Title: The quantum and private capacities of quantum channels, and the solution in the low-noise regime

Date: Oct 04, 2017 04:00 PM

URL: http://pirsa.org/17100071

Abstract: We first summarize background on the quantum capacity of a quantum channel, and explain why we know very little about this fundamental quantity, even for the qubit depolarizing channel (the quantum analogue of the binary symmetric channel) despite 20 years of effort by the community.

Then, we focus on low-noise quantum channels, and present recent results on the quantum capacity to leading order in the noise parameter. This in particular solves the quantum capacity problem (to leading order) for the qubit depolarizing channel, and provides a structure theorem for the capacity achieving codes. For low-noise channels, degenerate codes provide negligible superadditivity effect.

Analoguous results on the private capacity will be presented. Our results imply that for low-noise channels, there is negligible difference between coherence and privacy, and a key rate approaching the capacity can already be obtained using classical error correction and privacy amplification.

Joint work with Felix Leditzky and Graeme Smith

The quantum channel capacity problems, and the solution in the low-noise regime.

arXiv:1705.04335

Debbie Leung[1]

Joint work with Felix Leditzky and Graeme Smith[2]

Perimeter Institute, Oct 04, 2017

1: Dept CO & IQC, University of Waterloo, $NSERC, CIFAR, IC$

2: JILA, University of Colorado, Boulder

The quantum channel capacity problems, and the solution in the low-noise regime.

arXiv:1705.04335

Debbie Leung[1]

Joint work with Felix Leditzky and Graeme Smith[2]

Perimeter Institute, Oct 04, 2017

1: Dept CO & IQC, University of Waterloo, $NSERC, CIFAR, IC$

2: JILA, University of Colorado, Boulder

Punchline

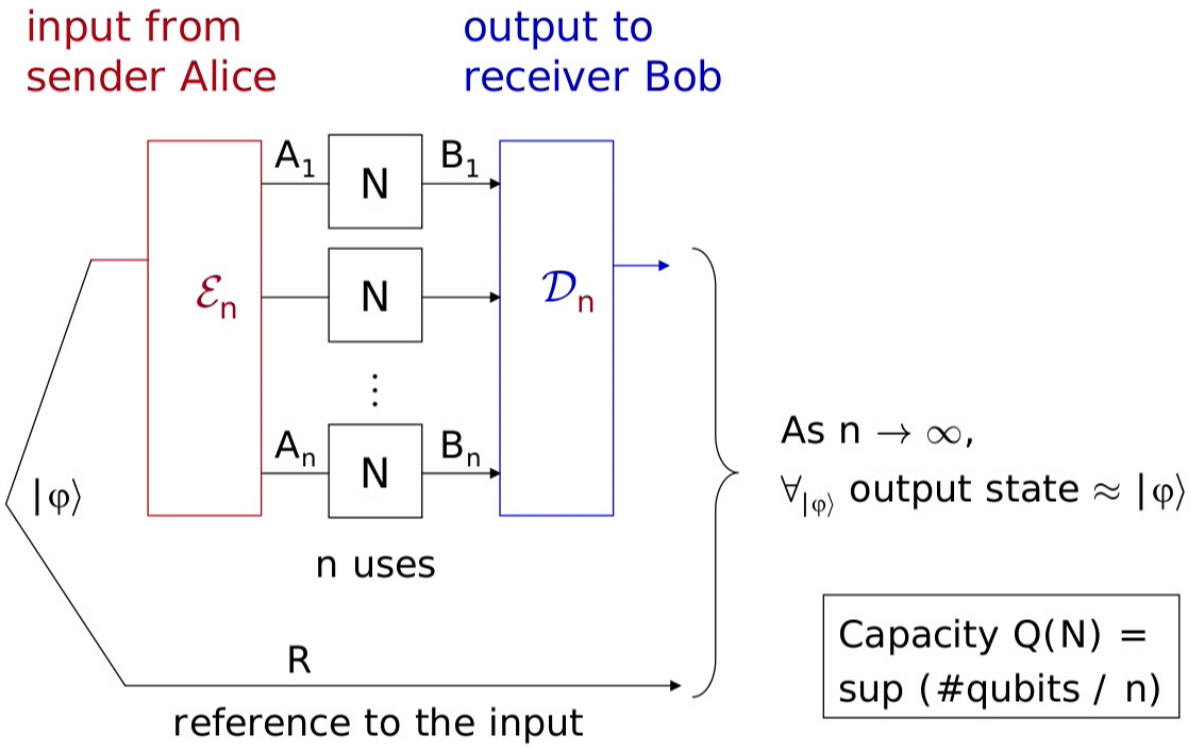
Capacities of quantum channels are fun but complicated.

