Capacity Estimates of TRO Channels

arXiv: 1509.07294 and arXiv: 1609.08594

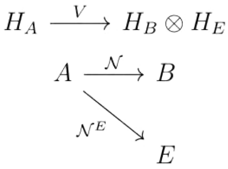
Li Gao

University of Illinois at Urbana-Champaign

QIP 2017, Microsoft Research, Seattle

Joint work with Marius Junge and Nicholas LaRacuente

Quantum capacity of a channel



Quantum channel (cptpm) $\mathcal{N} : \mathbb{B}(H_A) \to \mathbb{B}(H_B)$

- Stinespring dilation: $\mathcal{N} : \rho^A \to tr_E(V \rho^A V^\dagger)$
- Complementary channel: $\mathcal{N}^E : \rho^A \to tr_B(V \rho^A V^\dagger)$

Quantum capacity of a channel

$$H_A \xrightarrow{V} H_B \otimes H_E$$

$$A \xrightarrow{\mathcal{N}} B, \qquad A \xrightarrow{\mathcal{N}^E} E$$

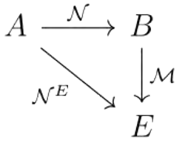
Quantum channel (cptpm) $\mathcal{N} : \mathbb{B}(H_A) \to \mathbb{B}(H_B)$

- Stinespring dilation: $\mathcal{N} : \rho^A \to tr_E(V\rho^A V^\dagger)$
- Complementary channel: $\mathcal{N}^E : \rho^A \to tr_B(V\rho^A V^\dagger)$

How many qubits per use of $\mathcal{N}$ can one transmit over it?

- Coherent information: $Q^{(1)}(\mathcal{N}) = \sup_\rho H(B)_\sigma - H(E)_\sigma$
  $\sigma^{BE} = V\rho^A V^\dagger$ and $H(B)_\sigma = -tr(\sigma^B \log \sigma^B)$.
- Quantum capacity [Lloyd-Shor-Devetak, 97]:
  $Q(\mathcal{N}) = \lim_{k\to\infty} \frac{1}{k} Q^{(1)}(\mathcal{N}^{\otimes k})$
- $\exists \mathcal{N}, Q^{(1)}(\mathcal{N}) < Q(\mathcal{N})$ [DiVincenzo-Shor-Smolin, 98]
- Regularization (the limit) is necessary but hard to compute.
- Qubit depolarizing channel $\mathcal{D}_\lambda(\rho) = (1-\lambda)\rho + \lambda\frac{1}{2}$.
  $Q(\mathcal{D}_\lambda)$ in general is open.

Degradable channels



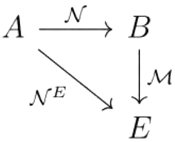
$\mathcal{N}$ is *degradable* if $\exists \mathcal{M}$ s.t. $\mathcal{N}^E = \mathcal{M} \circ \mathcal{N}$

- [Devetak-Shor, 05] shows that if $\mathcal{N}$ is degradable then

$$Q^{(1)}(\mathcal{N}) = Q(\mathcal{N})$$

- Hadamard channel are degradable. $\mathcal{N}(\rho) = \sum \langle h_i | \rho | h_j \rangle |i\rangle\langle j|$.

Degradable channels



$\mathcal{N}$ is *degradable* if $\exists \mathcal{M}$ s.t. $\mathcal{N}^E = \mathcal{M} \circ \mathcal{N}$

- [Devetak-Shor, 05] shows that if $\mathcal{N}$ is degradable then

$$Q^{(1)}(\mathcal{N}) = Q(\mathcal{N})$$

- Hadamard channel are degradable. $\mathcal{N}(\rho) = \sum \langle h_i|\rho|h_j\rangle |i\rangle\langle j|$.

Question

Other (nontrivial) channels which has $Q^{(1)}(\mathcal{N}) = Q(\mathcal{N})$?

Some general upper bounds on Q

- [Smith-Smolin-Winter, 08] Quantum capacity with symmetric side channels
- [Tomamichel-Wilde-Winter, 15] Rains relative entropy
- [Sutter et al, 15] Approximate degradable channels
- [Wang-Duan, 15] A semidefinite programming upper bound

Some general upper bounds on Q

- [Smith-Smolin-Winter, 08] Quantum capacity with symmetric side channels
- [Tomamichel-Wilde-Winter, 15] Rains relative entropy
- [Sutter et al, 15] Approximate degradable channels
- [Wang-Duan, 15] A semidefinite programming upper bound

New approach

An upper bound via analysis on Stinespring dilation.

