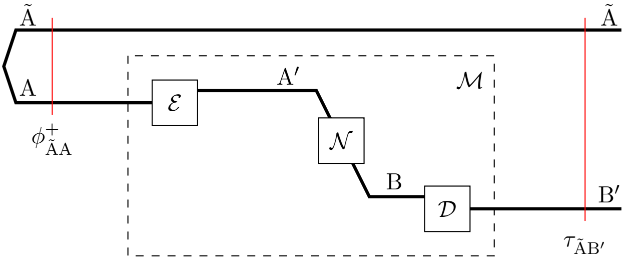
On the power on non-signalling and PPT-preserving codes

Debbie Leung (IQC - University of Waterloo)
Will Matthews (University of Cambridge)
arXiv:1406.7142

Channel coding



Size of code: $K = d_{\mathrm{A}} = d_{\mathrm{B}'}$.

Channel fidelity: $F = \mathrm{Tr}\tau_{\tilde{\mathrm{A}}\mathrm{B}'}\phi^+_{\tilde{\mathrm{A}}\mathrm{B}'} = K^{-1}\mathrm{Tr}\phi^+_{\mathrm{B}'\mathrm{A}}M_{\mathrm{B}'\mathrm{A}}$

$\phi^+_{\tilde{\mathrm{A}}\mathrm{A}} := |\phi^+\rangle\langle\phi^+|_{\tilde{\mathrm{A}}\mathrm{A}}, |\phi^+\rangle_{\tilde{\mathrm{A}}\mathrm{A}} := K^{-1/2}\sum_{0\le j<K}|j\rangle_{\tilde{\mathrm{A}}}|j\rangle_{\mathrm{A}}$

Choi operator: $L_{\mathrm{RQ}} = d_{\mathrm{Q}}\mathcal{L}_{\mathrm{R}\leftarrow\tilde{\mathrm{Q}}}\phi^+_{\tilde{\mathrm{Q}}\mathrm{Q}}, \mathcal{L}_{\mathrm{R}\leftarrow\mathrm{Q}}X_{\mathrm{Q}} = \mathrm{Tr}_{\mathrm{Q}}L_{\mathrm{RQ}}X^T_{\mathrm{Q}}$

Motivation

Basic question: How large can F be for given K and $\mathcal{N}$?

"One-shot" quantum information theory.

- Datta and Hsieh (1105.3321v2): general converse and achievability bounds for *entanglement-assisted* codes.
  - Asymptotically correct for $\mathcal{N}^{\otimes n}$, but not clear how to compute efficiently.
- Matthews and Wehner (1210.4722):
  - Related channel coding to hypothesis testing to obtain an asymptotically correct converse for entanglement-assisted codes.
  - SDP + channel symmetry $\to$ efficient computation for $\mathcal{N}^{\otimes n}$
  - Generalises (classical) results of Polyanskiy-Poor-Verdú (classical channels) and Wang and Renner (c-q channels).

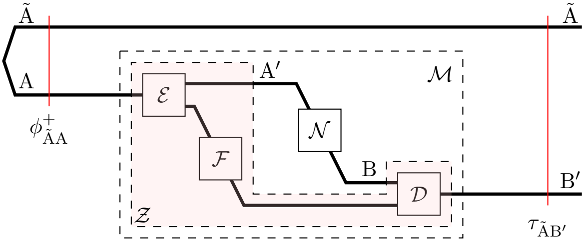
Motivation

- This work: Start with a very general class of codes and apply two 'nice' constraints obeyed by *unassisted* codes to obtain upper bounds on their channel fidelity.
- Not asymptotically correct...
- ...but efficiently computable.

