Can non-private channels transmit quantum information?

Graeme Smith
John A. Smolin

PRL 102, 010501 (2009)
quant-ph/0810.0276

Holevo quantity

$$\chi(\mathcal{N},\mathcal{E}) = S\left(\sum_i p_i\mathcal{N}(\rho_i)\right) - \sum_i p_i S(\mathcal{N}(\rho_i))$$

$$\text{for an ensemble } \{p_i,\rho_i\}$$

Privacy (one-shot)

$$\mathcal{P}^{(1)}(\mathcal{N}) = \max_{\mathcal{E}}\Big(\chi(\mathcal{N},\mathcal{E}) - \chi(\widehat{\mathcal{N}},\mathcal{E})\Big)$$

$$\mathcal{P}(\mathcal{N}) = \lim_{n\to\infty}\frac{1}{n}\mathcal{P}^{(1)}(\mathcal{N}^{\otimes n})$$ Regularized

Smith and Yard

$$\mathcal{Q}(\mathcal{N}_H) = \mathcal{Q}(\mathcal{A}) = 0 \text{ but } \mathcal{Q}(\mathcal{N}_H \otimes \mathcal{A}) > 0$$

$\mathcal{A}$ is the erasure channel

$\mathcal{N}_H$ is the Horodecki private channel

$\mathcal{P}(\mathcal{N}_H) > 0$ and $\mathcal{N}_H$ is PPT

$$\mathcal{Q}(\mathcal{A}) = \mathcal{P}(\mathcal{A}) = 0$$

$$\mathcal{Q}(\mathcal{N} \otimes \mathcal{A}) \geq \frac{1}{2}\mathcal{P}(\mathcal{N})$$

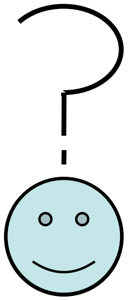
even when $\mathcal{Q}(\mathcal{N}) = 0$

so $\mathcal{Q}(\mathcal{N}_H \otimes \mathcal{A}) \geq \frac{1}{2}\mathcal{P}(\mathcal{N}_H) \simeq .01$

It would appear that the two kinds of resources are:

Symmetric Assistance (erasure)

Privacy



Superadditivity of quantum capacity might well be generic

Even *superactivation* might be common

The big problem is that we can hardly ever calculate the capacity

In part this is because of additivity problems

We don't even have good bounds on Q or P :

Best bound is the additive extension bound SS08

It can't detect superadditivity because it's an additive bound

Confining our attention to zero-capacity channels

PPT channels (Horodecki channel)

Antidegradable channels (Erasure channel)

