# 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]

Frontiers of Quantum Informatin Physics
KITP, Oct 13, 2017

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

2: JILA, University of Colorado, Boulder

# Punchline

Task: given many uses of a noisy communication channel, we want to send as much data, as accurately, as possible.

Classical: $\max_X I(X:Y)$ bits per use (miracle)

Quantum: surprising quantum advantages :)
more complicated optimizations :(

This talk: in the low noise regime, everything's simple
but no special quantum advantage (boring).

## Outline

* Background

    Quantum channel & capacities

* The quantum don't-knows

    Superadditivity, superactivity, $Q \neq P$

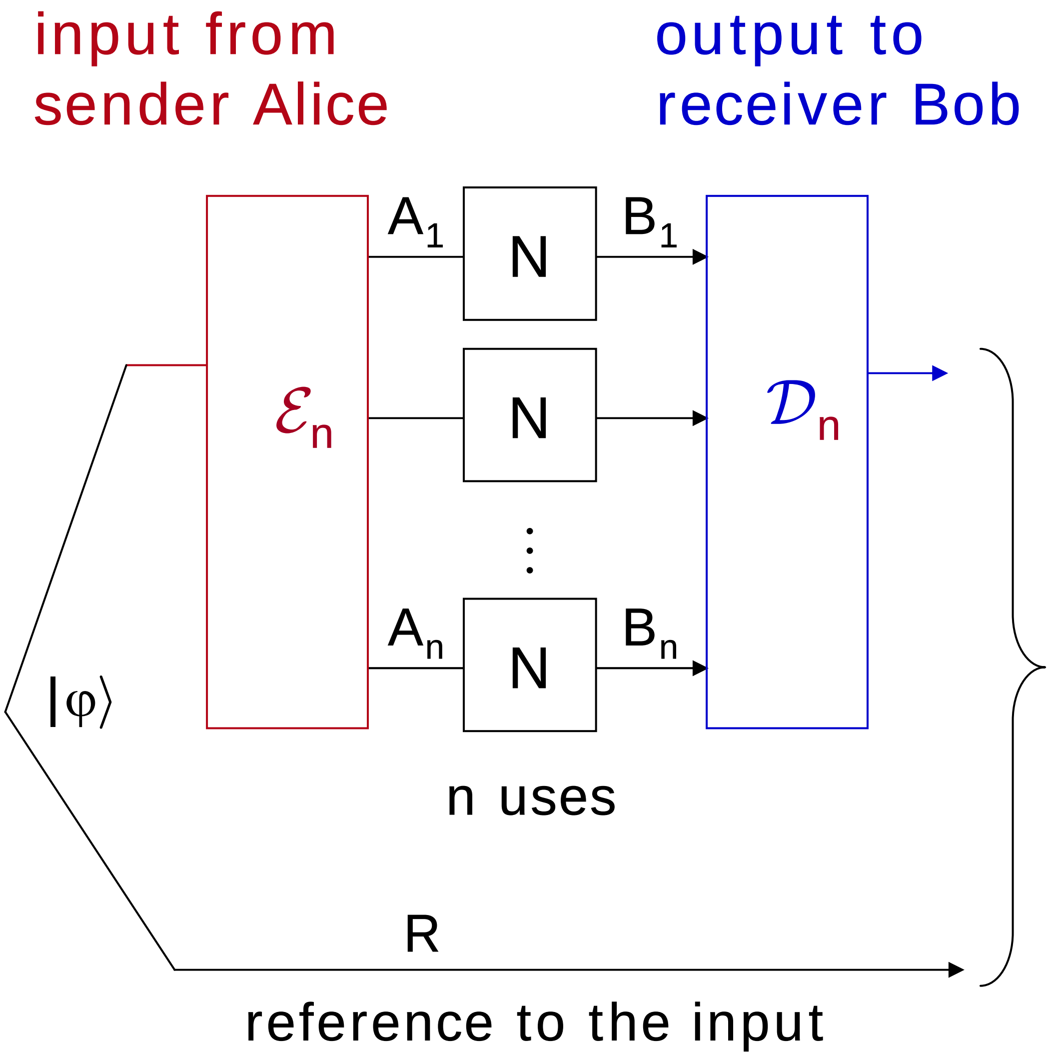
* The quantum knows

    Degradable channels, continuity, approx degradability

* Application to low noise channels

* Consequences

# Quantum data & discrete memoryless quantum channel




Fix n. Take only $\mathcal{E}_n$ ,$\mathcal{D}_n$

s.t $\mathcal{D}_n \circ N^{\otimes n} \circ \mathcal{E}_n \approx \mathcal{I}$

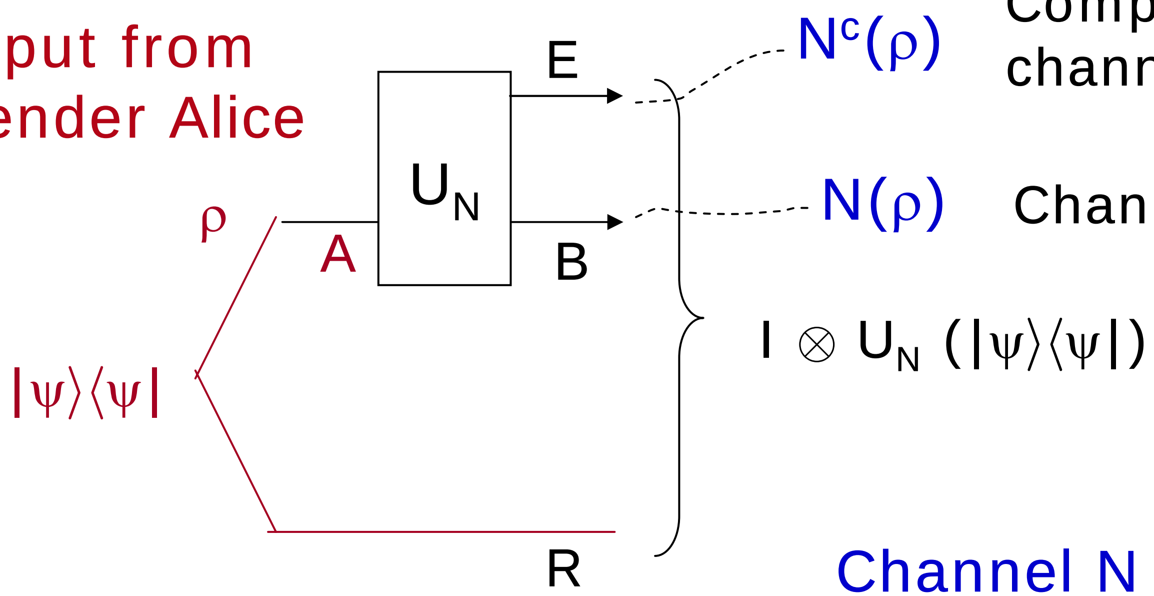
up to error $e_n$ .