Forward assisted codes

(0804.0180) Chiribella, D'Ariano, Perinotti

(quant-ph/0104027) Eggeling, Schlingemann, and Werner



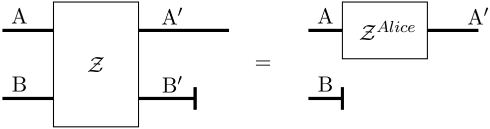
Most general form of linear map which takes operations to operations even when acting on part of a multipartite operation. The map only depends on $\mathcal{Z}_{A'B' \leftarrow AB} = \mathcal{D}_{B' \leftarrow RB} \mathcal{F}_{R \leftarrow Q} \mathcal{E}_{A'Q \leftarrow A}$, thus: $M_{B'A} = \mathrm{Tr}_{A'B} Z_{A'B'AB} N^T_{BA'}$.

$\mathcal{Z}_{A'B' \leftarrow AB}$ corresponds to a forward-assisted code (FAC) iff it is **non-signalling** from Bob to Alice.

Non-signalling quantum operations

$\mathcal{Z}_{\mathrm{A'B'}\leftarrow\mathrm{AB}}$ is **non-signalling** from Bob to Alice if

$$\mathrm{Tr}_{\mathrm{B'}}\mathcal{Z}_{\mathrm{A'B'}\leftarrow\mathrm{AB}} = \mathcal{Z}^{Alice}_{\mathrm{A'}\leftarrow\mathrm{A}}\mathrm{Tr}_{\mathrm{B}}.$$



In terms of the Choi operator for $\mathcal{Z}_{\mathrm{A'B'}\leftarrow\mathrm{AB}}$:

$$\mathrm{Tr}_{\mathrm{B'}} Z_{\mathrm{A'B'AB}} = (\mathrm{Tr}_{\mathrm{B'B}} Z_{\mathrm{A'B'AB}}/d_{\mathrm{B}}) \otimes \mathbb{1}_{\mathrm{B}}$$

Non-signalling from Alice to Bob if

$$\mathrm{Tr}_{\mathrm{A'}} Z_{\mathrm{A'B'AB}} = (\mathrm{Tr}_{\mathrm{A'A}} Z_{\mathrm{A'B'AB}}/d_{\mathrm{A}}) \otimes \mathbb{1}_{\mathrm{A}}$$

Forward assisted codes

Forward-assisted codes correspond to operators Z satisfying

$$\text{(CP): } Z_{\mathrm{A'B'AB}} \geq 0$$

$$\text{(TP): } \mathrm{Tr}_{\mathrm{A'B'}} Z_{\mathrm{A'B'AB}} = \mathbb{1}_{\mathrm{AB}}$$

$$\text{(NSBA): } \mathrm{Tr}_{\mathrm{B'}} Z_{\mathrm{A'B'AB}} = (\mathrm{Tr}_{\mathrm{B'B}} Z_{\mathrm{A'B'AB}} / d_{\mathrm{B}}) \otimes \mathbb{1}_{\mathrm{B}}$$

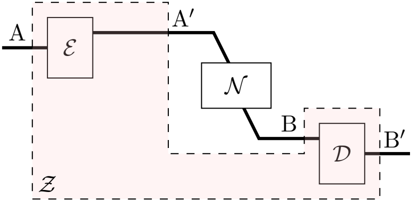
Channel fidelity of Z is

$$F = K^{-1} \mathrm{Tr} \phi_{\mathrm{B'A}} Z_{\mathrm{A'B'AB}} N^{T}_{\mathrm{BA'}}$$

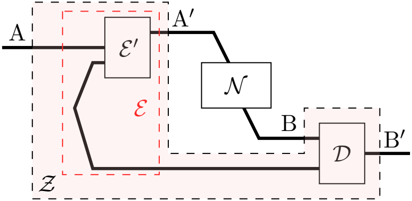
Without further constraints, can always achieve $F = 1$.

