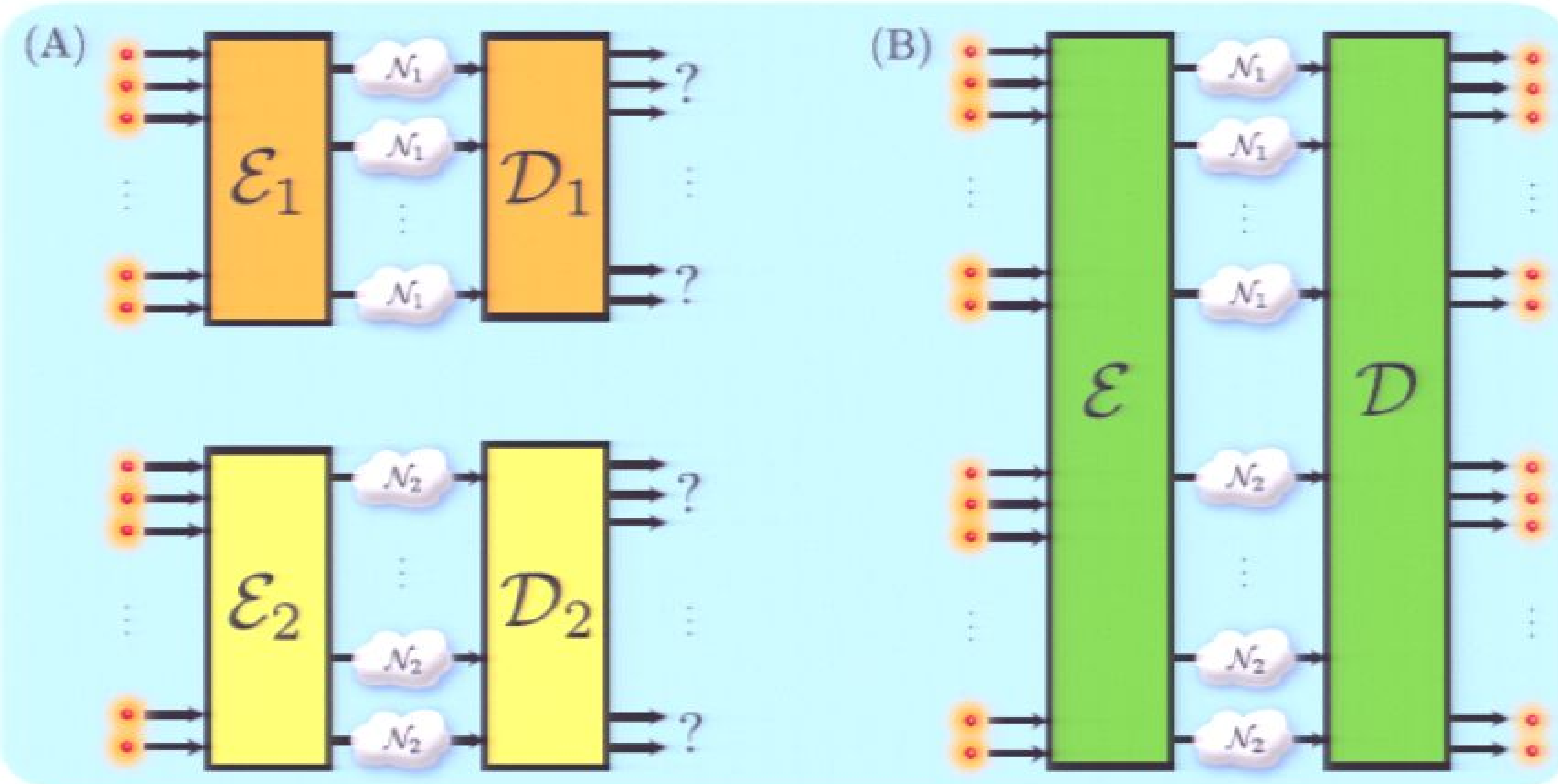
$$\mathcal{Q}(\mathcal{N}) \geq \mathcal{Q}^{(1)}(\mathcal{N}) = \max_{\rho^A} I_C(\rho^A)$$