As $n \to \infty$ $e_n \to 0$

$$\boxed{\text{Capacity } Q(N) = \sup_n (\#\text{qubits sent} / n)}$$

# Useful concepts and notations

input from sender Alice



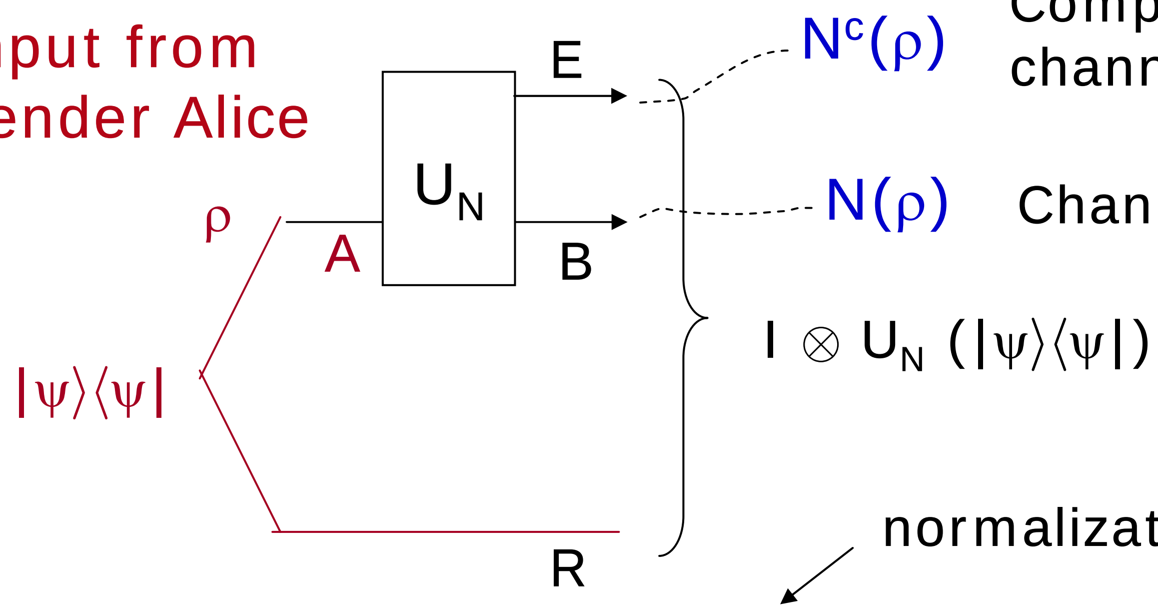

Complementary channel $N^c$ from A to E

Channel N from A to B

Channel N split input between receiver Bob and environment E

# 1-shot coherent information

input from
sender Alice




Complementary
channel $N^c$ from A to E

Channel N from A to B

normalization

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

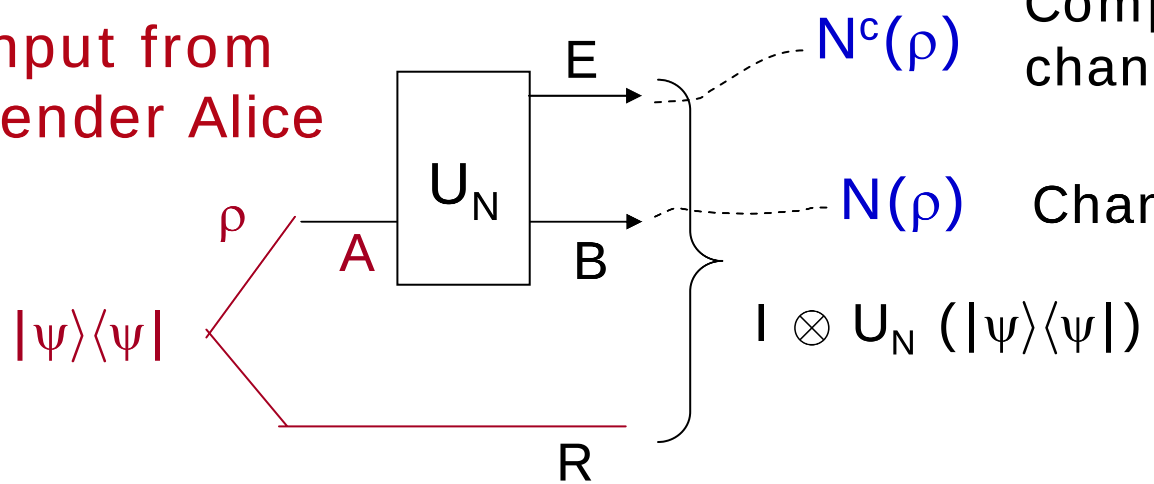
1-shot
coherent
info of N

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

info leaked
to the env