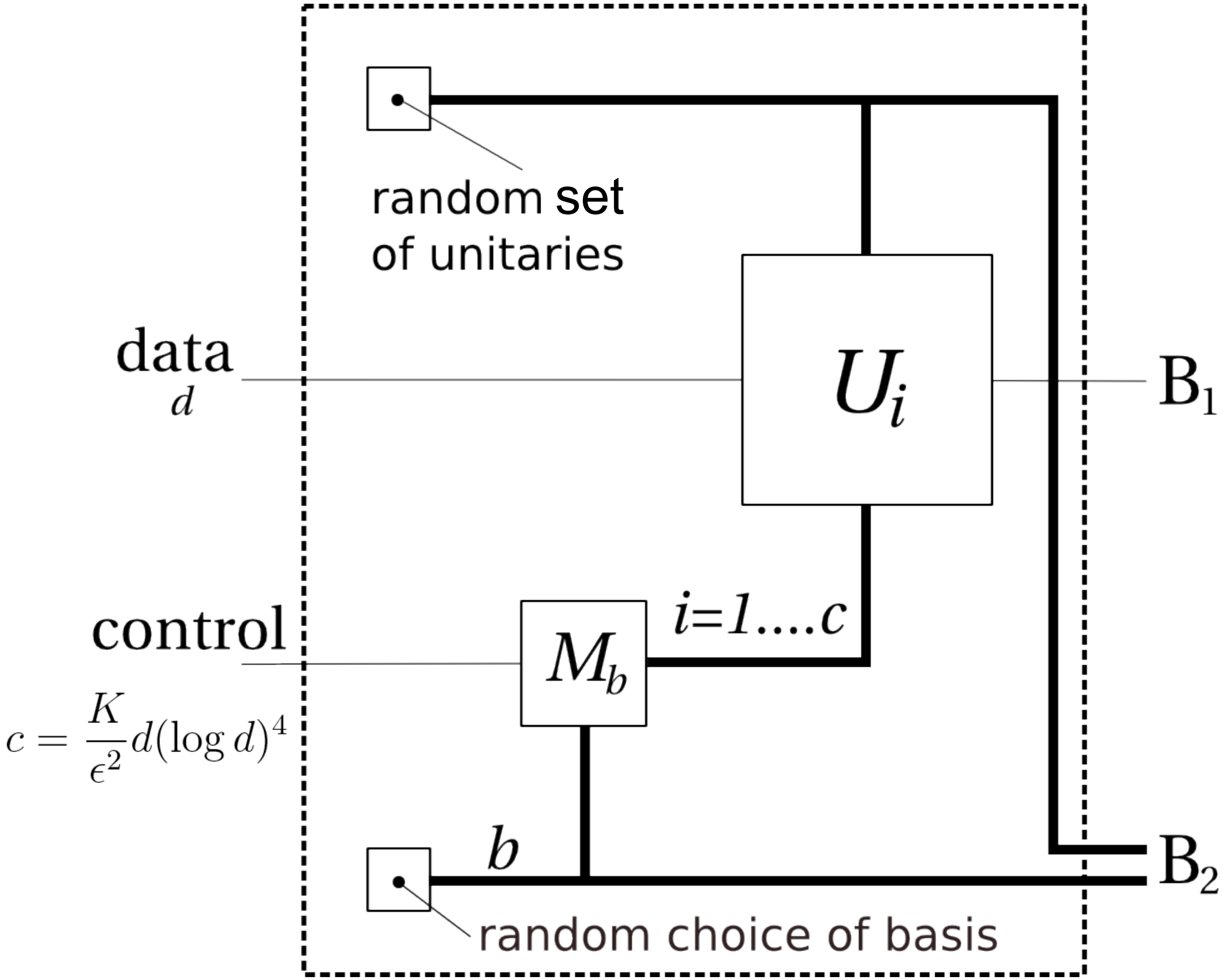
And that's it. Both are used in SY08

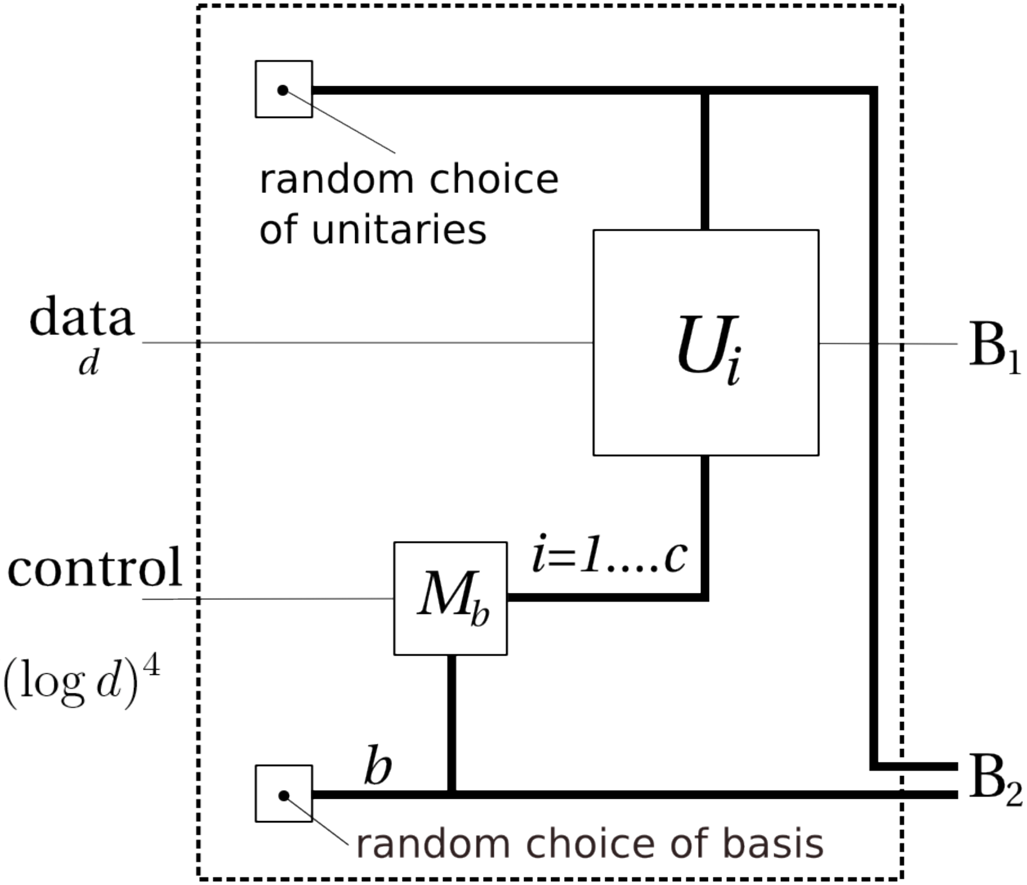
Other possibilities:

NPT bound-entangled channels?

$$\mathcal{Q} \leq \mathcal{P} \leq \mathcal{C} \text{ (the classical capacity)}$$

The Retro-correctible channel



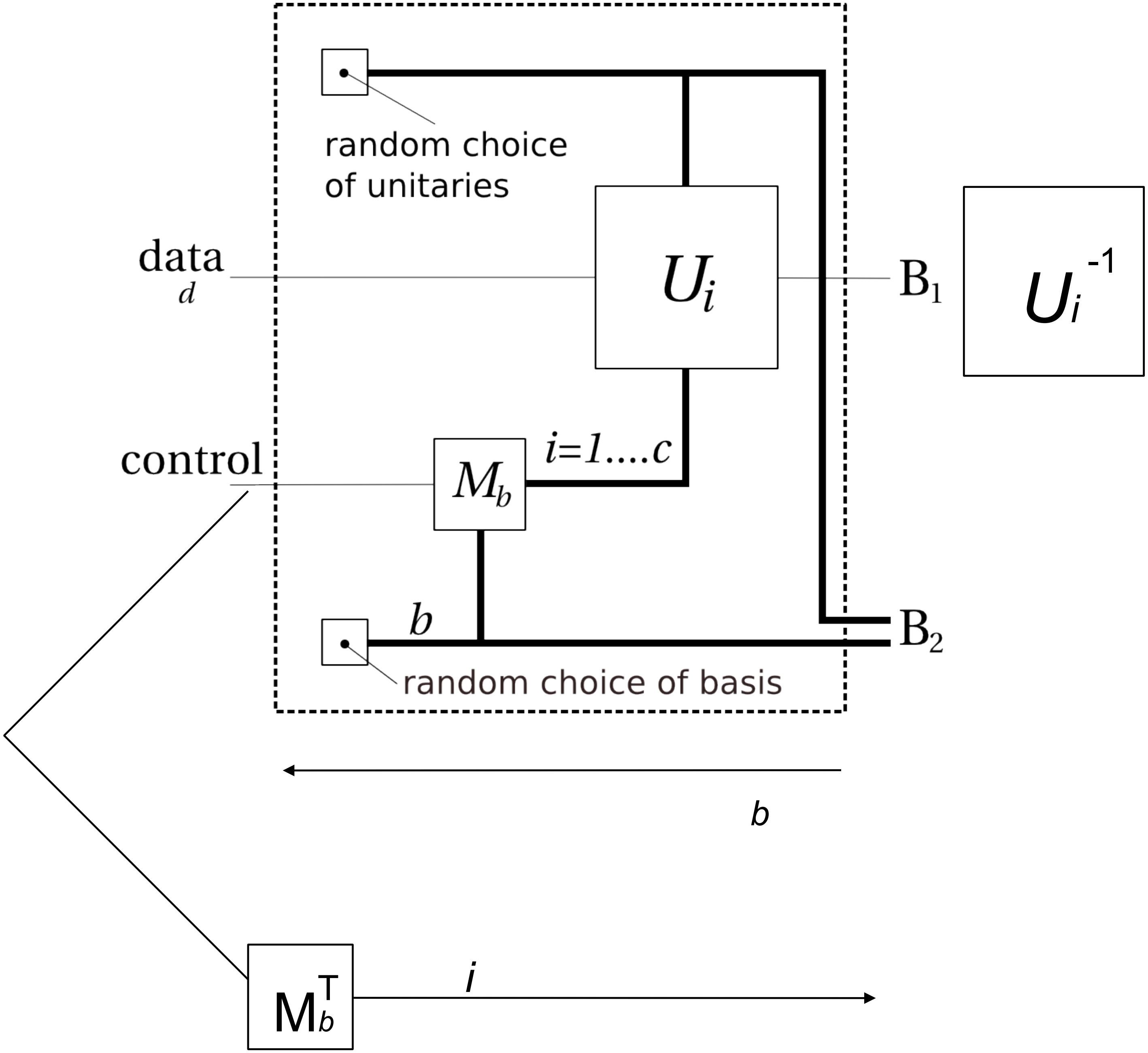


$$c = \frac{K}{\epsilon^2} d(\log d)^4$$

For large d $\chi(\mathcal{R}_d^\epsilon) \leq \epsilon$