But everything is simple in the low noise regime.

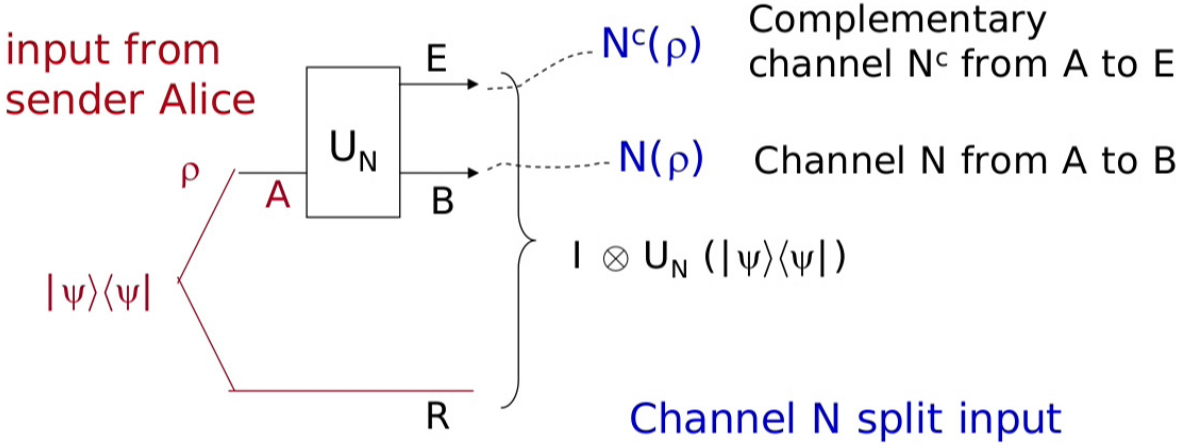
Outline

* Background
    - Quantum channel & capacities
* The quantum don't-knows
    - Superadditivity, superactivity, $Q \neq P$
* The quantum knows
    - Degradable channels, continuity, approx degradability
* Application to low noise channels
* Consequences

Quantum data & quantum channel (DMC)