# The Lloyd-Shor-Devetak theorem

input from sender Alice

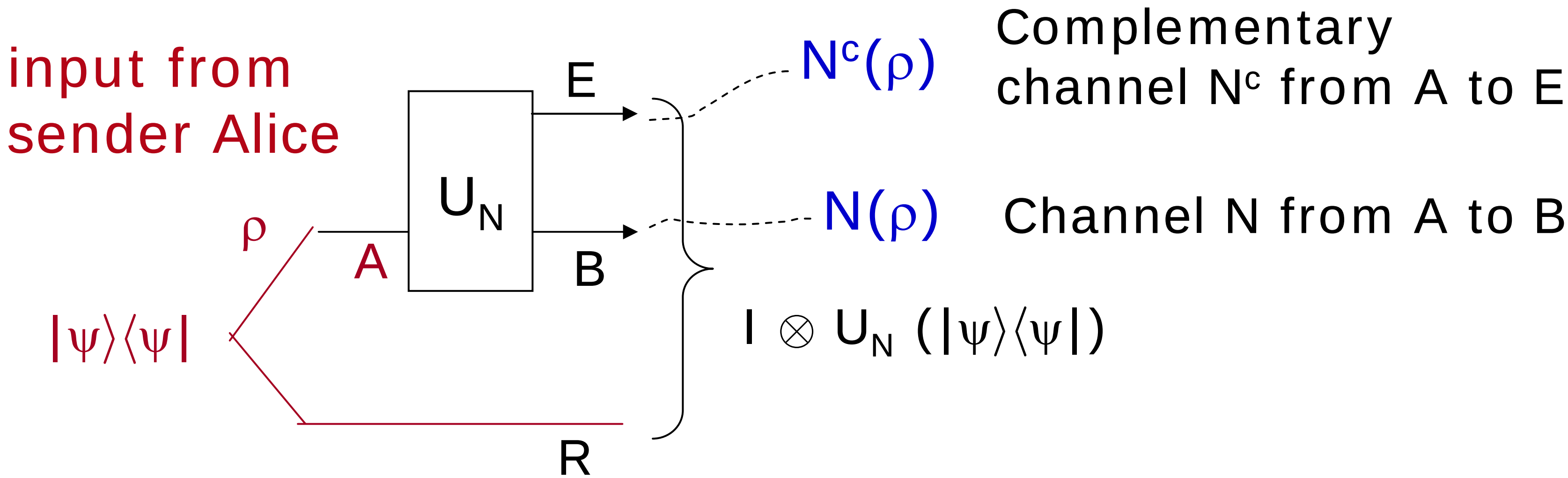



Complementary channel $N^c$ from A to E

Channel N from A to B

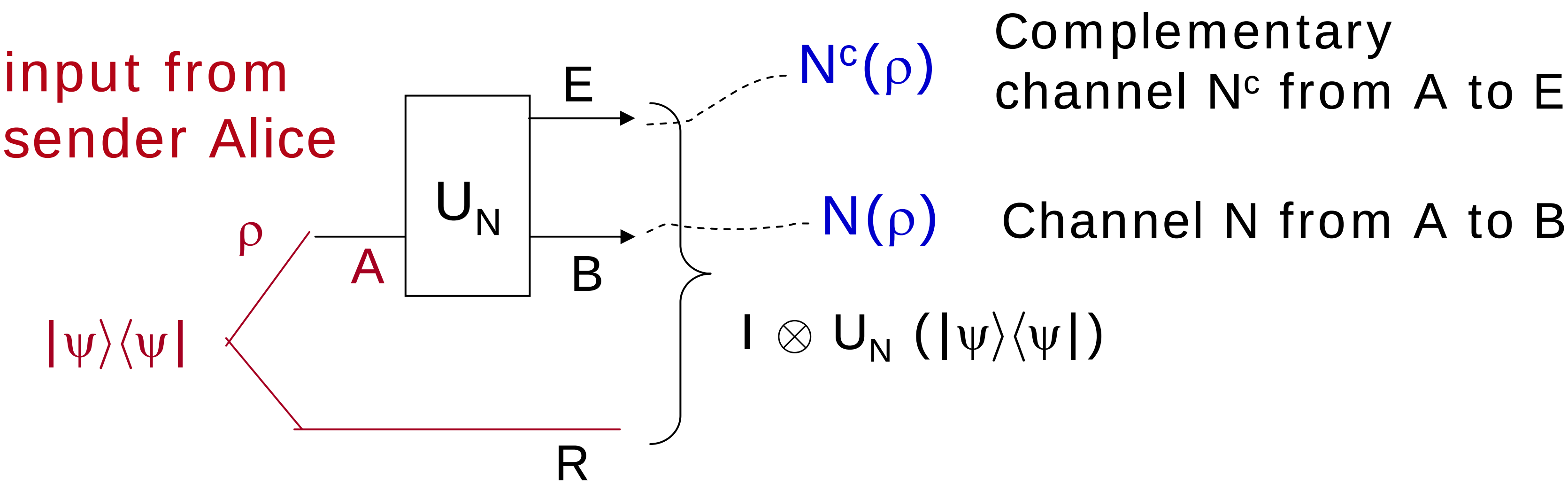
$$Q(N) \geq Q^{(1)}(N) := \max_{|\psi\rangle} \tfrac{1}{2} [I(R:B) - I(R:E)]$$

# The LSD theorem




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

# The LSD theorem




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

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

$$Q(N) \leq \sup_r Q^{(1)}(N^{\otimes r}) \, / \, r$$ (Schmacher & Westmoreland)

$$Q(N) = \sup_r Q^{(1)}(N^{\otimes r}) \, / \, r$$

# Outline

* Background

  Quantum channel & capacities (5mins?)