Outline

1. Introduction

2. Main Results
   - Two examples
   - TRO channels and their modifications
   - Comparison Theorem

3. Further Applications
   - Private capacity
   - Superadditivity
   - Strong converse rates

Example I

Let G be a finite group and $\{|g\rangle|\ g \in G\}$ be an orthonormal basis. Denote by $\lambda(g)$ the unitary $\lambda(g)|h\rangle = |gh\rangle$. For a probability distribution f on G,

$$\mathcal{N}_f(\rho) = \sum_g f(g)\lambda(g)\rho\lambda(g)^* \ .$$

Example I

Let G be a finite group and $\{|g\rangle |\ g \in G\}$ be an orthonormal basis. Denote by $\lambda(g)$ the unitary $\lambda(g)|h\rangle = |gh\rangle$. For a probability distribution f on G,

$$\mathcal{N}_f(\rho) = \sum_g f(g)\lambda(g)\rho\lambda(g)^* \ .$$

$$\max\{\log|G| - H(f), Q(\mathcal{N}_1)\} \leq Q(\mathcal{N}_f) \leq Q(\mathcal{N}_1) + \log|G| - H(f) \ .$$

Example I

Let G be a finite group and $\{|g\rangle | \ g \in G\}$ be an orthonormal basis. Denote by $\lambda(g)$ the unitary $\lambda(g)|h\rangle = |gh\rangle$. For a probability distribution f on G,

$$\mathcal{N}_f(\rho) = \sum_g f(g)\lambda(g)\rho\lambda(g)^* \ .$$

$$\max\{\log|G| - H(f), Q(\mathcal{N}_1)\} \leq Q(\mathcal{N}_f) \leq Q(\mathcal{N}_1) + \log|G| - H(f) \ .$$

- Not degradable if G is not commutative.
- $Q(\mathcal{N}_1) =$ logarithm of the largest degree of G's irreducible representations.

Example II

Let $-1 \leq \alpha \leq 1$.

$$\mathcal{N}_\alpha(\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}) = \begin{bmatrix} a_{11} + a_{22} & \alpha a_{13} & \alpha a_{24} \\ \alpha a_{31} & a_{33} & 0 \\ \alpha a_{42} & 0 & a_{44} \end{bmatrix} .$$

$$Q^{(1)}(\mathcal{N}_\alpha) = Q(\mathcal{N}_\alpha) = 1 - h(\frac{1+\alpha}{2}) \, ,$$

where $h(p) = -p \log p - (1-p) \log(1-p)$ is the binary entropy function.

Example II

Let $-1 \leq \alpha \leq 1$.

$$\mathcal{N}_\alpha(\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}) = \begin{bmatrix} a_{11} + a_{22} & \alpha a_{13} & \alpha a_{24} \\ \alpha a_{31} & a_{33} & 0 \\ \alpha a_{42} & 0 & a_{44} \end{bmatrix} .$$

$$Q^{(1)}(\mathcal{N}_\alpha) = Q(\mathcal{N}_\alpha) = 1 - h(\frac{1+\alpha}{2}) ,$$

where $h(p) = -p \log p - (1-p) \log(1-p)$ is the binary entropy function.

- Not degradable because the first 2×2 block goes to the environment.

Stinespring space

$\mathcal{N}(\rho^A) = tr_E(V\rho^A V^*)$ with $V : H_A \to H_E \otimes H_B$.

Definition

The *Stinespring space* of $\mathcal{N}$ is defined as $X^{\mathcal{N}} = VH_A \subset H_B \otimes H_E$.

- $X^{\mathcal{N}} \cong H_A$ as Hilbert space,.
- $\mathcal{N}$ is determined by $X^{\mathcal{N}} \subset H_B \otimes H_E$ (up to a unitary equivalence).

Stinespring space

$\mathcal{N}(\rho^A) = tr_E(V\rho^A V^*)$ with $V : H_A \to H_E \otimes H_B$.

Definition

The *Stinespring space* of $\mathcal{N}$ is defined as $X^{\mathcal{N}} = VH_A \subset H_B \otimes H_E$.