Useful concepts and notations

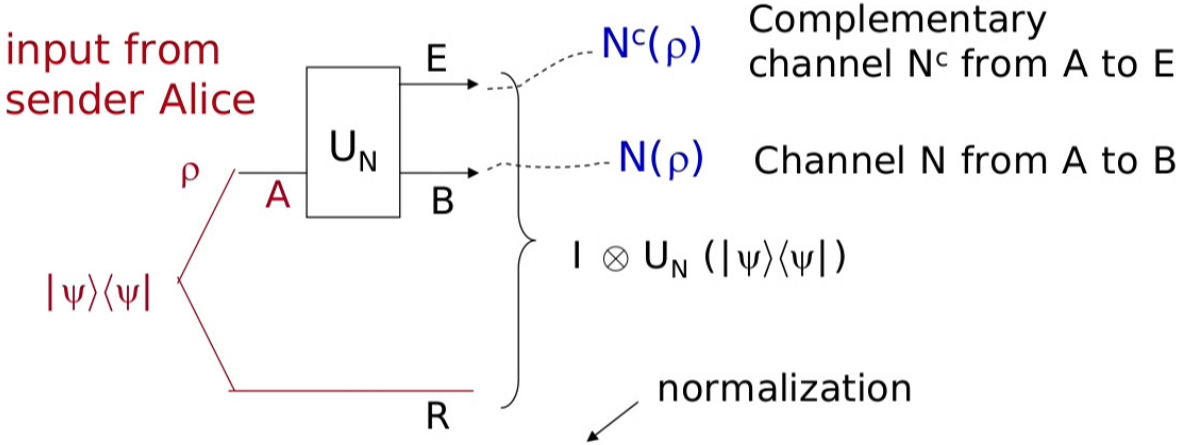


Complementary channel N^c from A to E

Channel N from A to B

Channel N split input between receiver Bob and environment E

The Lloyd-Shor-Devetak theorem



normalization

$$Q(N) \geq Q^{(1)}(N) := \max_{|\psi\rangle} \tfrac{1}{2} [I(R:B) - I(R:E)]$$

1-shot coherent info of N

S(R)+S(B)-S(BR)
S(·): von Neuman entropy of reduced state of ·

info leaked to the env

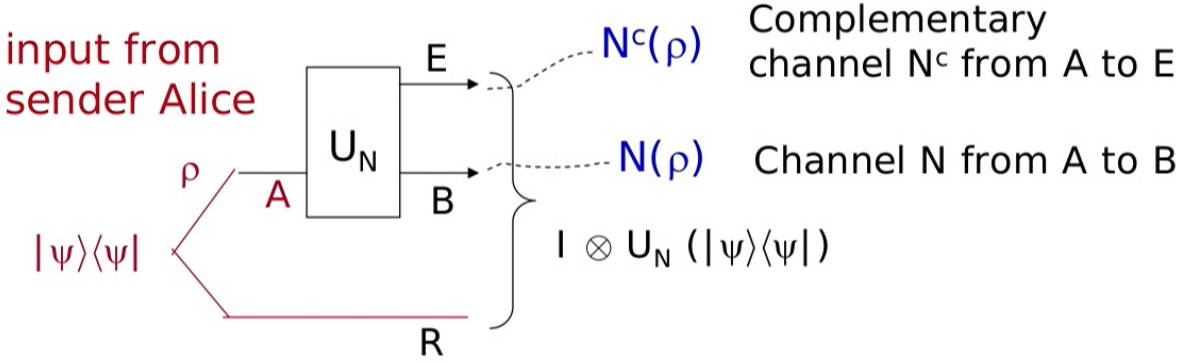
The quantum don't-knows

1. $\exists$ N s.t. $Q^{(1)}(N^{\otimes r}) > r$, $Q^{(1)}(N)$

2. $\exists$ N s.t. $Q^{(1)}(N^{\otimes r}) > 0$, $Q^{(1)}(N) = 0$

* $\sup_n$ needed
* no algorithm to determine if $Q(N) = 0$
* even simple channels exhibit superadditivity

The LSD theorem



$$Q(N) \geq Q^{(1)}(N) := \max_{|\psi\rangle} \tfrac{1}{2} [I(R:B) - I(R:E)]$$

$$Q(N) \geq Q^{(1)}(N^{\otimes n}) / n$$

$$Q(N) \leq \sup_n Q^{(1)}(N^{\otimes n}) / n$$ (Schmacher & Westmoreland)

The quantum don't-knows

1. $\exists$ N s.t. $Q^{(1)}(N^{\otimes r}) > r$, $Q^{(1)}(N)$

2. $\exists$ N s.t. $Q^{(1)}(N^{\otimes r}) > 0$, $Q^{(1)}(N) = 0$

DiVincenzo-Shor-Smolin 97:

"2." holds for r = 5 and some qubit depolarizing channel.

$$N_p(\rho) = (1\text{-}p)\ \rho + p/3\ X\ \rho\ X + p/3\ Y\ \rho\ Y + p/3\ Z\ \rho\ Z$$

$$= (1\text{-}\eta)\ \rho + \eta\ I/2 \qquad (\eta = 4p/3, \text{ quantum BSC})$$

$Q^{(1)}(N_p) = 0$ for $p \geq 0.1894$, but $Q^{(1)}(N_p^{\otimes r}) > 0$ for $p \leq 0.1904$.