* The quantum don't-knows

  Superadditivity, superactivity, $Q \neq P$

* The quantum knows

  Degradable channels, continuity, approx degradability

* Application to low noise channels

* Consequences

# The quantum don't-knows

Qubit depolarizing channel.

$$N_p(\rho) = (1-p)\,\rho + p/3\; X \rho X + p/3\; Y \rho Y + p/3\; Z \rho Z$$

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

$Q^{(1)}(N_p) = 0$ for $p \geq 0.1894$, but $Q^{(1)}(N_p^{\otimes 5}) > 0$ for $p \leq 0.1904$.

DiVincenzo-Shor-Smolin 97

# The quantum don't-knows

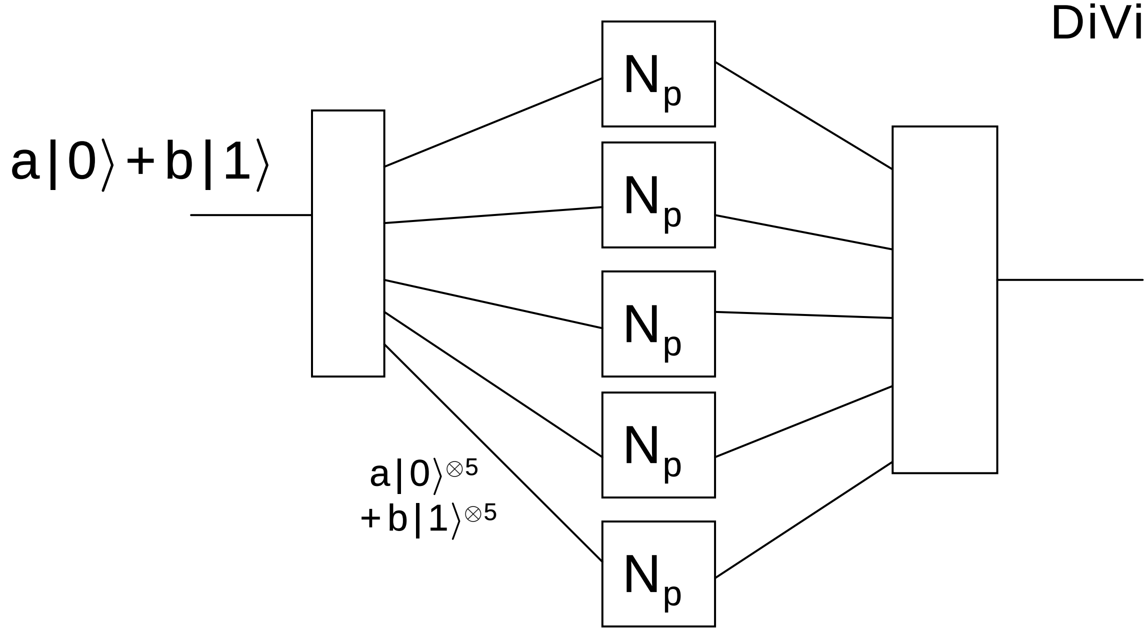
Qubit depolarizing channel.

$$N_p(\rho) = (1-p)\,\rho + p/3\; X\rho X + p/3\; Y\rho Y + p/3\; Z\rho Z$$

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

$Q^{(1)}(N_p) = 0$ for $p \geq 0.1894$, but $Q^{(1)}(N_p^{\otimes 5}) > 0$ for $p \leq 0.1904$.