- $X^{\mathcal{N}} \cong H_A$ as Hilbert space,.
- $\mathcal{N}$ is determined by $X^{\mathcal{N}} \subset H_B \otimes H_E$ (up to a unitary equivalence).

Via $H_B \otimes H_E \cong \mathbb{B}(H_E, H_B)$,

$$|x\rangle \in H_A \leftrightarrow V|x\rangle \in X^{\mathcal{N}} \leftrightarrow x \in \mathbb{B}(H_E, H_B)$$

$$\mathcal{N}(|x\rangle\langle y|) = xy^\dagger \ , \ \mathcal{N}^E(|x\rangle\langle y|) = y^\dagger x \ .$$

Stinespring space (cont'd)

Let $M_{n,m}$ be $n \times n$ complex matrices and $M_n = M_{n,n}$.

a) $\mathcal{N} = id : M_n \to M_n$, $X = M_{n,1}$. $\mathcal{N} = tr : M_n \to \mathbb{C}$, $X = M_{1,n}$

Stinespring space (cont'd)

Let $M_{n,m}$ be $n \times n$ complex matrices and $M_n = M_{n,n}$.

a) $\mathcal{N} = id : M_n \to M_n$, $X = M_{n,1}$. $\mathcal{N} = tr : M_n \to \mathbb{C}$, $X = M_{1,n}$

b) $\mathcal{N} = id_n \otimes tr_m : M_n \otimes M_m \to M_n$, $X = M_{n,m}$

Stinespring space (cont'd)

Let $M_{n,m}$ be $n \times n$ complex matrices and $M_n = M_{n,n}$.

a) $\mathcal{N} = id : M_n \to M_n$, $X = M_{n,1}$. $\mathcal{N} = tr : M_n \to \mathbb{C}$, $X = M_{1,n}$

b) $\mathcal{N} = id_n \otimes tr_m : M_n \otimes M_m \to M_n$, $X = M_{n,m}$

c) Let $\mathcal{N} = \oplus_k id_{n_k} \otimes tr_{m_k}$ be a direct sum of partial traces i.e.

$$\mathcal{N}(\begin{bmatrix} \rho_{11} & \cdots & \rho_{1k} \\ \vdots & \ddots & \vdots \\ \rho_{k1} & \cdots & \rho_{kk} \end{bmatrix}) = \begin{bmatrix} id_{n_1} \otimes tr_{m_1}(\rho_{11}) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & id_{n_k} \otimes tr_{m_k}(\rho_{kk}) \end{bmatrix},$$

$$\text{then } X = \oplus M_{n_k,m_k} = \begin{bmatrix} \ddots & & \\ & M_{n_k,m_k} & \\ & & \ddots \end{bmatrix}.$$

Stinespring space (cont'd)

Let $M_{n,m}$ be $n \times n$ complex matrices and $M_n = M_{n,n}$.

a) $\mathcal{N} = id : M_n \to M_n$, $X = M_{n,1}$. $\mathcal{N} = tr : M_n \to \mathbb{C}$, $X = M_{1,n}$

b) $\mathcal{N} = id_n \otimes tr_m : M_n \otimes M_m \to M_n$, $X = M_{n,m}$

c) Let $\mathcal{N} = \oplus_k id_{n_k} \otimes tr_{m_k}$ be a direct sum of partial traces i.e.

$$\mathcal{N}(\begin{bmatrix} \rho_{11} & \cdots & \rho_{1k} \\ \vdots & \ddots & \vdots \\ \rho_{k1} & \cdots & \rho_{kk} \end{bmatrix}) = \begin{bmatrix} id_{n_1} \otimes tr_{m_1}(\rho_{11}) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & id_{n_k} \otimes tr_{m_k}(\rho_{kk}) \end{bmatrix},$$

$$\text{then } X = \oplus M_{n_k,m_k} = \begin{bmatrix} \ddots & & \\ & M_{n_k,m_k} & \\ & & \ddots \end{bmatrix}.$$

This is the so-called *conditional expectation*. By [Fukuda-Wolf, 07]

$$Q^{(1)}(\mathcal{N}) = Q(\mathcal{N}) = \log \max_k n_k \ .$$

Ternary ring of operators (TRO)

- $X \cong \oplus_k (M_{n_k,m_k} \otimes \mathbb{C}1_{l_k})$ is a (finite dimensional) *ternary ring of operators*.