Non-signalling codes

$$\text{(NSAB): } \mathrm{Tr}_{\mathrm{A}'} Z_{\mathrm{A}'\mathrm{B}'\mathrm{AB}} = (\mathrm{Tr}_{\mathrm{A}'\mathrm{A}} Z_{\mathrm{A}'\mathrm{B}'\mathrm{AB}}/d_{\mathrm{A}}) \otimes \mathbb{1}_{\mathrm{A}}$$



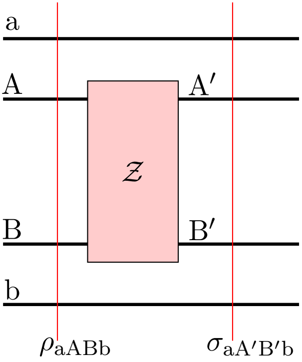
Unassisted code $(\mathbf{UA})$: $\mathcal{Z}_{\mathrm{A}'\mathrm{B}'\leftarrow\mathrm{AB}} = \mathcal{E}_{\mathrm{A}'\leftarrow\mathrm{A}}\mathcal{D}_{\mathrm{B}'\leftarrow\mathrm{B}}$
Local operations $(+$ shared randomness).



Entanglement-assisted codes $(\mathbf{EA})$: $\mathcal{Z}_{\mathrm{A}'\mathrm{B}'\leftarrow\mathrm{AB}} = \mathcal{E}'_{\mathrm{A}'\leftarrow\mathrm{Aa}}\mathcal{D}_{\mathrm{B}'\leftarrow\mathrm{Bb}}\psi_{\mathrm{ab}}$
Local operations and shared entanglement.

$$\mathbf{NS} \supseteq \mathbf{EA} \supseteq \mathbf{UA}.$$

PPT-preserving codes



Rains (quant-ph/0008047)
Transpose map $\mathbf{t}_\mathrm{Q} : |i\rangle\langle j|_\mathrm{Q} \mapsto |j\rangle\langle i|_\mathrm{Q}$.

Any separable ρ_AB has positive partial-transpose (PPT): $\mathbf{t}_\mathrm{A}\rho_\mathrm{AB} \geq 0$.

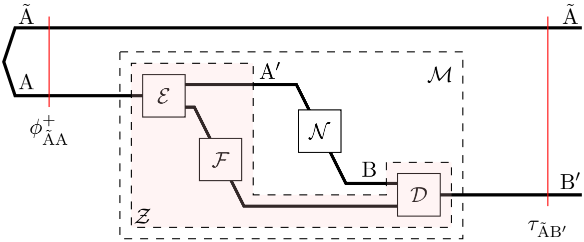
$\mathcal{Z}_{\mathrm{A'B'}\leftarrow\mathrm{AB}}$ is PPT-preserving (PPTp) iff $\mathbf{t}_\mathrm{aB}\rho_\mathrm{aABb} \geq 0. \implies \mathbf{t}_\mathrm{aB'}\sigma_\mathrm{aA'B'b}$.

For $d_\mathrm{A'} = d_\mathrm{B} = 1$: $\mathcal{Z}_{\mathrm{A'B'}\leftarrow\mathrm{AB}}$ is called *PPT-binding* or *Horodecki* channel. Zero-quantum capacity.

By a PPT-preserving code, we mean any FAC whose bipartite operation is PPT-preserving. Additional constraint: (PPTp): $\mathbf{t}_\mathrm{A'A} Z_\mathrm{A'B'AB} \geq 0$. We denote this class of codes by $\mathbf{PPTp}$

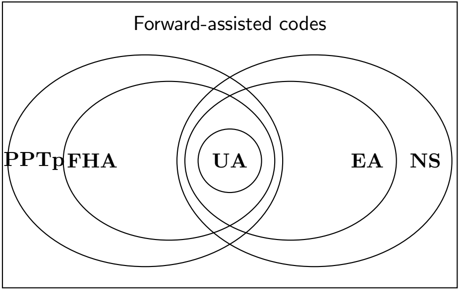
$$\mathbf{PPTp} \supseteq \mathbf{UA},\ \mathbf{PPTp} \not\supseteq \mathbf{EA}.$$

PPT-preserving codes



- We say a forward-assisted code is $\mathbf{FHA}$ if $\mathcal{F}$ is Horodecki.
- $\mathbf{FHA} \subseteq \mathbf{PPTp}$.
- Superactivation (Smith-Yard): Combination of Horodecki channel and (zero quantum capacity) 50 percent erasure channel can have positive capacity.
- Expect $\mathbf{FHA}$ capacity $>$ $\mathbf{UA}$ capacity sometimes.