The quantum don't-knows

1. $\exists$ N s.t. $Q^{(1)}(N^{\otimes r}) > r$, $Q^{(1)}(N)$

2. $\exists$ N s.t. $Q^{(1)}(N^{\otimes r}) > 0$, $Q^{(1)}(N) = 0$

DiVincenzo-Shor-Smolin 97:

"2." holds for r = 5 and some qubit depolarizing channel.

$$N_p(\rho) = (1\text{-}p)\ \rho + p/3\ X\ \rho\ X + p/3\ Y\ \rho\ Y + p/3\ Z\ \rho\ Z$$

$$= (1\text{-}\eta)\ \rho + \eta\ I/2 \qquad (\eta = 4p/3, \text{ quantum BSC})$$

$Q^{(1)}(N_p) = 0$ for $p \geq 0.1894$, but $Q^{(1)}(N_p^{\otimes r}) > 0$ for $p \leq 0.1904$.

Still known after 20 years:

What is $Q(N_p)$ for $0 \leq p \leq ¼$? Is $Q(N_p) = 0$ for $p \in [0.1904, 0.25]$?

The quantum don't-knows

1. $\exists$ N s.t. $Q^{(1)}(N^{\otimes r}) > r$, $Q^{(1)}(N)$

2. $\exists$ N s.t. $Q^{(1)}(N^{\otimes r}) > 0$, $Q^{(1)}(N) = 0$

DiVincenzo-Shor-Smolin 97:

"2." holds for r = 5 and some qubit depolarizing channel.

$$N_p(\rho) = (1\text{-}p)\ \rho + p/3\ X\ \rho\ X + p/3\ Y\ \rho\ Y + p/3\ Z\ \rho\ Z$$

$$= (1\text{-}\eta)\ \rho + \eta\ I/2 \qquad (\eta = 4p/3, \text{ quantum BSC})$$

$Q^{(1)}(N_p) = 0$ for $p \geq 0.1894$, but $Q^{(1)}(N_p^{\otimes r}) > 0$ for $p \leq 0.1904$.

The quantum don't-knows

1. $\exists$ N s.t. $Q^{(1)}(N^{\otimes r}) > r$, $Q^{(1)}(N)$

2. $\exists$ N s.t. $Q^{(1)}(N^{\otimes r}) > 0$, $Q^{(1)}(N) = 0$

DiVincenzo-Shor-Smolin 97:

$Q^{(1)}(N_p) := \max_{|\psi\rangle} \frac{1}{2} [I(R:B) - I(R:E)] = 0$

$Q^{(1)}(N_p^{\otimes 5}) \geq \frac{1}{2} [I(R:B_1 \cdots B_5) - I(R:E_1 \cdots E_5)] > 0$

A completely non-classical effect:

Encode one qubit into 5 using a degenerate code whose entanglement makes different errors act identically on the code space, and heavily suppresses $I(R:E_1 \cdots E_5)$ while not so heavily suppresses $I(R:B_1 \cdots B_5)$.

NB. More recent results have r = 2, and simple channels.

The quantum don't-knows

1. $\exists$ N s.t. $Q^{(1)}(N^{\otimes r}) > r$, $Q^{(1)}(N)$

2. $\exists$ N s.t. $Q^{(1)}(N^{\otimes r}) > 0$, $Q^{(1)}(N) = 0$

3. $\forall$ r, $\exists$ N $Q^{(1)}(N^{\otimes r}) = 0$ but $Q(N) > 0$.

Cubitt, Elkouss, Matthews, Ozols, Peres-Garcia, Strelchuk 14

We do not know whether
the problem "determine $Q(N) = 0$ or > 0"
is decidable or not.

The quantum don't-knows

4. $\exists\ N_1, N_2$ s.t. $Q(N_1) = Q(N_2) = 0$, $Q^{(1)}(N_1 \otimes N_2) > 0$

Superactivation of quantum capacity. Smith and Yard, 2009.

4'. $\exists\ N_1, N_2$ s.t. $Q(N_1) = 0$, $Q(N_2) \leq 2$, $Q^{(1)}(N_1 \otimes N_2) \approx \frac{1}{2} \log d_{in}$

Extensive non-additivity of Q. Smith and Smolin, 2009.

