The little
we know …

Degradable channels

Definition.

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

The little
we know …

Degradable channels

Definition.

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

Capacities for degradable channels

Theorem [Devetak-Shor 04]

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

The little
we know …

Degradable channels

Definition.

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

Capacities for degradable channels

Theorem [Devetak-Shor 04]

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

Idea: ½ [I(R:B) – I(R:E)]   (max of this gives $Q^{(1)}$)

= subadditive quantity + S(E') – S(E)   0 if N deg

where E' = output of $M \circ N$ for any M.

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

Use continuity bounds for capacities [L, Smith 09].

e.g., $Q(N) \approx Q(N') + (-)\ 4\ \varepsilon \log \varepsilon$

$= Q^{(1)}(N') + (-)\ 4\ \varepsilon \log \varepsilon$

for any M degradable, $\| N - N' \|_{\diamond} \leq \varepsilon$.

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

Use continuity bounds for capacities [L, Smith 09] :

e.g., $Q(N) \approx Q(N') + (-)\ 4\ \varepsilon \log \varepsilon$

$= Q^{(1)}(N') + (-)\ 4\ \varepsilon \log \varepsilon$

for any M degradable, $\| N - N' \|_{\diamond} \leq \varepsilon$.

Hard to minimize

The little
we know …

A nice twist [Sutter, Scholz, Winter, Renner 14]

Definition [approx degradable channel]

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 [Sutter, Scholz, Winter, Renner 14]

Definition [approx degradable channel]

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

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

The little we know …

A nice twist [Sutter, Scholz, Winter, Renner 14]

Definition [approx degradable channel]

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 $| Q(N) - Q^{(1)}(N) | \leq -\eta \log \eta + O(\eta)$

Similarly $| P(N) - Q^{(1)}(N) | \leq O(\eta \log \eta)$ …

Throughout this talk, every story on Q(N) has a parallel in P(N) …

The little
we know …

A nice twist [Sutter, Scholz, Winter, Renner 14]

Definition [approx degradable channel]

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 $|\, Q(N) - Q^{(1)}(N) \,| \leq -\eta \log \eta + O(\eta)$

Original Devetak-Shor

Idea: ½ [I(R:B) – I(R:E)] (max of this gives $Q^{(1)}$)

= subadditive quantity + S(E') – S(E)

where E' = output of $M \circ N$ for any M.

Here:
r use version
well-behaved
by continuity
bounds if N
approx deg

The little we know …

A nice twist [Sutter, Scholz, Winter, Renner 14]

Definition [approx degradable channel]

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

Theorem [Sutter, Scholz, Winter, Renner 14]

If N is η-degradable,

then $| Q(N) - Q^{(1)}(N) | \le -\eta \log \eta + O(\eta)$

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

Outline

* Background

    Quantum channel & capacities

* The quantum don't-knows

    Superadditivity, superactivity, $Q \neq P$

* The quantum knows (5 mins?)

    Degradable channels, continuity, approx degradability

* Application to low noise channels (10mins?)

* Consequences

What we found:

η is much smaller than expected for low noise channels !!

1. If $\| N - I \|_\diamond \leq \varepsilon$, $\eta \leq 2\, \varepsilon^{1.5}$.

2. For depolarizing channel N_p ($\|N_p - I\|_\diamond = 2p$), $\eta = O(p^2)$!

What we found:

η is much smaller than expected for low noise channels !!

1. If $|| N - I ||_\diamond \leq \varepsilon$, $\eta \leq 2\, \varepsilon^{1.5}$.

2. For depolarizing channel N_p ($||N_p - I||_\diamond = 2p$), $\eta = O(p^2)$!

Consequences:

1. $Q(N) \approx P(N) \approx Q^{(1)}(N)$ up to $O(\varepsilon^{1.5} \log \varepsilon)$ corrections

2. $Q(N_p) \approx P(N_p) \approx Q^{(1)}(N_p) = 1 - h(p) - p \log 3$

up to $O(p^2 \log p)$ corrections

Consequences:

1. $Q(N) \approx P(N) \approx Q^{(1)}(N)$ up to $O(\varepsilon^{1.5} \log \varepsilon)$ corrections

2. $Q(N_p) \approx P(N_p) \approx Q^{(1)}(N_p) = 1 - h(p) - p \log 3$

up to $O(p^2 \log p)$ corrections

* $Q(N) \approx P(N)$ to the same order.
  Key rate does not exceed quantum data rate.
  (NB Quantum data is private, $Q(N) \geq P(N)$.)

* A random non-degenerate code for sending quantum data, and simple privacy amplification and classical ECC for sending key achieve rate $Q^{(1)}(N)$. Our results show that these simple techniques are almost rate optimal.
  No need to work any harder !!

Why is η so small for low noise channels ??

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.

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

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

To min η =

$||N_p^c - M \circ N_p ||_\diamond$

$\approx I$

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 $\eta =$

$||N_p^c - M \circ N_p||_\diamond$

$\approx I$

First try: $M = N_P^c$!!

Got $\eta \leq 2p^{1.5}$!   Works for all N !!