Relationships between classes

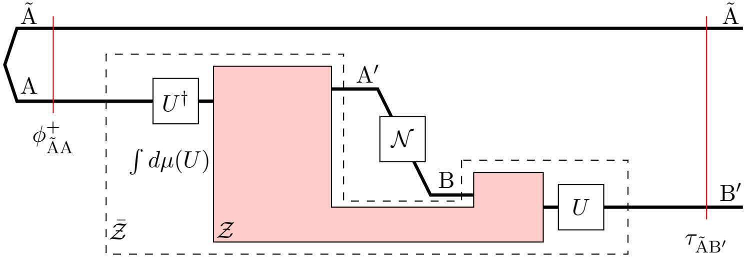


Closed under composition and convex combination.
For each class Ω we define:

$F^{\Omega}(\mathcal{N}, K) := \max K^{-1} \mathrm{Tr} \phi_{\mathrm{B'A}} Z_{\mathrm{A'B'AB}} N^{T}_{\mathrm{BA'}}$
for $d_{\mathrm{A}} = d_{\mathrm{B'}} = K$ and $Z_{\mathrm{A'B'AB}} \in \Omega$.

Capacity: $Q^{\Omega}(\mathcal{N}) := \sup\{r : \lim_{n\to\infty} F^{\Omega}(\mathcal{N}^{\otimes n}, \lfloor 2^{rn} \rfloor) = 1\}$.

Simplification of codes



$U \otimes \bar{U}|\phi^+\rangle = |\phi^+\rangle$ implies $\bar{\mathcal{Z}}_{\mathrm{A'B'}\leftarrow\mathrm{AB}}$ has same fidelity as $\mathcal{Z}_{\mathrm{A'B'}\leftarrow\mathrm{AB}}$. $\mathcal{Z}_{\mathrm{A'B'}\leftarrow\mathrm{AB}} \in \Omega \implies \bar{\mathcal{Z}}_{\mathrm{A'B'}\leftarrow\mathrm{AB}} \in \Omega$.
If μ is Haar probability measure on $\mathrm{U}(K)$:

$$\bar{Z}_{\mathrm{A'B'AB}} := \int d\mu(U) U_{\mathrm{B'}} \otimes \bar{U}_{\mathrm{A}} Z_{\mathrm{A'B'AB}} U^\dagger_{\mathrm{B'}} \otimes U^T_{\mathrm{A}},$$

$$= K(\phi^+_{\mathrm{B'A}} \otimes \Lambda_{\mathrm{A'B}} + (\mathbb{1} - \phi^+)_{\mathrm{B'A}} \otimes \Gamma_{\mathrm{A'B}}).$$

State of A' : $\rho_{\mathrm{A'}} = (\Lambda_{\mathrm{A'}} + (K^2 - 1)\Gamma_{\mathrm{A'}}) d_{\mathrm{B}}^{-1}$

Semidefinite programs

NSBA condition for $\bar{Z}$ is: $\Lambda_{\mathrm{A'B}} + (K^2 - 1)\Gamma_{\mathrm{A'B}} = \rho_{\mathrm{A'}} \otimes \mathbb{1}_{\mathrm{B}}$, with which we can eliminate $\Gamma_{\mathrm{A'B}}$ in the expression for $\bar{Z}$.
The channel fidelity simplifies to