The quantum don't-knows

5. $\exists$ N s.t. Q(N) = 0, P(N) > 0

where P(N) = private capacity of N (best rate of classical data transmission that is unknown to the DMC environment)

Karol, Michal, and Pawel Horodecki + Oppenheim 2003

5'. $\exists$ N s.t. Q(N) $\leq$ 1, P(N) = log d_{in}

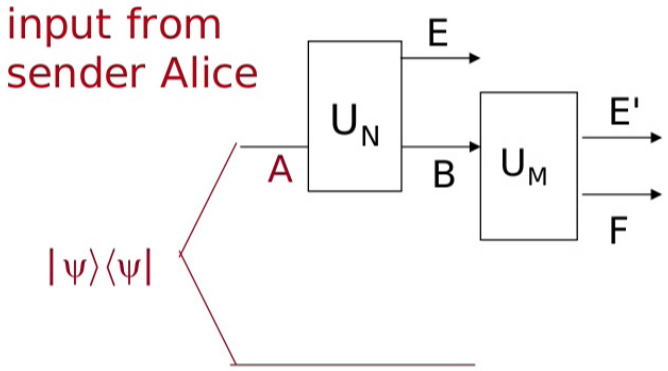
Privacy without coherence. Leung, Li, Smith and Smolin, 2014.

The little we know …

Degradable channels

Definition.

N is degradable if ∃ another channel M s.t. $N^c = M \circ N$.



Degradable means:

$\forall\, |\psi\rangle$ final state is invariant under swapping E and E'

The little we know ...

Capacities for degradable channels

Theorem [Devetak-Shor 04]

If N is degradable then $Q(N) = Q^{(1)}(N)$.

Proof (a few slides later).

The little we know …

Continuity for channel capacities

Theorem [L, Smith 09]

If $|| N - M ||_\diamond \leq \varepsilon$,

then $| Q(N) - Q(M) | \leq 8\, \varepsilon \log |B| + 4\, h(\varepsilon) \approx -4\, \varepsilon \log \varepsilon$

where $h(x) = -x \log x - (1-x) \log (1-x)$

(binary entropy function)

$$|| N-M ||_\diamond = \max_{|\psi\rangle} || I \otimes (N-M) (|\psi\rangle\langle\psi|) ||_1$$

(diamond norm distance, best bias to discriminate N from M)

An idea that doesn't work well enough ...

Continuity bound from degradable channels:

For any N, $Q(N) \approx Q^{(1)}(M) + 8\,\varepsilon \log |B| + 4\,h(\varepsilon)$

for any degradable M with $|| N\text{-}M ||_\diamond \leq \varepsilon$

Correct, but ...

* Hard to minimize ε.
* $8\,\varepsilon \log |B| + 4\,h(\varepsilon) \approx -4\,\varepsilon \log \varepsilon$ which vanishes with ε, but slope infinite at $\varepsilon = 0$.
* For low noise channels, upper bound is trivial, as the obvious M is the identity channel & $Q^{(1)}(M)$ trivially big.

The little we know …

A nice twist

Definition [approx degradable channel, Sutter et al 14]

N is η-degradable if $\exists$ channel M s.t. $||N^c - M \circ N||_\diamond \leq \eta$.

The little we know …

A nice twist

Definition [approx degradable channel, Sutter et al 14]
N is η-degradable if $\exists$ channel M s.t. $||N^c - M \circ N||_\diamond \leq \eta$.

When $\eta = 0$, N is degradable.

Extend the Devetak-Shor proof for degradable channel having $Q(N) = Q^{(1)}(N)$ via a continuity argument.

The little
we know …

A nice twist

Definition [approx degradable channel, Sutter et al 14]
N is η-degradable if $\exists$ channel M s.t. $||N^c - M \circ N||_\diamond \leq \eta$.

Theorem [Sutter, Scholz, Winter, Renner 14]
If N is η-degradable,
then $| Q(N) - Q^{(1)}(N) | \leq -\eta \log \eta + O(\eta)$

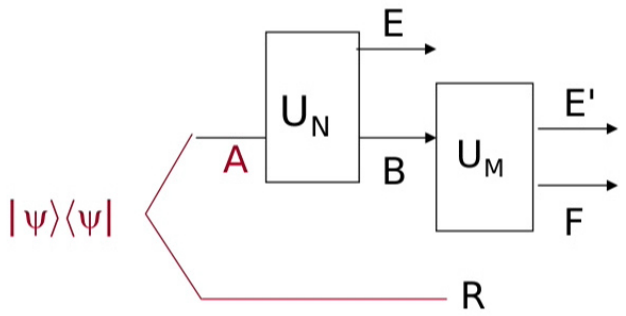
Advantage:
- M and η can be numerically minimized as an SDP