Ternary ring of operators (TRO)

- $X \cong \oplus_k (M_{n_k,m_k} \otimes \mathbb{C}1_{l_k})$ is a (finite dimensional) *ternary ring of operators*.

Definition [Hestenes, 79]

A *ternary ring of operators* (TRO) X is a closed subspace of $\mathbb{B}(H, K)$ such that

$$x, y, z \in X \Rightarrow xy^\dagger z \in X \ .$$

Ternary ring of operators (TRO)

- $X \cong \oplus_k (M_{n_k,m_k} \otimes \mathbb{C}1_{l_k})$ is a (finite dimensional) *ternary ring of operators*.

Definition [Hestenes, 79]

A *ternary ring of operators* (TRO) X is a closed subspace of $\mathbb{B}(H,K)$ such that

$$x, y, z \in X \Rightarrow xy^\dagger z \in X \ .$$

We call $\mathcal{N}$ a *TRO channel* if $X^{\mathcal{N}}$ is a TRO.

- If $X^{\mathcal{N}} \cong \oplus_k M_{n_k,m_k}$, then $\mathcal{N} \cong \oplus_k (id_{n_k} \otimes tr_{m_k})$.

Modification of TRO channels

Modification by matrix multiplication:

$$\begin{array}{ccccc} H_A & & X^{\mathcal{N}} & & \mathbb{B}(H_E, H_B) \\ |x\rangle & \xrightarrow{V} & x & \longrightarrow & x \cdot a \end{array}$$

Question. When this gives a channel? "$x \to x \cdot a$" an isometry?

Modification of TRO channels

Modification by matrix multiplication:

$$\begin{array}{ccccc} H_A & & X^{\mathcal{N}} & & \mathbb{B}(H_E, H_B) \\ |x\rangle & \xrightarrow{V} & x & \longrightarrow & x \cdot a \end{array}$$

Question. When this gives a channel? "$x \to x \cdot a$" an isometry?

- The normalized trace $\tau(\rho) = \frac{1}{n} tr(\rho)$ on M_n.
- A positive $f \in M_n$ is a normalized density if $\tau(f) = 1$.

Definition

Two $*$-subalgebra $\mathcal{A}, \mathcal{B} \subset M_n$ are *independent* if

$$\tau(xy) = \tau(x)\tau(y), x \in \mathcal{A}, y \in \mathcal{B} .$$

An element $f \in M_n$ is independent of $\mathcal{A}$ if the C^*-algebra generated by f (the closure of all polynomials of f and $f^\dagger$) is independent of $\mathcal{A}$.

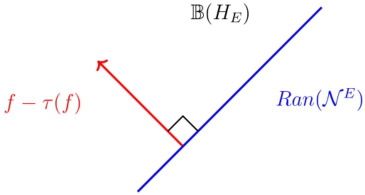
Answer. When $f = aa^\dagger$ is a normalized density independent of $Ran(\mathcal{N}^E)$.

Modification of TRO channels (cont'd)

Let $\mathcal{N}$ be a TRO channel $\mathcal{N}(|x\rangle\langle y|) = xy^\dagger$ and $f \in \mathbb{B}(H_E)$ be a normalized density independent of $Ran(\mathcal{N}^E)$. Then the map

$$\mathcal{N}_f(|x\rangle\langle y|) = x \cdot f \cdot y^\dagger$$

is again a channel (cptp).



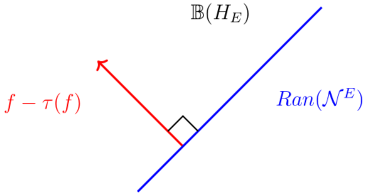
Modification of TRO channels (cont'd)

Let $\mathcal{N}$ be a TRO channel $\mathcal{N}(|x\rangle\langle y|) = xy^\dagger$ and $f \in \mathbb{B}(H_E)$ be a normalized density independent of $Ran(\mathcal{N}^E)$. Then the map

$$\mathcal{N}_f(|x\rangle\langle y|) = x \cdot f \cdot y^\dagger$$

is again a channel (cptp).

- $\mathcal{N}_1 = \mathcal{N}$.
- $\mathcal{N}_f$ is a lifting of $\mathcal{N}$, i.e. $\mathcal{E} \circ \mathcal{N}_f = \mathcal{N}$ where $\mathcal{E}$ is the conditional expectation from $\mathbb{B}(H_B)$ onto $Ran(\mathcal{N})$.