DiVincenzo-Shor-Smolin 97



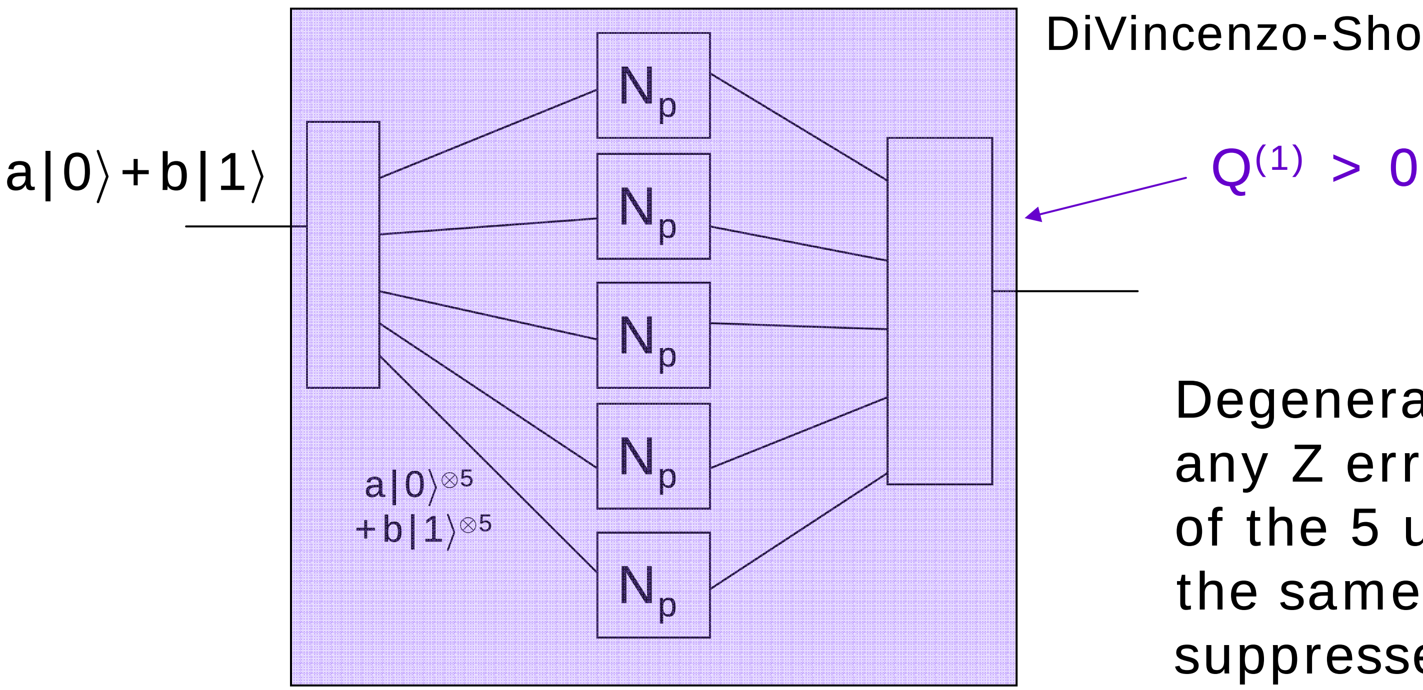
# The quantum don't-knows

Qubit depolarizing channel.

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

$Q^{(1)}(N_p) = 0$ for $p \geq 0.1894$, but $Q^{(1)}(N_p^{\otimes 5}) > 0$ for $p \leq 0.1904$.

DiVincenzo-Shor-Smolin 97




Degenerate code any Z error on any of the 5 uses acts the same, which suppresses I(R:E).

## The quantum don't-knows

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 $Q^{(1)}(N_p^{\otimes 5}) > 0$ for $p \leq 0.1904$.

DiVincenzo-Shor-Smolin 97

Still unknown after 20 years:

What is $Q(N_p)$ for $0 < p < ¼$?

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

## The quantum don't-knows

$$Q(N) = \sup_r Q^{(1)}(N^{\otimes r}) / r$$

* $Q^{(1)}$ can be superadditive and $\sup_r$ to stay for general N

* no algorithm to determine if $Q(N) = 0$

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

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

## 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 unknown to the 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.

## Outline

* Background

    Quantum channel & capacities (5 mins?)

* The quantum don't-knows

    Superadditivity, superactivity, $Q \neq P$ (10 mins?)

* The quantum knows

    Degradable channels, continuity, approx degradability

* Application to low noise channels

* Consequences

The little
we know …

# Degradable channels

Definition.

N is degradable if ∃ 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: $\frac{1}{2}$ [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 $\eta$-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 $\eta$-degradable if $\exists$ channel M s.t. $||N^c - M \circ N||_\diamond \le \eta$.