therefore $\mathcal{Q} \leq \mathcal{P} \leq \mathcal{C} = \chi \leq \epsilon$

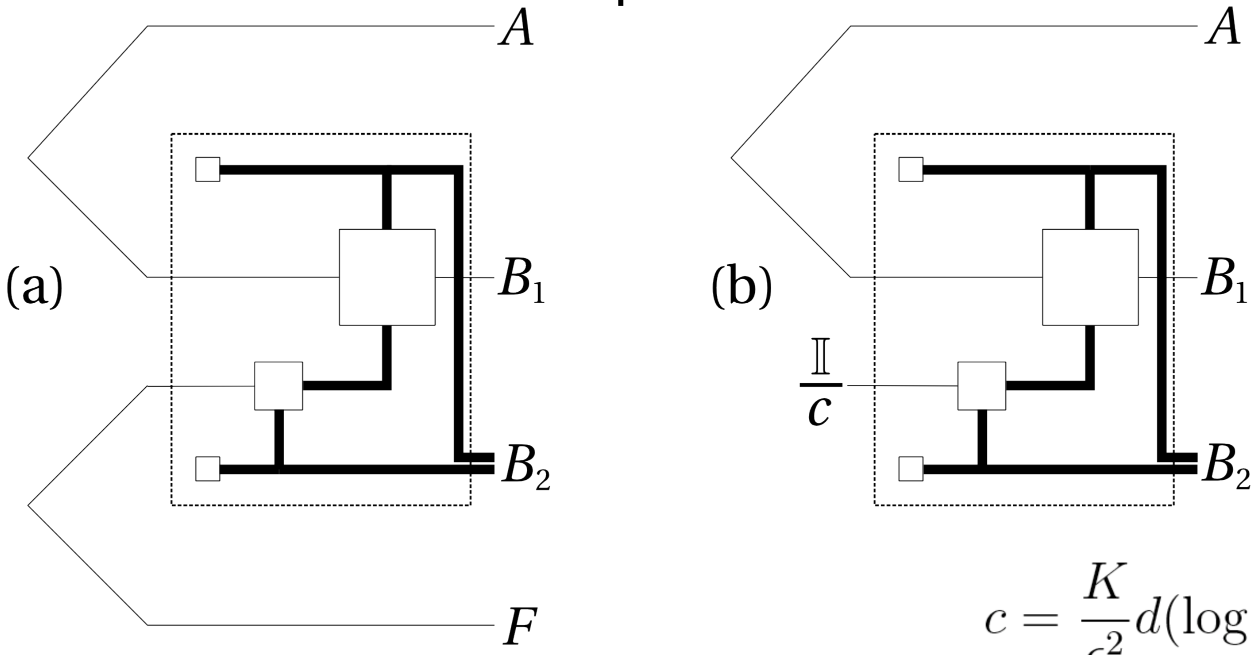
Either classical capacity is small like we want, OR there is a HUGE violation of the additivity of the Holevo quantity—We can't lose!