- Coherent information $I_C(\rho^A) = H(B) - H(E)$
- Lower bound tight for 'degradable channels' [DS]
- Best we can currently prove:

$$\mathcal{Q}(\mathcal{N}) = \lim_{k\to\infty} \frac{1}{k} \mathcal{Q}^{(1)}(\mathcal{N}^{\otimes k})$$

- $\mathcal{Q}$ is 'regularization' of $\mathcal{Q}^{(1)}$

$\mathcal{Q}$ is not additive $(0 + 0 > 0)$

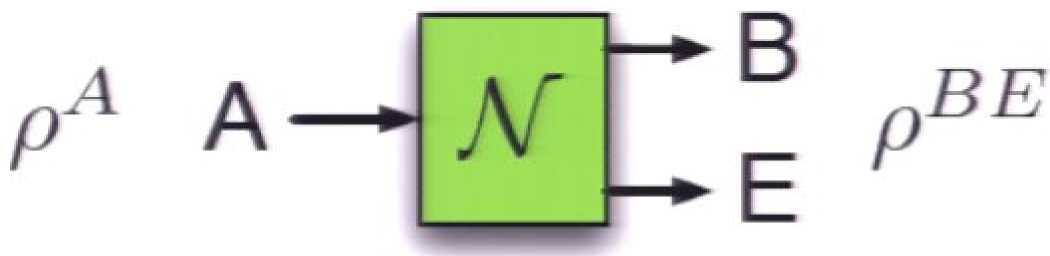


There exist channels $\mathcal{N}_1$ and $\mathcal{N}_2$ such that

$$\mathcal{Q}(\mathcal{N}_1) = \mathcal{Q}(\mathcal{N}_2) = 0, \quad \mathcal{Q}(\mathcal{N}_1 \otimes \mathcal{N}_2) > 0$$

Should I pay for 0-capacity channels?

General formula for $\mathcal{Q}$?



- Random codes [L,S,D,HHWY]

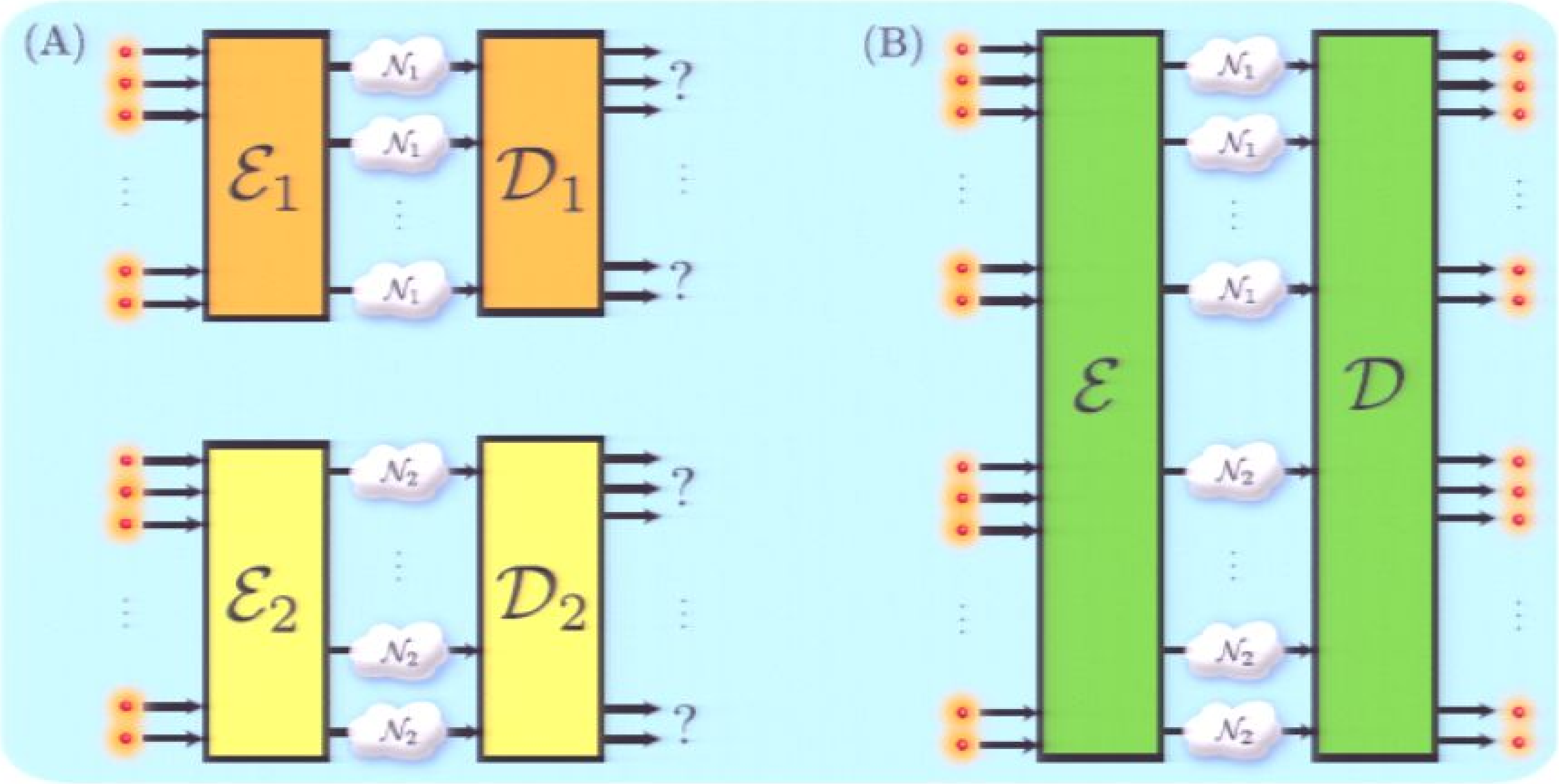
$$\mathcal{Q}(\mathcal{N}) \geq \mathcal{Q}^{(1)}(\mathcal{N}) = \max_{\rho^A} I_C(\rho^A)$$