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

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

The little we know ...

Definition [approx degradable channel]

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

Theorem [Sutter, Scholz, Winter, Renner 14]

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

Theorem [Sutter, Scholz, Winter, Renner 14]

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

Theorem [Sutter, Scholz, Winter, Renner 14]

If N is $\eta$-degradable,

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

Advantage:

- M and $\eta$ can be numerically minimized as an SDP

Remaining problem:

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

## 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:

$\eta$ 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:

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

$\approx I$

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 !!

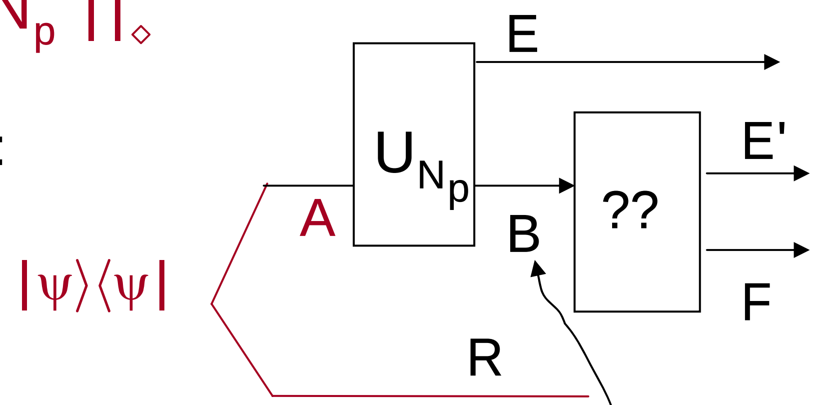
Theorem: Let a = 8/3.

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

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

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

Second try:




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

Theorem: Let a = 8/3.

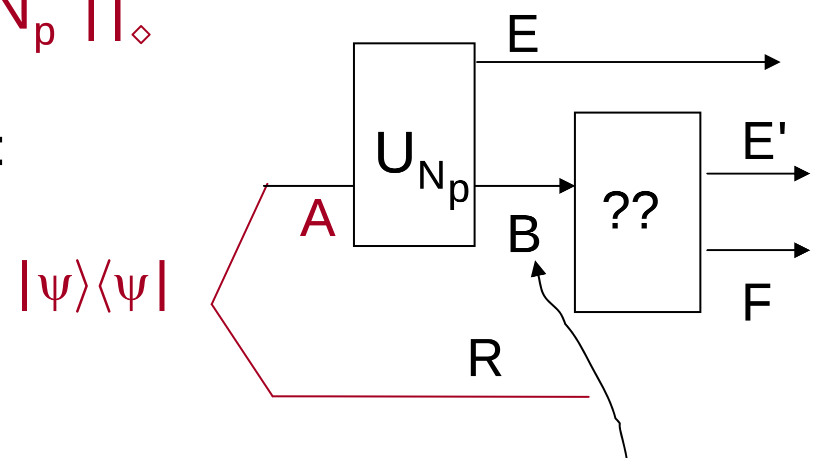
$$|| N_p^c - N_{p+ap^2}^c \circ N_p ||_\diamond \leq 8/9\ (6+\sqrt{2})\ p^2 + O(p^3)$$

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 !!