$$F = \mathrm{Tr} N_{\mathrm{A'B}}^{\mathrm{T}} \Lambda_{\mathrm{A'B}}$$

while the constraints simplify to

$$\begin{aligned} 0 \leq \Lambda_{\mathrm{A'B}} &\leq \rho_{\mathrm{A'}} \otimes \mathbb{1}_{\mathrm{B}} \\ \rho_{\mathrm{A'}} &\geq 0, \mathrm{Tr}\rho_{\mathrm{A'}} = 1 \\ \mathbf{NS}: &\Lambda_{\mathrm{B}} = \mathbb{1}_{\mathrm{B}}/K^2 \\ \mathbf{PPTp}: &\begin{cases} \mathbf{t}_{\mathrm{B}}[\Lambda_{\mathrm{A'B}}] \geq -\rho_{\mathrm{A'}} \otimes \mathbb{1}_{\mathrm{B}}/K, \\ \mathbf{t}_{\mathrm{B}}[\Lambda_{\mathrm{A'B}}] \leq \rho_{\mathrm{A'}} \otimes \mathbb{1}_{\mathrm{B}}/K. \end{cases} \end{aligned}$$

Further simplification possible for covariant $\mathcal{N}$.

Non-signalling codes and the hypothesis-testing bound

For success probability over classical channels:

- Zero-error case: Cubitt, Leung, WM, Winter (1003.3195)
- General case: WM (1109.5417). Performance of NS codes equivalent to powerful hypothesis-testing based upper bound of Polyanskiy, Poor and Verdú.

The WM-Wehner generalisation of the PPV bound gives an SDP upper-bound for performance of entanglement-assisted codes:

$$\begin{aligned} F^{\mathbf{EA}}(\mathcal{N},K) \leq B(\mathcal{N},K) = & \max \mathrm{Tr} N^{\mathrm{T}}_{\mathrm{A'B}} \Lambda_{\mathrm{A'B}} \\ & 0 \leq \Lambda_{\mathrm{A'B}} \leq \rho_{\mathrm{A'}} \otimes \mathbb{1}_{\mathrm{B}} \\ & \rho_{\mathrm{A'}} \geq 0, \mathrm{Tr} \rho_{\mathrm{A'}} = 1 \\ & \Lambda_{\mathrm{B}} \leq \mathbb{1}_{\mathrm{B}} / K^2 \end{aligned}$$

Non-signalling codes and the hypothesis-testing bound

Our SDP for $F^{\mathbf{NS}}(\mathcal{N}, K)$ differs from $B(\mathcal{N}, K)$ only in having an *equality* in the constraint $\Lambda_{\mathrm{B}} \leq \mathbb{1}_{\mathrm{B}}/K^2$ so

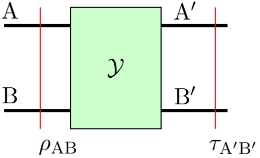
$$F^{\mathbf{EA}}(\mathcal{N}, K) \leq F^{\mathbf{NS}}(\mathcal{N}, K) \leq B(\mathcal{N}, K).$$

Does $F^{\mathbf{NS}}(\mathcal{N}, K) = B(\mathcal{N}, K)$? True for classical channels.
Since the bound B is asymptotically tight,

$$Q^{\mathbf{NS}}(\mathcal{N}_{\mathrm{B}\leftarrow\mathrm{A}'}) = Q^{\mathbf{EA}}(\mathcal{N}_{\mathrm{B}\leftarrow\mathrm{A}'}) = \frac{1}{2}\max_{\rho_{\mathrm{A}'}} I(\mathrm{R}:\mathrm{B})_{\mathcal{N}_{\mathrm{B}\leftarrow\mathrm{A}'}\rho_{\mathrm{RA}'}}$$

where $\rho_{\mathrm{RA}'}$ is a purification of $\rho_{\mathrm{A}'}$.
(Bennett, Shor, Smolin, Thapliyal - quant-ph/0106052)