- Coherent information $I_C(\rho^A) = H(B) - H(E)$
- Lower bound tight for 'degradable channels' [DS]
- Best we can currently prove:

$$\mathcal{Q}(\mathcal{N}) = \lim_{k \to \infty} \frac{1}{k} \mathcal{Q}^{(1)}(\mathcal{N}^{\otimes k})$$

- $\mathcal{Q}$ is 'regularization' of $\mathcal{Q}^{(1)}$

$\mathcal{Q}$ is not additive $(0 + 0 > 0)$



There exist channels $\mathcal{N}_1$ and $\mathcal{N}_2$ such that

$$\mathcal{Q}(\mathcal{N}_1) = \mathcal{Q}(\mathcal{N}_2) = 0, \quad \mathcal{Q}(\mathcal{N}_1 \otimes \mathcal{N}_2) > 0$$

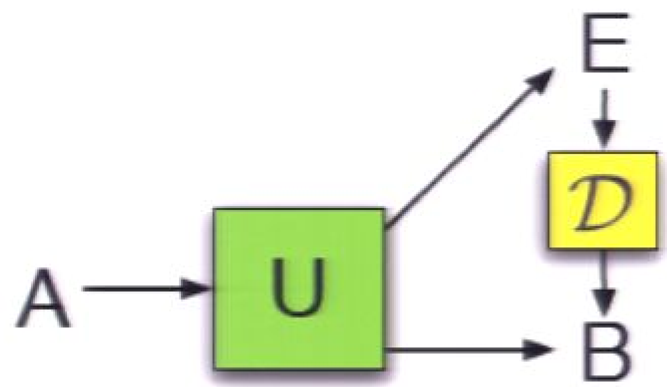
Should I pay for 0-capacity channels?

$\mathcal{Q} = 0$ channels

- $\mathcal{Q} = 0$ does not imply uncorrelated
- No complete classification known
- Not convex!
- Two important convex subsets (m/f?):

- $\mathcal{Q} = 0$ for different reasons (they cancel each other)
- Can have $\mathcal{Q} > 0$ in between...