Remaining problem:
- the gap is still $O(-\eta \log \eta)$ which has infinite slope wrt η

The Devetak-Shor-Sutter-et-al proof

The little we know …

Consider any input, any channel N followed by channel M:



$\frac{1}{2}\,[I(R:B) - I(R:E)]$ ← $Q^{(1)}$ is the max of this

$= S(B) - S(E)$ (by expanding the mutual info)

$= S(E'F) - S(E)$ (unitary does not change evals)

$= \underbrace{S(E'F) - S(E')}_{S(F|E')} + \underbrace{S(E') - S(E)}_{\approx S(E)}$

$= S(F|E') + h(\eta/2) + O(\eta)$ if N η-degradable, $S(E')\approx S(E)$

subadditive

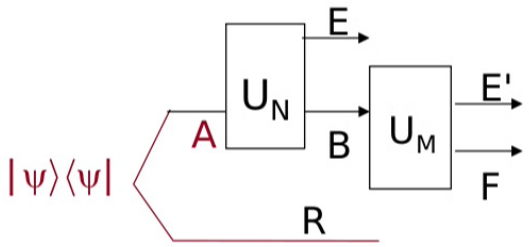
hope: similarly controllable for n-uses of N

The Devetak-Shor-Sutter-et-al proof

The little we know …

For any channel N:

$\frac{1}{2}\,[I(R:B) - I(R:E)]$
$= S(F|E') + S(E') - S(E)$



For $N^{\otimes n}$: (still just one R)

$\frac{1}{2}\,[I(R:B_1\cdots B_n) - I(R:E_1\cdots E_n)]$
$= S(F_1\cdots F_n|E_1'\cdots E_n') + S(E_1'\cdots E_n') - S(E_1\cdots S_n)$
$\leq \sum_{i=1}^{n} S(F_i|E_i') + S(E_1'\cdots E_n') - S(E_1\cdots S_n)$

$\leq -O(n\,\eta\,\log\,\eta)$

by continity argument applied to N^c and $M\circ N$ if N is η degradable

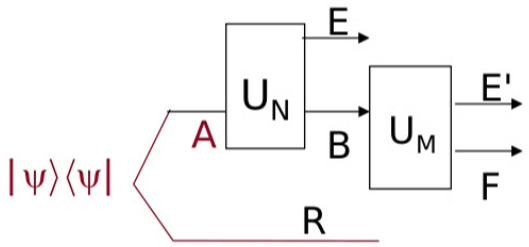
(as in LS09, or tighter results in Sutter et al)

The Devetak-Shor-Sutter-et-al proof

The little we know …

For any channel N:

$\frac{1}{2}\,[I(R:B) - I(R:E)]$
$= S(F|E') + S(E') - S(E)$



For $N^{\otimes n}$: (still just one R)

$\frac{1}{2}\,[I(R:B_1\cdots B_n) - I(R:E_1\cdots E_n)]$
$= S(F_1\cdots F_n|E_1'\cdots E_n') + S(E_1'\cdots E_n') - S(E_1\cdots S_n)$
$\leq \sum_{i=1}^{n} S(F_i|E_i') + S(E_1'\cdots E_n') - S(E_1\cdots S_n)$

$\leq -O(n\,\eta\,\log\,\eta)$

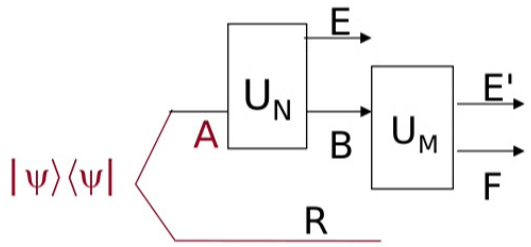
$\leq Q^{(1)}(N_i) + O(\eta\,\log\,\eta)$
from 2 slides ago

The Devetak-Shor-Sutter-et-al proof

The little we know …

For any channel N:

$\frac{1}{2}\,[I(R:B) - I(R:E)]$
$= S(F|E') + S(E') - S(E)$



For $N^{\otimes n}$: (still just one R)

$\frac{1}{2}\,[I(R:B_1\cdots B_n) - I(R:E_1\cdots E_n)]$
$= S(F_1\cdots F_n|E_1'\cdots E_n') + S(E_1'\cdots E_n') - S(E_1\cdots S_n)$
$\leq \sum_{i=1}^{n} S(F_i|E_i') + S(E_1'\cdots E_n') - S(E_1\cdots S_n)$
$\leq n\,[\,Q^{(1)}(N) + O(\eta \log \eta)\,]$

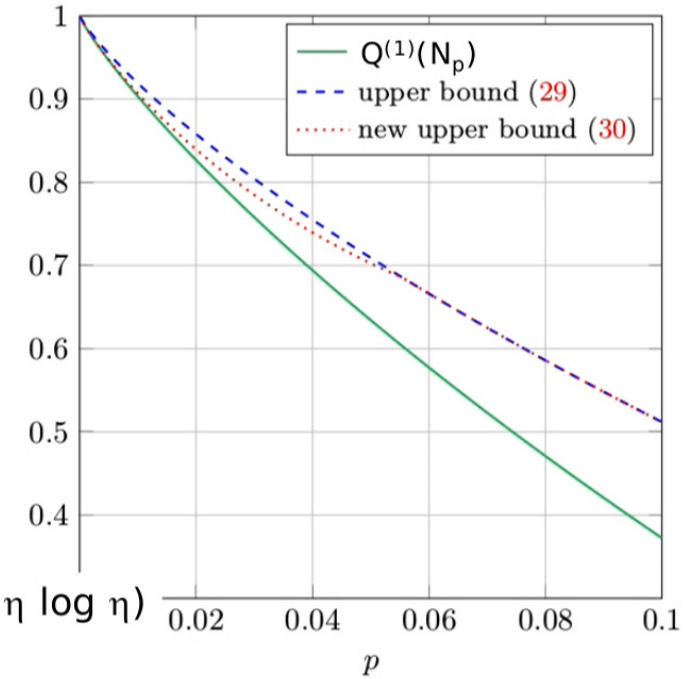
$Q(N) = \sup_{n\to\infty} 1/n \max_{|\psi\rangle} \frac{1}{2}\,[I(R:B_1\cdots B_n) - I(R:E_1\cdots E_n)]$
$\leq Q^{(1)}(N) + O(\eta \log \eta)$

After Sutter's talk in July 2015, I asked about the implications for the depolarizing channel N_p, and he shared the following (arXiv replacement) and the data.

The new upper bound on $Q(N_p)$ is very close to $Q^{(1)}(N_p)$ but insuff data to determine if $|Q(N_p)-Q^{(1)}(N_p)|$ is sublinear in p or not ...

Earlier this year, Felix got convincing data $|Q(N_p)-Q^{(1)}(N_p)| \sim O(p^2)$.

$\leq O(-\eta \log \eta)$



Qn: is $\eta \sim O(p^2)$?

How to prove it? What M_p degrades N_p so well?

Theorem: Let $a = 8/3$.

$$|| N_p{}^c - N_{p+ap^2}{}^c \circ N_p ||_\diamond \leq 8/9\ (6+\sqrt{2})\ p^2 + O(p^3)$$

Theorem: Let a = 8/3.

$$|| \, N_p{}^c - N_{p+ap^2}{}^c \circ N_p \, ||_\diamond \leq \underbrace{8/9 \; (6+\sqrt{2}) \; p^2 + O(p^3)}$$

take this η, plug it in
Sutter et al upper bound

Theorem:

$$1 - h(p) - p \log 3 \; \leq \; Q(\, N_p \,)$$
$$\leq \underbrace{1 - h(p) - p \log 3} - \frac{16}{9}(6 + \sqrt{2})\, p^2 \log p + O(p^2)$$

