

# Additivity and Random Unitary Channels

arXiv:0804.1936

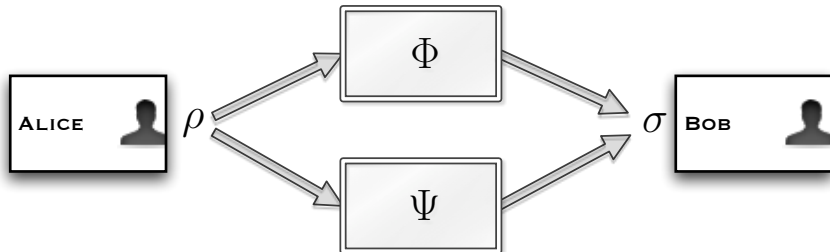
Bill Rosgen

Institute for Quantum Computing  
University of Waterloo

September 24, 2008



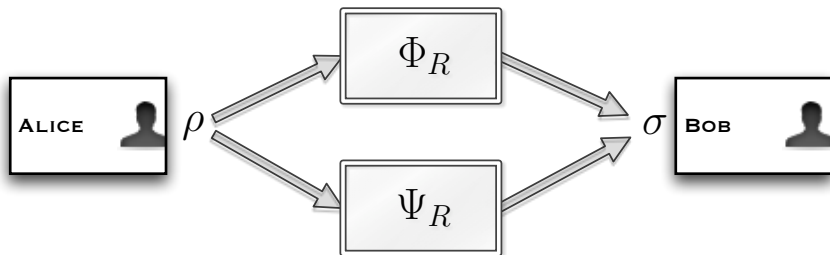
# What is this talk about?



- ▶ Alice prepares  $\rho$  sends it to Bob, who measures  $\sigma$ .
- ▶ Does Alice need to use entangled  $\rho$  to get optimal rate?

# What this talk is about.

- ▶ Does the problem get easier if  $\Phi$  and  $\Psi$  are restricted?



- ▶ This talk is about this problem on random unitary channels.

# Outline

Additivity

Mixed Unitary Channels

Construction

Sketch of Proof

# Quantum channels

A channel is a linear completely positive trace preserving map.

- ▶  $\text{tr } \Phi(X) = \text{tr } X$
- ▶ If  $X \geq 0$  then  $(\Phi \otimes I_{\mathcal{F}})(X) \geq 0$



# Examples of channels

- ▶ Completely depolarizing channel

$$N(\rho) = \mathbb{1}/d, \quad N \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} 1/3 & 0 & 0 \\ 0 & 1/3 & 0 \\ 0 & 0 & 1/3 \end{pmatrix}$$

- ▶ Completely dephasing channel

$$D(|i\rangle\langle j|) = \delta_{ij}|i\rangle\langle j|, \quad D \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{pmatrix}$$

## Representations of channels

There are two representations of channels that we will need.

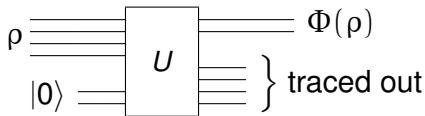
### Definition (Kraus representation)

There exist operators  $A_i$  such that  $\sum_i A_i^* A_i = \mathbb{1}$  and  $\Phi(X) = \sum_i A_i X A_i^*$ .

### Definition (Stinespring dilation)

For a channel on states on  $\mathcal{A}$ , there exists a unitary  $U$  on  $\mathcal{A} \otimes \mathcal{B}$  such that

$$\Phi(X) = \text{tr}_{\mathcal{B}} U(X \otimes |0\rangle\langle 0|)U^*.$$



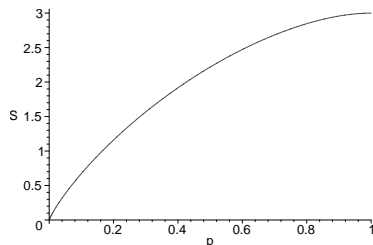
# Entropy

## Definition

The von Neumann entropy of a density matrix  $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$  is

$$S(\rho) = -\text{tr } \rho \log \rho = -\sum_i \lambda_i \log \lambda_i.$$

- ▶  $S(\mathbb{1}/d) = \log d$
- ▶  $S(|\psi\rangle\langle\psi|) = 0$
- ▶  $S(p\mathbb{1}/d + (1-p)|\psi\rangle\langle\psi|)$ :