Anti-degradable channels



- Environment can simulate output
- $\mathcal{Q} = 0$ by no cloning
- Stable under $\bigotimes$ (so $0 + 0 = 0$)
- Example: U maps into (anti)-symmetric subspace of BE e.g. 50%-erasure channel $\mathcal{A}(\rho) = \frac{1}{2}\rho + \frac{1}{2}|\text{erase}\rangle\langle\text{erase}|$
- Such 'symmetric channels' are also degradable
- $\mathcal{Q}$ completely understood for degradable

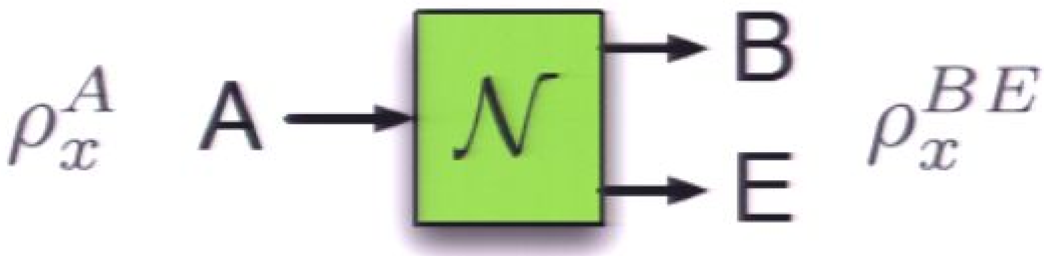
Horodecki channels

- Entanglement-binding channels
- Only creates states with Positive Partial Transpose:

$$\left(\rho^{AB}\right)^{\Gamma} = \begin{pmatrix} \begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix}^{T} & \begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix}^{T} \\ \begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix}^{T} & \begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix}^{T} \end{pmatrix} \geq 0$$

- Cannot go from $\rho^{\Gamma} \geq 0 \longrightarrow \rho^{\Gamma} \ngeq 0$ by LOCC
- $\mathcal{Q} = 0$ because (any entangled pure state)$^{\Gamma} \ngeq 0$
- Stable under $\bigotimes$ (so $0 + 0 = 0$)
- Some allow private classical communication

Private channels

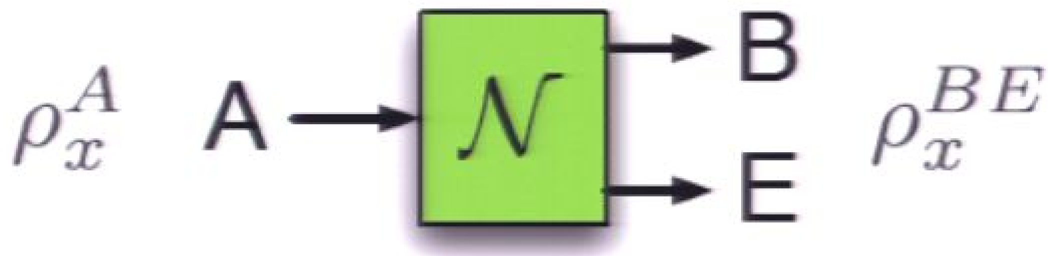


- Private capacity $\mathcal{P}(\mathcal{N}) = \#$ bits can reliably send requiring that $\rho^{E^n} \approx$ independent of message
- $\exists$ private Horodecki channels with $\mathcal{Q} = 0, \mathcal{P} > 0$ [H^3O,H^3P]
- $\mathcal{P}(\mathcal{N})$ is regularized maximum of private information

$$\mathcal{P}^{(1)} = \max_{p(x),\rho_x^A} I(X;B) - I(X;E)$$

- Coherent information is private information restricted to pure states:

Private channels



- Private capacity $\mathcal{P}(\mathcal{N}) = \#$ bits can reliably send requiring that $\rho^{E^n} \approx$ independent of message
- $\exists$ private Horodecki channels with $\mathcal{Q} = 0, \mathcal{P} > 0$ [H^3O,H^3P]
- $\mathcal{P}(\mathcal{N})$ is regularized maximum of private information

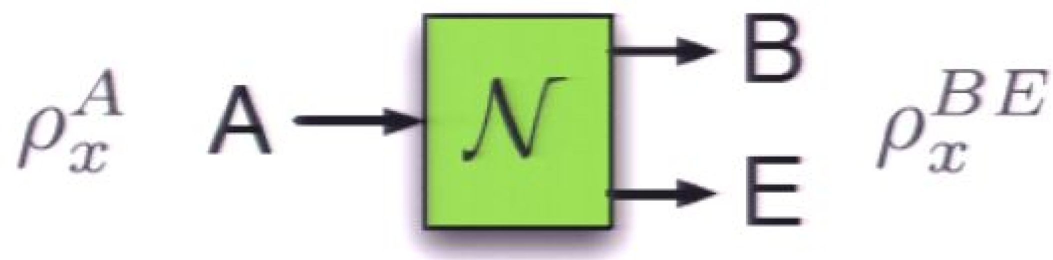
$$\mathcal{P}^{(1)} = \max_{p(x),\rho_x^A} I(X;B) - I(X;E)$$