Capacity with 2-way classical communication is log *d*

$$\mathcal{Q} \ge I_{\text{coh}} = S(B) - S(AB)$$

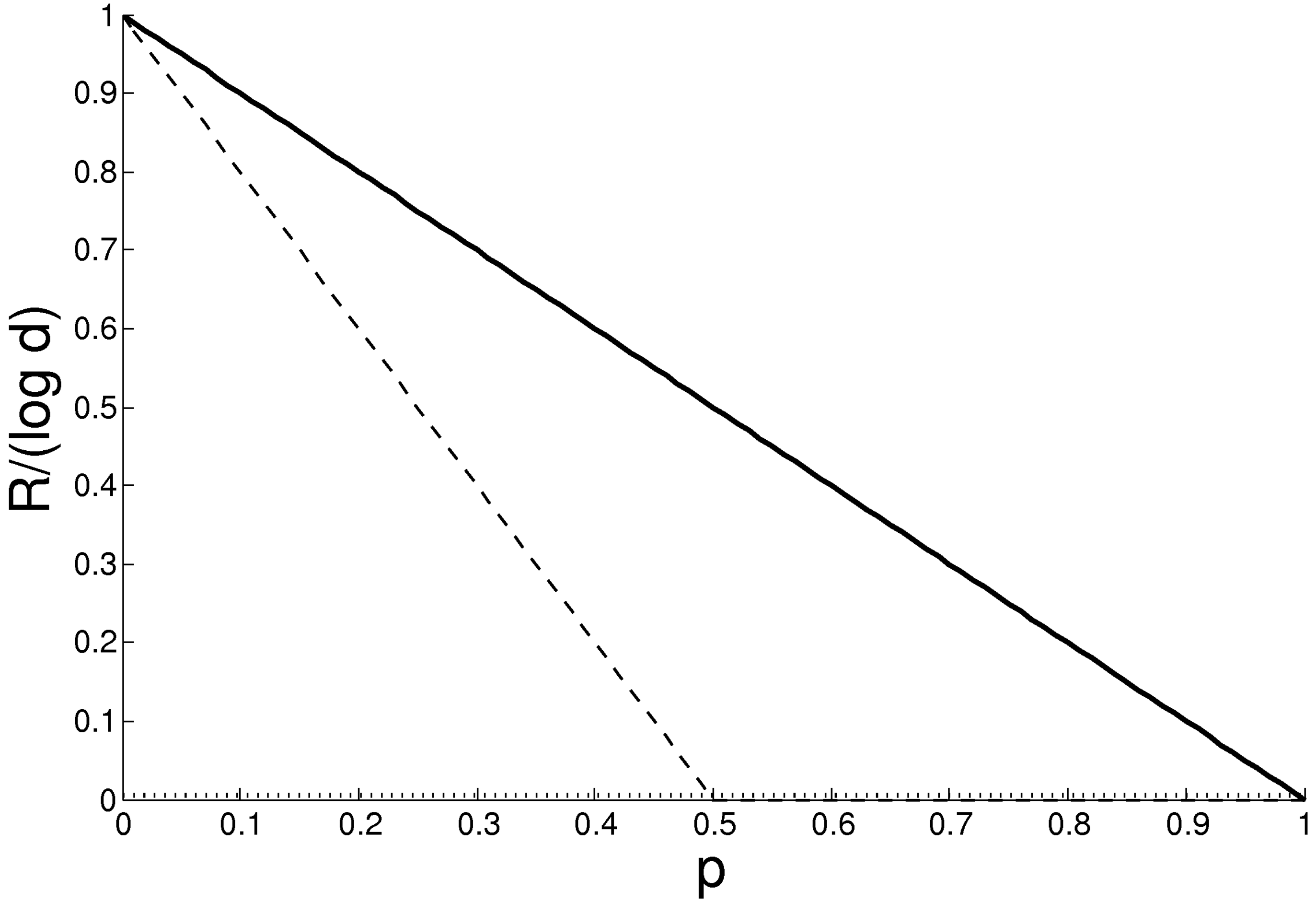
Because of the erasure flag, the coherent information breaks up into two terms



$$c = \frac{K}{\epsilon^2} d(\log d)^4$$

$$I_{\text{coh}}^{\text{not erased}} = \log d \qquad I_{\text{coh}}^{\text{erased}} \ge -4\log\log d - \log(K/\epsilon^2)$$

$$I_{\text{coh}} \ge \frac{1}{2}\log d - 2\log\log d + \frac{1}{2}\log(K/\epsilon^2)$$



R/(log d)
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
p

Recap:

$$\mathcal{Q}(\mathcal{R}_d^\epsilon) \leq \mathcal{P}(\mathcal{R}_d^\epsilon) \simeq 0$$

$$\mathcal{Q}(\mathcal{A}) = \mathcal{P}(\mathcal{A}) = 0$$

$$\mathcal{P}(\mathcal{R}_d^\epsilon \otimes \mathcal{A}) \geq \mathcal{Q}(\mathcal{R}_d^\epsilon \otimes \mathcal{A}) \geq \frac{1}{2}\log d$$

Open questions:

Remove the approximately (problem is bounds again)

Reasonable sized output dimensions (and bounds)

Remove dependence of additivity of Holevo quantity

Or could the crazy idea that the Holevo quantity is extremely nonadditive actually be true?

Something that doesn't depend on additivity of Holevo quantity

Wide separation between quantum capacity and
1-shot coherent information

$$\mathcal{T} \text{ lets you choose } \mathcal{R}_d^\epsilon \text{ or } \mathcal{A}$$

$$\mathcal{Q}^{(1)}(\mathcal{T}) \simeq 0 \text{ (either choice is useless)}$$

$$\mathcal{Q}(\mathcal{T}) \geq \tfrac{1}{2}\mathcal{Q}^{(1)}(\mathcal{T} \otimes \mathcal{T}) \geq \tfrac{1}{8}\log D_{\text{in}}$$

$$\text{compared to } 0.0025 \log D_{\text{in}} \text{ from SY08}$$