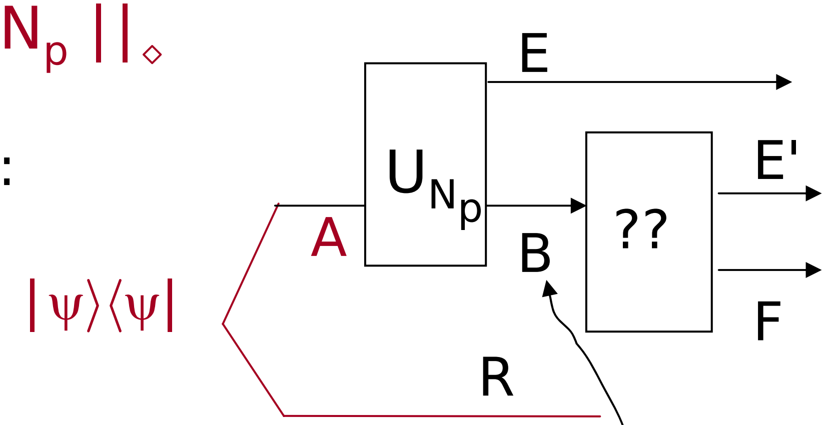
Theorem: Let a = 8/3.

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

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

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

Second try:



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

Theorem: Let $a = 8/3$.

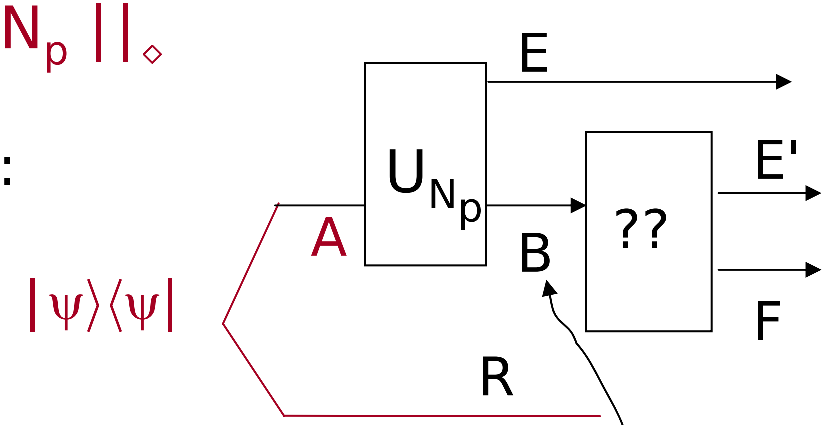
$$\| N_p^c - N_{p+ap^2}^c \circ N_p \|_\diamond \leq 8/9\,(6+\sqrt{2})\, p^2 + O(p^3)$$

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

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

Second try:

E has a little info from A



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

Theorem: Let a = 8/3.

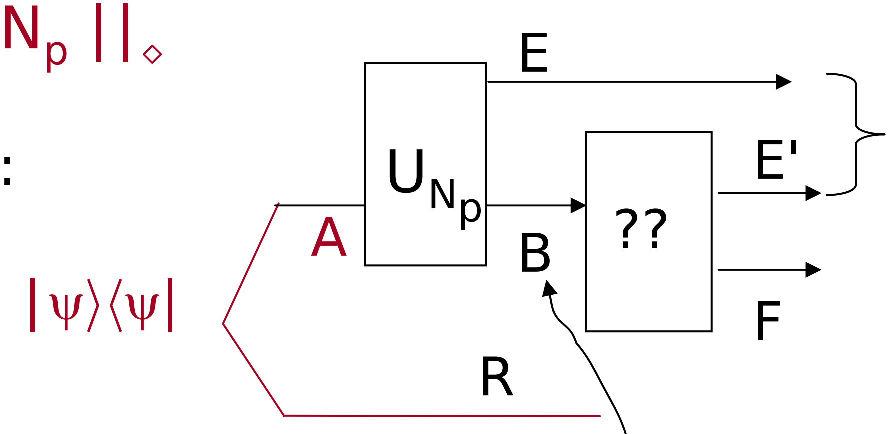
$$|| N_p^c - N_{p+ap^2}^c \circ N_p ||_\diamond \le 8/9\,(6+\sqrt{2})\, p^2 + O(p^3)$$

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

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

Second try:

E has a little info from A



Goal: make these similar

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

Theorem: Let a = 8/3.

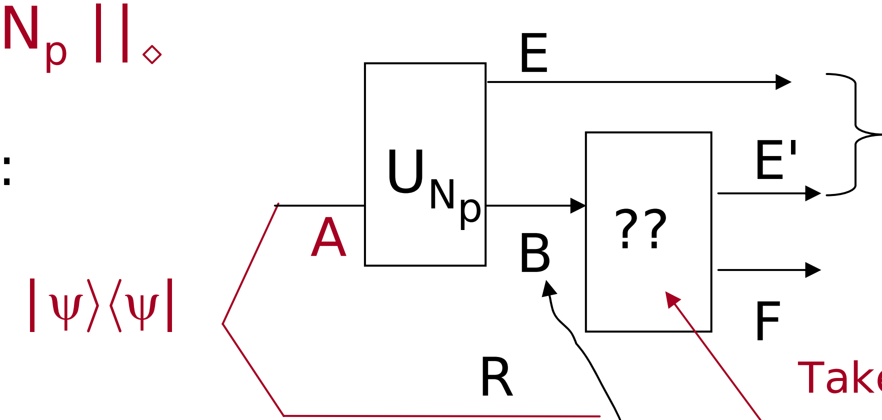
$$\| N_p^c - N_{p+ap^2}^c \circ N_p \|_\diamond \leq 8/9\,(6+\sqrt{2})\,p^2 + O(p^3)$$

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

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

Second try:

E has a little info from A



Goal: make these similar

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 ...

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

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 …
For example this includes the BB84 channel used for QKD …

Similar results hold for higher dimensional Pauli channels