- Coherent information is private information restricted to pure states:

$$I_c(\rho_A) = H(B) - H(E) = I(X;B) - I(X;E)$$

for any ensemble with $\sum_x p(x)|\psi_x\rangle\langle\psi_x|^A = \rho^A$

Counterexample to additivity of $\mathcal{Q}$

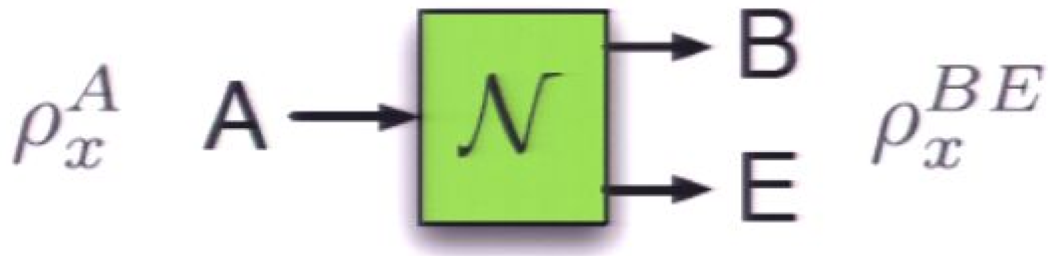


Theorem. Let $p(x)$, $\{\rho_x^A\}$ and $\mathcal{N}$ be given. Let $\mathcal{E}$ be a 50%-erasure channel with input dimension $\sum_x \text{rank}(\rho_x^A)$. Then

$$\mathcal{Q}^{(1)}(\mathcal{N} \otimes \mathcal{E}) \geq \frac{1}{2} I(X;B) - \frac{1}{2} I(X;E)$$

$\exists$ private Horodecki channel with 4D input such that on uniform ensemble $|x\rangle\langle x| \otimes I_2/2$, we have $I(X;B) - I(X;E) > .02$. So together with a 4D erasure channel, it has $\mathcal{Q} > .01$.

Counterexample to additivity of $\mathcal{Q}$



Theorem. Let $p(x)$, $\{\rho_x^A\}$ and $\mathcal{N}$ be given. Let $\mathcal{E}$ be a 50%-erasure channel with input dimension $\sum_x \text{rank}(\rho_x^A)$. Then

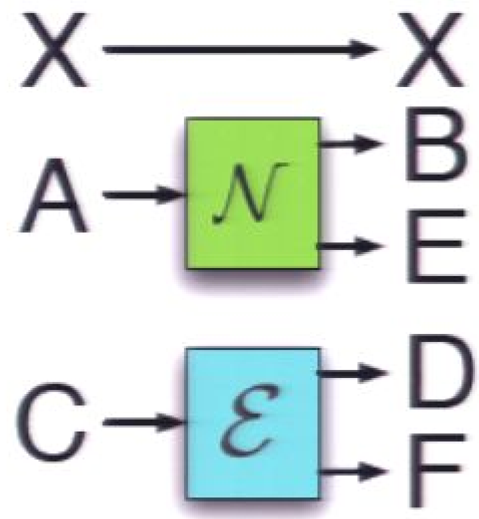
$$\mathcal{Q}^{(1)}(\mathcal{N} \otimes \mathcal{E}) \geq \frac{1}{2} I(X;B) - \frac{1}{2} I(X;E)$$

$\exists$ private Horodecki channel with 4D input such that on uniform ensemble $|x\rangle\langle x| \otimes I_2/2$, we have $I(X;B) - I(X;E) > .02$. So together with a 4D erasure channel, it has $\mathcal{Q} > .01$.