Comparison Theorem (main technical result)

Let $1 < p \leq \infty$ and $\frac{1}{p} + \frac{1}{p'} = 1$. Recall $\| f \|_{\tau,p} = \tau(|f|^p)^{\frac{1}{p}}$.

Theorem

Let $\mathcal{N} : B(H_A) \to B(H_B)$ be a TRO channel and f a normalized density independent of $Ran(\mathcal{N}^E)$. For any positive $\rho \in \mathbb{B}(H_A)$ and $\sigma \in Ran(\mathcal{N})$,

$$D_p(\mathcal{N}(\rho)||\sigma) \leq D_p(\mathcal{N}_f(\rho)||\sigma) \leq D_p(\mathcal{N}(\rho)||\sigma) + p' \log \| f \|_{\tau,p}$$

Sandwiched Renyi-p divergence:

$$D_p(\rho||\sigma) = \begin{cases} p' \log \| \sigma^{-\frac{1}{2p'}} \rho \sigma^{-\frac{1}{2p'}} \|_p & \text{if } \operatorname{supp}(\rho) \subset \operatorname{supp}(\sigma) \\ +\infty & \text{else} \end{cases}$$

Sandwiched Rényi-p divergence D_p

$\| \rho \|_p = tr(|\rho|^p)^{\frac{1}{p}}$. For $\rho, \sigma \geq 0$,

$$D_p(\rho||\sigma) = \begin{cases} p' \log \| \sigma^{-\frac{1}{2p'}} \rho \sigma^{-\frac{1}{2p'}} \|_p & \text{if } \operatorname{supp}(\rho) \subset \operatorname{supp}(\sigma) \\ +\infty & \text{else} \end{cases}$$

- $\lim_{p \to 1} D_p(\rho||\sigma) = D(\rho||\sigma) := tr(\rho(\log \rho - \log \sigma))$
- Data processing inequality: $D_p(\rho||\sigma) \geq D_p(\mathcal{N}(\rho)||\mathcal{N}(\sigma))$. (will be used)

Sandwiched Rényi-p divergence D_p

$\|\rho\|_p = tr(|\rho|^p)^{\frac{1}{p}}$. For $\rho, \sigma \geq 0$,

$$D_p(\rho||\sigma) = \begin{cases} p' \log \|\sigma^{-\frac{1}{2p'}} \rho \sigma^{-\frac{1}{2p'}}\|_p & \text{if } \operatorname{supp}(\rho) \subset \operatorname{supp}(\sigma) \\ +\infty & \text{else} \end{cases}$$

- $\lim_{p\to 1} D_p(\rho||\sigma) = D(\rho||\sigma) := tr(\rho(\log\rho - \log\sigma))$
- Data processing inequality: $D_p(\rho||\sigma) \geq D_p(\mathcal{N}(\rho)||\mathcal{N}(\sigma))$. (will be used)

- Coherent information: $Q^{(1)}(\mathcal{N}) = \sup_{\rho\in S(AA')} I_c(A'\rangle B)_\sigma$, where $\sigma^{A'B} = id_{A'} \otimes \mathcal{N}(\rho^{AA'})$ and

$$I_c(A\rangle B)_\rho = H(B) - H(AB) = D(\rho^{AB}||1\otimes\rho^B) = \inf_{\sigma^B} D(\rho^{AB}||1\otimes\rho^B).$$

Capacity bounds

Corollary

$$Q(\mathcal{N}) \leq Q(\mathcal{N}_f) \leq Q(\mathcal{N}) + \tau(f \log f)$$

In particular, $Q(\mathcal{N}) = \log \max_k n_k$ *if* $X^{\mathcal{N}} = \oplus_k (M_{n_k, m_k})$.

Capacity bounds

Corollary

$$Q(\mathcal{N}) \leq Q(\mathcal{N}_f) \leq Q(\mathcal{N}) + \tau(f \log f)$$

In particular, $Q(\mathcal{N}) = \log \max_k n_k$ *if* $X^{\mathcal{N}} = \oplus_k (M_{n_k,m_k})$.

Proof.