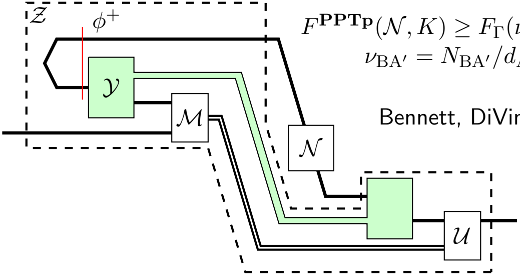
PPTp codes and entanglement distillation



$F_\Gamma(\rho_{\mathrm{AB}}, K) := \max_{\mathcal{Y}\in\mathbf{PPTp}} \mathrm{Tr}\,\phi^+_{\mathrm{A'B'}}\tau_{\mathrm{A'B'}}$, $d_{\mathrm{A'}} = d_{\mathrm{B'}} = K$

Rains quant-ph/0008047

W.l.o.g. $\mathcal{Y}$ can be taken to be NS in both directions.



$F^{\mathbf{PPTp}}(\mathcal{N}, K) \geq F_\Gamma(\nu_{\mathrm{BA'}}, K)$

$\nu_{\mathrm{BA'}} = N_{\mathrm{BA'}}/d_{\mathrm{A'}}$

Bennett, DiVincenzo, Smolin, Wootters quant-ph/9604024

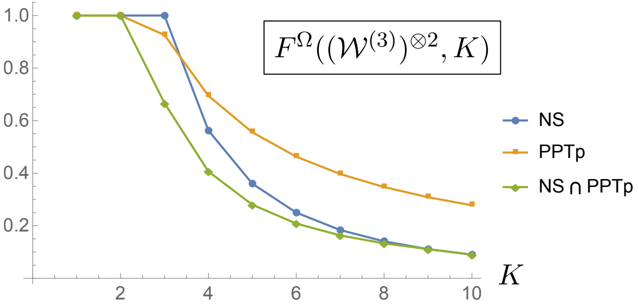
If $\mathcal{N}$ can be implemented using one copy of $\nu_{\mathrm{BA'}}$ and classical communication then $F^{\mathbf{PPTp}}(\mathcal{N}, K) = F_\Gamma(\nu_{\mathrm{BA'}}, K)$.

Werner-Holevo channels

Qutrit Werner-Holevo channel: $\mathcal{W}^{(3)} : X \mapsto \frac{1}{2}(\mathbb{1}\mathrm{Tr}X - X^{\mathrm{T}})$.

$\mathcal{W}^{(3)}$ is symmetric, therefore $Q(\mathcal{W}^{(3)}) = 0$, however...

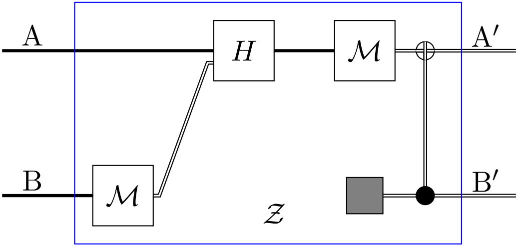
$Q^{\mathbf{PPTp}}(\mathcal{W}^{(3)}) = Q_0^{\mathbf{PPTp}}(\mathcal{W}^{(3)}) = \log\frac{5}{3}$ (using results of Rains).



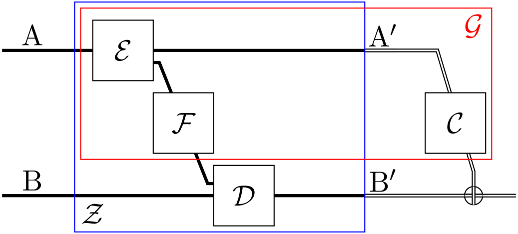
$$F^{\mathbf{NS}\cap\mathbf{PPTp}}((\mathcal{W}^{(3)})^{\otimes 2}) = 1 \implies Q_0^{\mathbf{NS}\cap\mathbf{PPTp}}(\mathcal{W}^{(3)}) \geq 1/2!$$

Can this be achieved by $\mathbf{FHA}$?