Proof

Define $|\rho\rangle^{XAC} = \sum_x \sqrt{p(x)}|x\rangle^X|\rho_x\rangle^{AC}$

so $\rho^{XA} = \sum_x p(x)|x\rangle\langle x|^X \otimes \rho_x^A$

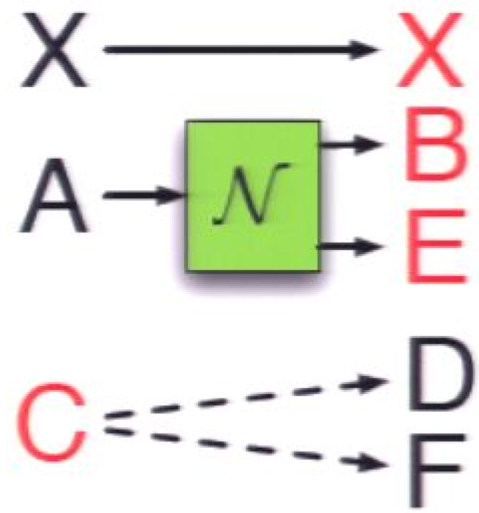


$$Q^{(1)} \geq H(BD) - H(EF)$$

Proof

Define $|\rho\rangle^{XAC} = \sum_x \sqrt{p(x)}|x\rangle^X |\rho_x\rangle^{AC}$

so $\rho^{XA} = \sum_x p(x)|x\rangle\langle x|^X \otimes \rho_x^A$



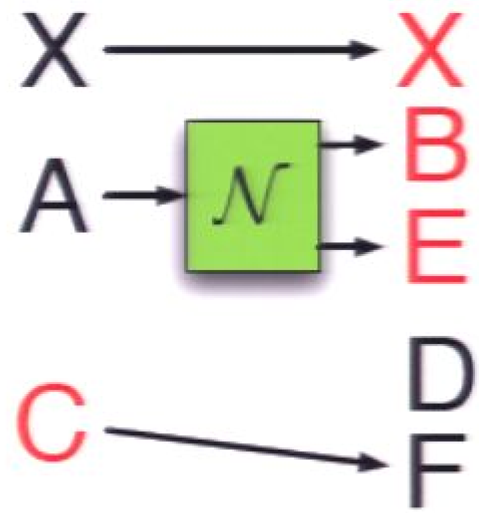
$Q^{(1)} \geq H(BD) - H(EF)$

write as entropies on state $|\rho\rangle^{XBEC}$ before erasure $\mathcal{E}$

Proof

Define $|\rho\rangle^{XAC} = \sum_x \sqrt{p(x)}|x\rangle^X|\rho_x\rangle^{AC}$

so $\rho^{XA} = \sum_x p(x)|x\rangle\langle x|^X \otimes \rho_x^A$

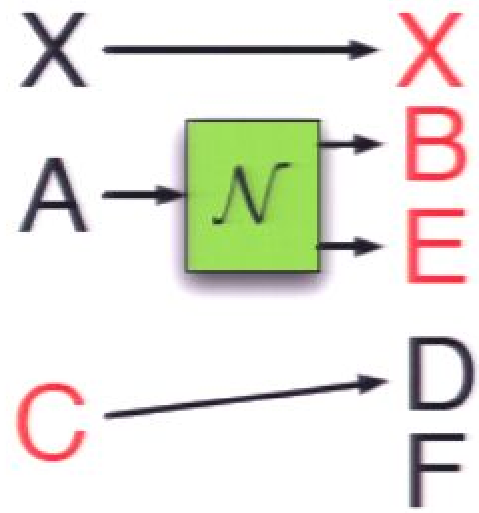


$$
\begin{aligned}
Q^{(1)} &\geq H(BD) - H(EF) \\
&\quad \text{write as entropies on state } |\rho\rangle^{XBEC} \text{ before erasure } \mathcal{E} \\
&= \tfrac{1}{2}(H(B) - H(EC))
\end{aligned}
$$

Proof

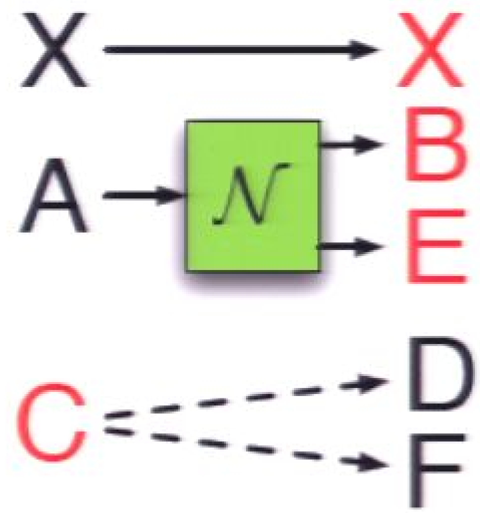
Define $|\rho\rangle^{XAC} = \sum_x \sqrt{p(x)}|x\rangle^X |\rho_x\rangle^{AC}$