- Apply the comparison to $(id \otimes \mathcal{N}_f) = (id \otimes \mathcal{N})_f$,

$$D_p(\mathcal{N}(\rho^{AA'})||\sigma) \leq D_p(\mathcal{N}_f(\rho^{AA'})||\sigma) \leq D_p(\mathcal{N}(\rho^{AA'})||\sigma) + p' \log \| f \|_{\tau,p}$$

- Take limit $p \to 1$, choose $\sigma = 1 \otimes \mathcal{N}(\rho^A)$ and then take supremum over all bipartite states $\rho^{AA'}$.

$$Q^{(1)}(\mathcal{N}) \leq Q^{(1)}(\mathcal{N}_f) \leq Q^{(1)}(\mathcal{N}) + \tau(f \log f)$$

- Regularization: $(\mathcal{N}_f)^{\otimes k} = (\mathcal{N}^{\otimes k})_{f^{\otimes k}}$, $\tau(f^{\otimes k} \log f^{\otimes k}) = k\tau(f \log f)$.

Proof of Comparison Theorem

- The lower bound follows from data processing inequality. $\mathcal{E} \circ \mathcal{N}_f = \mathcal{N}$

$$\Rightarrow D_p(\mathcal{N}_f(\rho)||\sigma) \geq D_p(\mathcal{E} \circ \mathcal{N}_f(\rho)||\mathcal{E}(\sigma)) = D_p(\mathcal{N}(\rho)||\sigma) \ .$$

Proof of Comparison Theorem

- The lower bound follows from data processing inequality. $\mathcal{E}\circ\mathcal{N}_f=\mathcal{N}$

$$\Rightarrow D_p(\mathcal{N}_f(\rho)||\sigma)\geq D_p(\mathcal{E}\circ\mathcal{N}_f(\rho)||\mathcal{E}(\sigma))=D_p(\mathcal{N}(\rho)||\sigma)\ .$$

- Upper bound via complex interpolation.
  - Consider the right matrix multiplication: $x\to x\cdot a$
  - Complex interpolation (Stein's theorem).
    $\|xa\|_\infty\leq\|x\|_\infty\|a\|_\infty,\ \|xa\|_2=\|x\|_2\|a\|_{2,\tau}$ (independence).

$$\Rightarrow\|xa\|_{2p}\leq\|x\|_{2p}\|a\|_{2p,\tau}\ .$$

  - Let $\rho=\eta\eta^\dagger$ and $f=aa^\dagger$. Then $\|f\|_p=\|a\|_{2p}^2$ and

$$\|\sigma^{-\frac{1}{2p'}}\mathcal{N}_f(\rho)\sigma^{-\frac{1}{2p'}}\|_p=\|\sigma^{-\frac{1}{2p'}}\eta a\|_{2p}^2$$

$$\leq\|\sigma^{-\frac{1}{2p'}}\eta\|_{2p}^2\|a\|_{2p,\tau}^2=\|\sigma^{-\frac{1}{2p'}}\mathcal{N}(\rho)\sigma^{-\frac{1}{2p'}}\|_p\|f\|_{\tau,p}$$

Capacity bounds

Corollary

$$Q(\mathcal{N}) \leq Q(\mathcal{N}_f) \leq Q(\mathcal{N}) + \tau(f \log f)$$

In particular, if $X^{\mathcal{N}} = \oplus_k (M_{n_k,m_k})$, $Q(\mathcal{N}) = \log \max_k n_k$.

Remarks.

- Entropy with respect to τ:

$$\lim_{p \to 1} p' \log \| f \|_p = \tau(f \log f) = \log |E| - H(\frac{1}{|E|} f)$$

.

- "Local" comparison: for any subspace $A_0 \subset A$,

$$Q(\mathcal{N}|_{A_0}) \leq Q(\mathcal{N}_f|_{A_0}) \leq Q(\mathcal{N}|_{A_0}) + \tau(f \log f) \ .$$

Outline

1. Introduction
2. Main Results
   - Two examples
   - TRO channels and their modifications
   - Comparison Theorem
3. Further Applications
   - Private capacity
   - Superadditivity
   - Strong converse rates

Classical private capacity of a channel

The private capacity of $\mathcal{N}$ is

$$P(\mathcal{N}) = \lim_k \frac{1}{k} P^{(1)}(\mathcal{N}^{\otimes k}) \ , \ P^{(1)}(\mathcal{N}) = \sup_{\rho^{XA}} I(X{:}B)_\sigma - I(X{:}E)_\sigma \ ,$$

where $I(A{:}B) = H(A) + H(B) - H(AB)$, and
$\sigma^{XBE} = \sum_x p(x)|x\rangle\langle x| \otimes V\rho_x^A V^\dagger$.