PPT-p. and NS $\not\subseteq$ **FHA**



All systems are qubits. $\mathcal{M}$ is computational basis measurement; H is (classically controlled) Hadamard.
LOCC $\implies$ PPT-preserving.
Non-signalling in both directions.

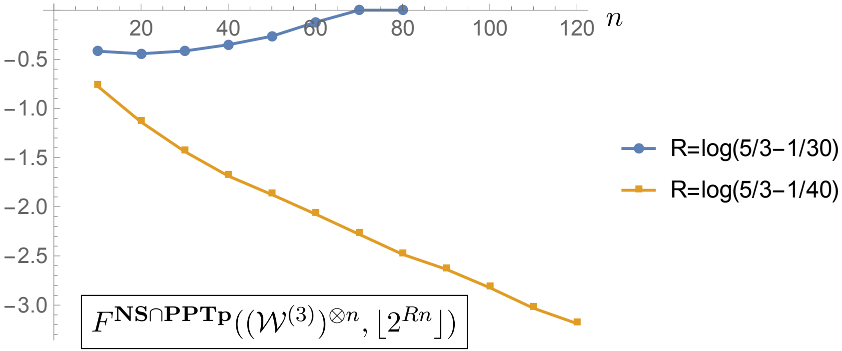


$\mathcal{G} := \mathcal{F} \otimes \mathcal{C} \circ \mathcal{E}$
$\mathrm{Tr}\mathcal{G}(|0\rangle\langle 0|)\mathcal{G}(|1\rangle\langle 1|) = 0,$
$\mathrm{Tr}\mathcal{G}(|+\rangle\langle +|)\mathcal{G}(|-\rangle\langle -|) = 0$

Cubitt and Smith (0912.2737): $\mathcal{G}$ has quantum zero-error capacity.
Therefore, so must $\mathcal{F}$.

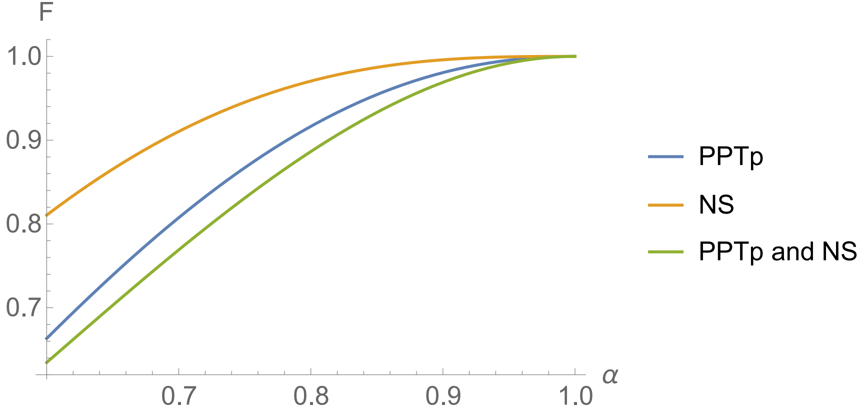
$Q^{\mathbf{NS}\cap\mathbf{PPTp}}(\mathcal{W}^{(3)}) < Q^{\mathbf{PPTp}}(\mathcal{W}^{(3)})$?

$$Q^{\mathbf{PPTp}}(\mathcal{W}^{(3)}) = Q_0^{\mathbf{PPTp}}(\mathcal{W}^{(3)}) = \log\frac{5}{3}$$



Example: Qubit depolarising channel

$$F^{\Omega}(\mathcal{D}_{\alpha}^{\otimes 5}, 2)$$



Outlook

- Investigate further constraints e.g. k-extendibility.
- What is the asymptotic capacity of PPTp / PPTp-NS codes?
- Is true zero-error superactivation possible?

Outlook

- Investigate further constraints e.g. k-extendibility.
- What is the asymptotic capacity of PPTp / PPTp-NS codes?
- Is true zero-error superactivation possible?

Thanks!