so $\rho^{XA} = \sum_x p(x)|x\rangle\langle x|^X \otimes \rho_x^A$



$$
\begin{aligned}
Q^{(1)} &\geq H(BD) - H(EF) \\
&\quad \text{write as entropies on state } |\rho\rangle^{XBEC} \text{ before erasure } \mathcal{E} \\
&= \tfrac{1}{2}(H(B) - H(EC)) + \tfrac{1}{2}(H(BC) - H(E))
\end{aligned}
$$

Proof



Define $|\rho\rangle^{XAC} = \sum_x \sqrt{p(x)}|x\rangle^X|\rho_x\rangle^{AC}$

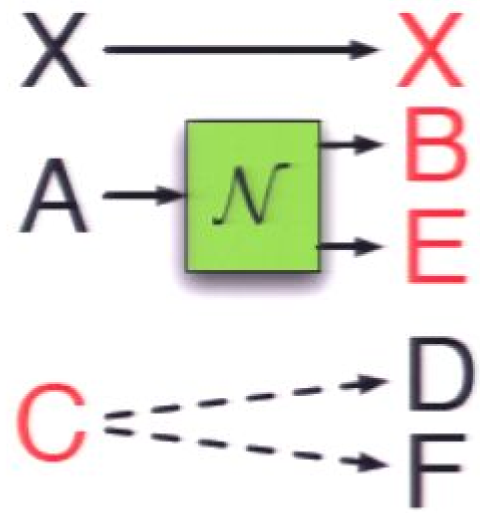
so $\rho^{XA} = \sum_x p(x)|x\rangle\langle x|^X \otimes \rho_x^A$

$$
\begin{aligned}
Q^{(1)} &\geq H(BD) - H(EF) \\
&\quad \text{write as entropies on state } |\rho\rangle^{XBEC} \text{ before erasure } \mathcal{E} \\
&= \tfrac{1}{2}(H(B) - H(EC)) + \tfrac{1}{2}(H(BC) - H(E)) \\
&= \tfrac{1}{2}(H(B) - H(XB)) + \tfrac{1}{2}(H(XE) - H(E)) \quad \left(\text{on } |\rho\rangle^{XBEC}\right)
\end{aligned}
$$

Proof

Define $|\rho\rangle^{XAC} = \sum_x \sqrt{p(x)}|x\rangle^X|\rho_x\rangle^{AC}$

so $\rho^{XA} = \sum_x p(x)|x\rangle\langle x|^X \otimes \rho_x^A$



$$
\begin{aligned}
Q^{(1)} &\geq H(BD) - H(EF) \\
&\quad \text{write as entropies on state } |\rho\rangle^{XBEC} \text{ before erasure } \mathcal{E} \\
&= \tfrac{1}{2}(H(B) - H(EC)) + \tfrac{1}{2}(H(BC) - H(E)) \\
&= \tfrac{1}{2}(H(B) - H(XB)) + \tfrac{1}{2}(H(XE) - H(E)) \quad \left(\text{on } |\rho\rangle^{XBEC}\right) \\
&= \tfrac{1}{2}I(X;B) - \tfrac{1}{2}I(X;E)
\end{aligned}
$$

Wrapping up

Other implications:

- $\mathcal{Q}$ is not convex! (Even though $\mathcal{C}$ and I_C are)

$$(1-p)\,\mathcal{N}\otimes|0\rangle\langle 0| + p\,\mathcal{E}\otimes|1\rangle\langle 1|, \quad p < .0041$$

- Still hope for some channels with $\mathcal{Q} = 0$

Wrapping up

Other implications:

- $\mathcal{Q}$ is not convex! (Even though $\mathcal{C}$ and I_C are)

$$(1-p)\,\mathcal{N}\otimes|0\rangle\langle 0| + p\,\mathcal{E}\otimes|1\rangle\langle 1|, \quad p < .0041$$