Classical private capacity of a channel

The private capacity of $\mathcal{N}$ is

$$P(\mathcal{N}) = \lim_k \frac{1}{k} P^{(1)}(\mathcal{N}^{\otimes k}) \ , \ P^{(1)}(\mathcal{N}) = \sup_{\rho^{XA}} I(X{:}B)_\sigma - I(X{:}E)_\sigma \ ,$$

where $I(A{:}B) = H(A) + H(B) - H(AB)$, and
$\sigma^{XBE} = \sum_x p(x)|x\rangle\langle x| \otimes V\rho_x^A V^\dagger$.

- $P^{(1)}(\mathcal{N}) < P(\mathcal{N})$ possible [Smith-Renes-Smolin, 08]
- $Q^{(1)}(\mathcal{N}) \leq P^{(1)}(\mathcal{N})$ and $Q(\mathcal{N}) \leq P(\mathcal{N})$ (1 ebit $\Rightarrow$ 1 kbit).
- For degradable channels, $Q^{(1)}(\mathcal{N}) = Q(\mathcal{N}) = P^{(1)}(\mathcal{N}) = P(\mathcal{N})$. [Smolin, 08]

Corollary

$Q(\mathcal{N}) = P(\mathcal{N}) \leq P(\mathcal{N}_f) \leq P(\mathcal{N}) + \tau(f \log f) = Q(\mathcal{N}) + \tau(f \log f)$

Superadditivity

- [Winter-Yang, 16] introduced the potential capacities

$$Q^{(p)}(\mathcal{N}) = \sup_{\mathcal{M}} Q^{(1)}(\mathcal{N} \otimes \mathcal{M}) - Q^{(1)}(\mathcal{M}),$$

$$P^{(p)}(\mathcal{N}) = \sup_{\mathcal{M}} P^{(1)}(\mathcal{N} \otimes \mathcal{M}) - P^{(1)}(\mathcal{M}) \ .$$

- $\mathcal{N}$ is *strongly additive* for $Q^{(1)}$ (resp. $P^{(1)}$) iff $Q^{(p)}(\mathcal{N}) = Q^{(1)}(\mathcal{N})$ (resp. $P^{(p)}(\mathcal{N}) = P^{(1)}(\mathcal{N})$).

Superadditivity

- [Winter-Yang, 16] introduced the potential capacities

$$Q^{(p)}(\mathcal{N}) = \sup_{\mathcal{M}} Q^{(1)}(\mathcal{N} \otimes \mathcal{M}) - Q^{(1)}(\mathcal{M}),$$

$$P^{(p)}(\mathcal{N}) = \sup_{\mathcal{M}} P^{(1)}(\mathcal{N} \otimes \mathcal{M}) - P^{(1)}(\mathcal{M}) \, .$$

- $\mathcal{N}$ is *strongly additive* for $Q^{(1)}$ (resp. $P^{(1)}$) iff $Q^{(p)}(\mathcal{N}) = Q^{(1)}(\mathcal{N})$ (resp. $P^{(p)}(\mathcal{N}) = P^{(1)}(\mathcal{N})$).

Corollary

$$Q(\mathcal{N}) = Q^{(p)}(\mathcal{N}) \le Q^{(p)}(\mathcal{N}_f) \le P^{(p)}(\mathcal{N}_f) \le P^{(p)}(\mathcal{N}) + \tau(f \log f) = Q(\mathcal{N}) + \tau(f \log f)$$

- Observe that $\mathcal{N}_f \otimes \mathcal{M} = (\mathcal{N} \otimes \mathcal{M})_{f \otimes 1}$.

Strong converse rates

Let $P^\dagger$ (resp. $Q^\dagger$) denote the smallest strong converse rate for private (resp. quantum) communication.

- [Wilde-Tomamichel-Berta, 16] shows that for any channel

$$P^\dagger(\mathcal{N}) \le E_R(\mathcal{N}),$$

where E_R the relative entropy of entanglement

$$E_R(\mathcal{N}) = \sup_\rho E_R(id \otimes \mathcal{N}(\rho)) \, , E_R(\rho^{AB}) = \inf_{\sigma \in S(A:B)} D(\rho||\sigma) \, .$$

Strong converse rates

Let $P^\dagger$ (resp. $Q^\dagger$) denote the smallest strong converse rate for private (resp. quantum) communication.