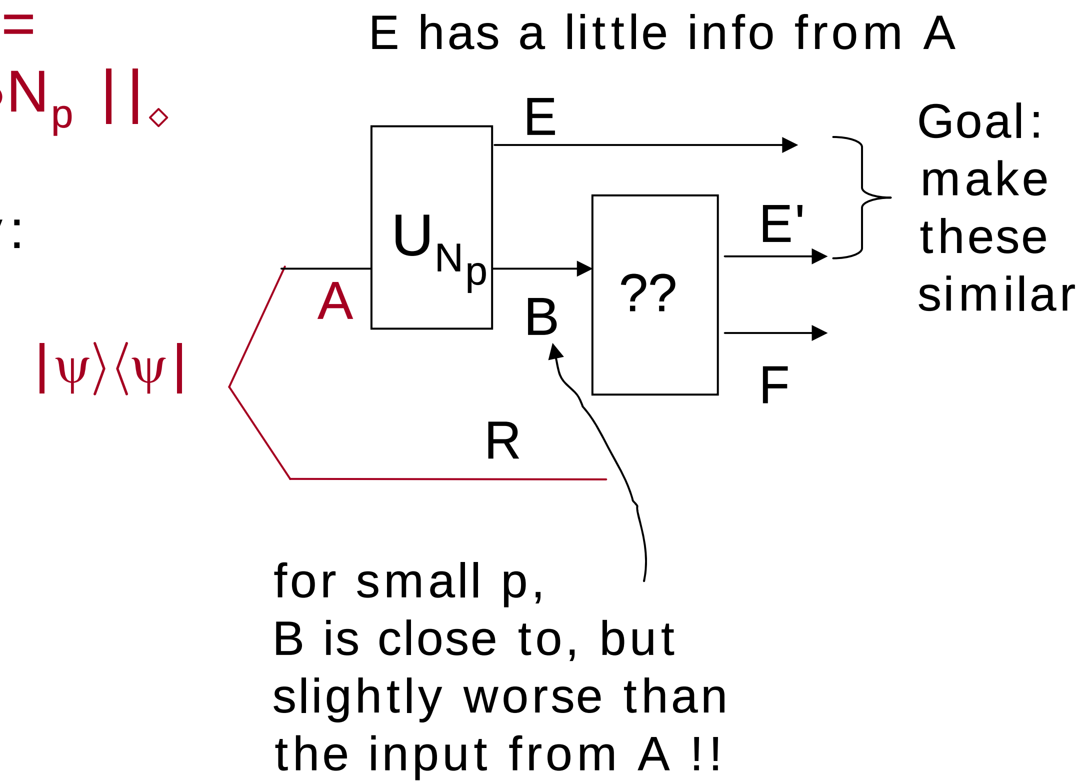
Theorem: Let a = 8/3.

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

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

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

Second try:



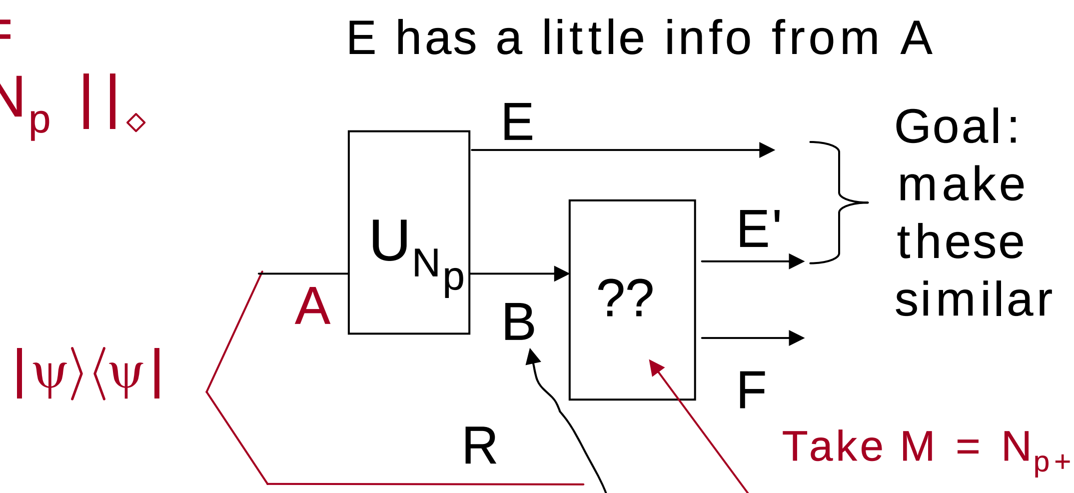
Theorem: Let a = 8/3.

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

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

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

Second try:




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

Similar results hold for higher dimensional Pauli 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

Open problems:

1. For a general channel N with $|| N - I ||_\diamond \leq \varepsilon$ ,
   is $\eta$ closer to $O(\varepsilon^{1.5})$ or $O(\varepsilon^2)$?

2. For what value of p does $Q(N_p) = 0$?

3. If $Q(N_p) > Q^{(1)}(N_p)$, can we understand why ?
   cf $Q^{(1)}(N_p^c) > 0 \quad \forall\, p > 0$ !!

4. Is "$Q(N)=0$?" decidable or not?