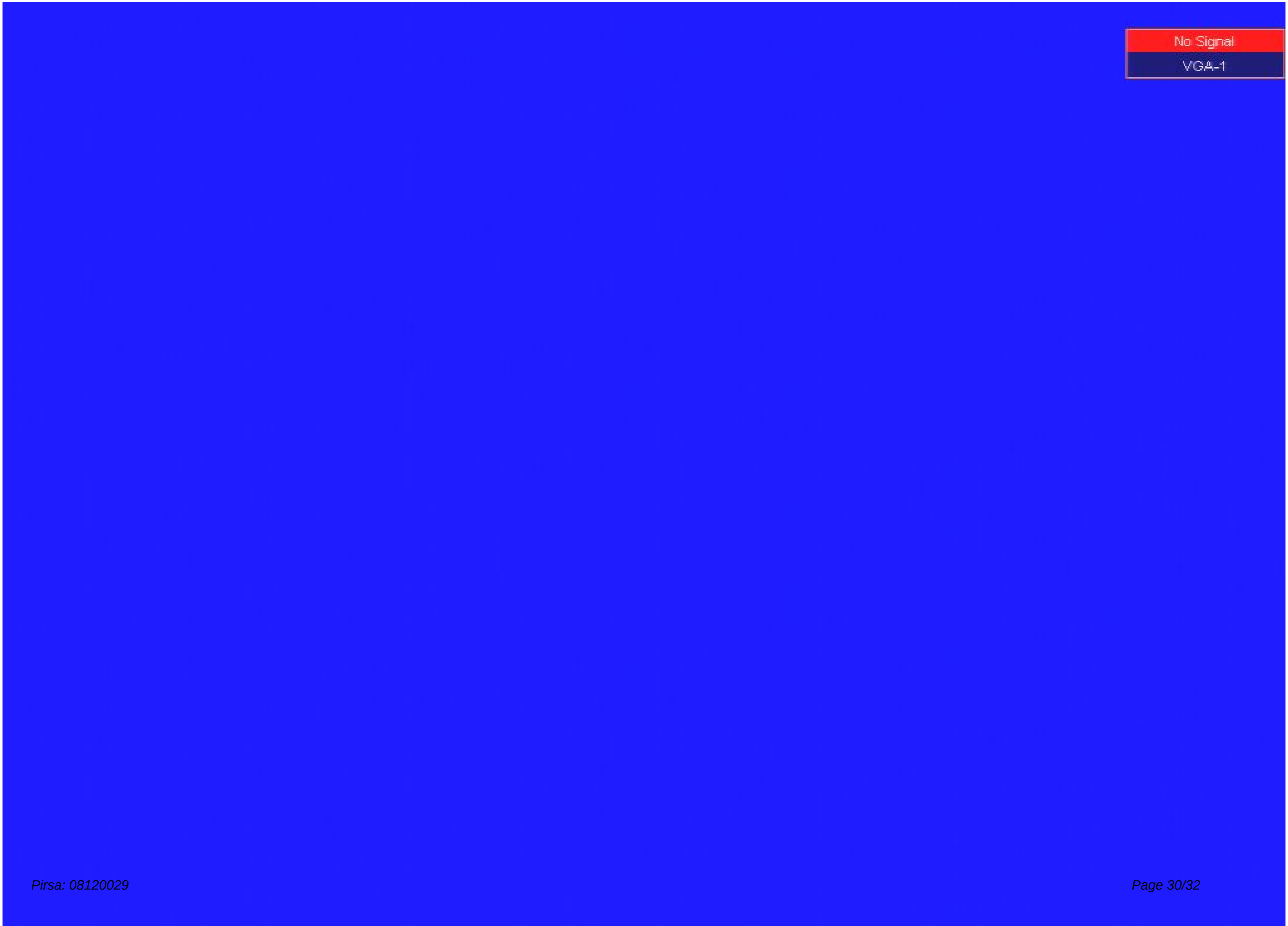
- Still hope for some channels with $\mathcal{Q} = 0$

Some questions:

- How do I price quantum bandwidth?

  What characterizes info. conveying properties of $\mathcal{N}$?

- Characterize $\mathcal{Q} = 0$ channels
- Are there more classes of them?
- Boundary of anti-degradable channels?


No Signal
VGA-1

No Signal
VGA-1


No Signal
VGA-1