- [Wilde-Tomamichel-Berta, 16] shows that for any channel

$$P^\dagger(\mathcal{N}) \le E_R(\mathcal{N}),$$

where E_R the relative entropy of entanglement

$$E_R(\mathcal{N}) = \sup_\rho E_R(id \otimes \mathcal{N}(\rho)) \, , E_R(\rho^{AB}) = \inf_{\sigma \in S(A:B)} D(\rho || \sigma) \, .$$

Corollary

$E_R(\mathcal{N}_f) \le E_R(\mathcal{N}) + \tau(f \log f)$, $E_R(\mathcal{N}) = Q(\mathcal{N})$ *and in particular*

$$Q(\mathcal{N}) \le Q^\dagger(\mathcal{N}_f) \le P^\dagger(\mathcal{N}_f) \le Q(\mathcal{N}) + \tau(f \log f)$$

Final Example

Write $\rho = \begin{bmatrix} \rho_{11} & \cdots & \rho_{14} \\ \vdots & \ddots & \vdots \\ \rho_{41} & \cdots & \rho_{44} \end{bmatrix}$ with ρ_{jk} being 4×4 matrices.

$$\mathcal{N}_f(\rho) = \sum_{1 \le j,k \le 4} tr(\rho_{jk} f_{jk}) |j\rangle\langle k|$$

where $f = \begin{bmatrix} 1 & \alpha_3 Z \otimes Z & -i\alpha_2 Y \otimes Y & \alpha_1 X \otimes X \\ \alpha_3 Z \otimes Z & 1 & \alpha_1 X \otimes X & -i\alpha_2 Y \otimes Y \\ i\alpha_2 Y \otimes Y & \alpha_1 X \otimes X & 1 & -\alpha_3 Z \otimes Z \\ \alpha_1 X \otimes X & i\alpha_2 Y \otimes Y & -\alpha_3 Z \otimes Z & 1 \end{bmatrix}$.

X, Y, Z Pauli matrices.

Final Example

Write $\rho = \begin{bmatrix} \rho_{11} & \cdots & \rho_{14} \\ \vdots & \ddots & \vdots \\ \rho_{41} & \cdots & \rho_{44} \end{bmatrix}$ with ρ_{jk} being 4×4 matrices.

$$\mathcal{N}_f(\rho) = \sum_{1 \le j,k \le 4} tr(\rho_{jk} f_{jk}) |j\rangle\langle k|$$

where $f = \begin{bmatrix} 1 & \alpha_3 Z \otimes Z & -i\alpha_2 Y \otimes Y & \alpha_1 X \otimes X \\ \alpha_3 Z \otimes Z & 1 & \alpha_1 X \otimes X & -i\alpha_2 Y \otimes Y \\ i\alpha_2 Y \otimes Y & \alpha_1 X \otimes X & 1 & -\alpha_3 Z \otimes Z \\ \alpha_1 X \otimes X & i\alpha_2 Y \otimes Y & -\alpha_3 Z \otimes Z & 1 \end{bmatrix}$.

X, Y, Z Pauli matrices.

$$\begin{aligned} Q^{(1)}(\mathcal{N}_f) = P^{(1)}(\mathcal{N}_f) = Q^{\dagger}(\mathcal{N}_f) = P^{\dagger}(\mathcal{N}_f) \\ = Q^{(p)}(\mathcal{N}_f) = P^{(p)}(\mathcal{N}_f) = 1 - h(\frac{1 + |\alpha|}{2}) . \end{aligned}$$

where $|\alpha| = \sqrt{|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2} \le 1$ (Bloch sphere).

Summary

- TRO channels are orthogonal sums of partial traces.
- Using analysis on Stinespring space, we give capacities estimates on modifications of TRO channels.
- Examples wit nonzero capacity that is strongly additive, has strong converse but not degradable.

Summary

- TRO channels are orthogonal sums of partial traces.
- Using analysis on Stinespring space, we give capacities estimates on modifications of TRO channels.
- Examples wit nonzero capacity that is strongly additive, has strong converse but not degradable.

Thanks!

Marius Junge

Nicholas LaRacuente