$Q^{(1)}(N_p)$

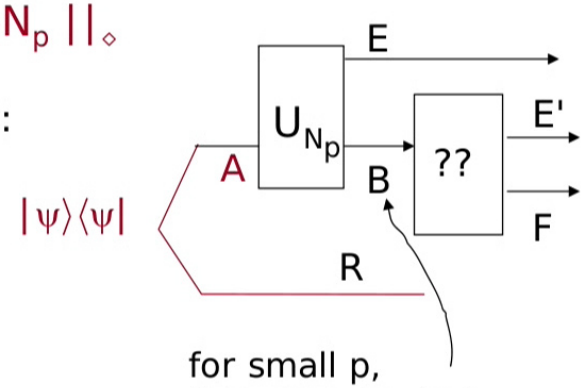
Theorem: Let a = 8/3.

$$|| N_p^c - N_{p+ap^2}^c \circ N_p ||_\diamond \leq 8/9\ (6+\sqrt{2})\ p^2 + O(p^3)$$

Why $N_{p+ap^2}^c$ is a good degrading map:

To min η =
$||N_p^c - M \circ N_p||_\diamond$

Second try:



for small p,
B is close to, but
slightly worse than
the input from A !!

Theorem: Let a = 8/3.

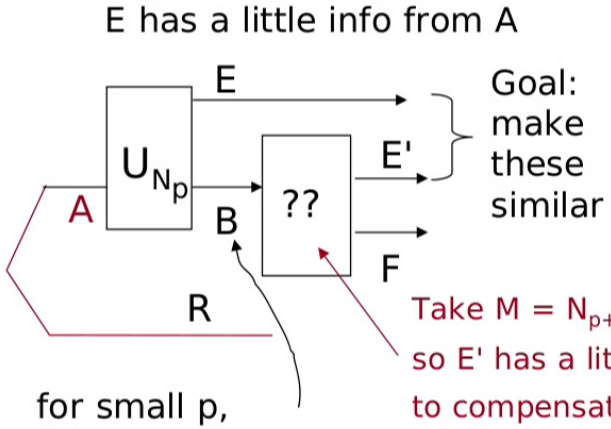
$$|| N_p^c - N_{p+ap^2}^c \circ N_p ||_\diamond \leq 8/9\ (6+\sqrt{2})\ p^2 + O(p^3)$$

Why $N_{p+ap^2}^c$ is a good degrading map:

To min η = $||N_p^c - M \circ N_p||_\diamond$

Second try:

$|\psi\rangle\langle\psi|$



for small p, B is close to, but slightly worse than the input from A !!

Take $M = N_{p+ap^2}^c$ for a>0 so E' has a little more of B, to compensate for the fact that B is a "slightly lesser" version of A. Adjust a, and see what's optimal ...

Extensions:

Similar results hold for the Pauli channel:

$$N(\rho) = (1-p_0)\,\rho + p_1\, X\,\rho\, X + p_2\, Y\,\rho\, Y + p_3\, Z\,\rho\, Z$$

There are more features in N^c to model, but we have more parameters in the degrading map to play with ..

Similar results hold for higher dimensional Pauli channels

Similar headache, and similar results hold for the private classical capacity of these channels. Some of these channels in the low-noise regime are crucial for quantum key distribution.

Theorem: If $|| N - I ||_\diamond \leq \varepsilon$, then $||N^c - N^c \circ N||_\diamond \leq 2\ \varepsilon^{1.5}$

Theorem:

For low noise channels, with $||\mathcal{N} - I||_\diamond \leq \epsilon$,

$$Q(\mathcal{N}) = Q^{(1)}(\mathcal{N}) + O(\epsilon^{1.5} \log \epsilon)$$

$$P(\mathcal{N}) = Q^{(1)}(\mathcal{N}) + O(\epsilon^{1.5} \log \epsilon)$$

Outline

* Background

  Quantum channel & capacities

* The quantum don't-knows

  Superadditivity, superactivity, $Q \neq P$

* The quantum knows

  Degradable channels, continuity, approx degradability

  Low noise channels

* Consequences – no point to work too hard to optimize various communication tasks for low-noise channels

Outline

* Background

  Quantum channel & capacities

* The quantum don't-knows

  Superadditivity, superactivity, $Q \neq P$

* The quantum knows

  Degradable channels, continuity, approx degradability

  Low noise channels

* Consequences – no point to work too hard to optimize various communication tasks for low-noise channels