- ▶  $S(p\rho + (1-p)\sigma) \geq pS(\rho) + (1-p)S(\sigma)$

# Holevo capacity

- ▶ The classical capacity of one use of a channel  $\Phi$  is<sup>1</sup>

$$C_{\chi}(\Phi) = \max_{\rho_i, |\psi_i\rangle} S\left(\sum_i \rho_i \Phi(|\psi_i\rangle\langle\psi_i|)\right) - \sum_i \rho_i S(\Phi(|\psi_i\rangle\langle\psi_i|)).$$

Examples:

- ▶ For  $N(\rho) = \mathbb{1}/d$ ,  $C_{\chi}(N) = 0$ .
- ▶  $C_{\chi}(D) = C_{\chi}(I) = \log d$ .

---

<sup>1</sup>Schumacher and Westmoreland 1997, Holevo 1998

# Additivity?

The classical capacity of a channel  $\Phi$  is

$$C(\Phi) = \lim_{n \rightarrow \infty} \frac{1}{n} C_X(\Phi^{\otimes n}).$$

This limit is not required if the additivity conjecture holds.

Conjecture (Additivity of  $C_X^2$ )

$$C_X(\Phi \otimes \Psi) \stackrel{?}{=} C_X(\Phi) + C_X(\Psi)$$

---

<sup>2</sup>Bennett, Fuchs, and Smolin 1996

# Minimum output entropy

For a channel  $\Phi$ , how pure can the output be?

## Definition

$$S_{\min}(\Phi) = \min_{\rho} S(\Phi(\rho))$$

Examples:

- ▶  $S_{\min}(N) = S(N(\rho)) = S(\mathbb{1}) = \log d$
- ▶  $S_{\min}(D) = S(D(|0\rangle\langle 0|)) = S(|0\rangle\langle 0|) = 0$

## Another conjecture

### Conjecture (Additivity of $S_{\min}$ <sup>3</sup>)

$$S_{\min}(\Phi \otimes \Psi) \stackrel{?}{=} S_{\min}(\Phi) + S_{\min}(\Psi)$$

This conjecture is globally equivalent to the previous one, as well as the strong superadditivity of the entanglement of formation<sup>4</sup>.

- ▶ This is really a conjecture about *entanglement*, i.e. does

$$\begin{aligned} S_{\min}(\Phi) + S_{\min}(\Psi) &= \min_{\rho, \sigma} S((\Phi \otimes \Psi)(\rho \otimes \sigma)) \\ &\stackrel{?}{=} \min_{\rho} S((\Phi \otimes \Psi)(\rho)) \\ &= S_{\min}(\Phi \otimes \Psi) \end{aligned}$$

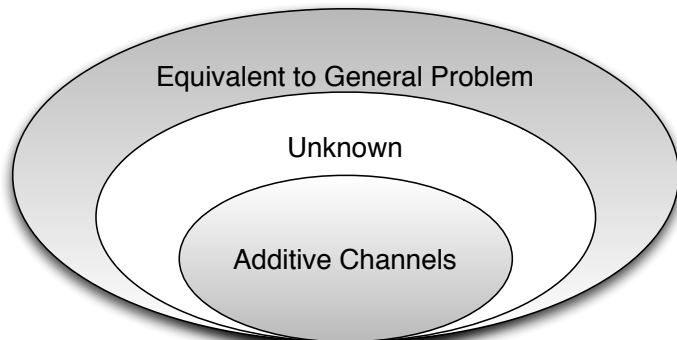
<sup>3</sup>King and Ruskai 2001, who attribute it to Shor

<sup>4</sup>Shor 2004

## What is known?

Previous work on the  $S_{\min}$  conjecture falls into two groups:

1. Proving the conjecture for restricted channels
2. Proving the equivalence of the conjecture on restricted channels



# Classes of additive channels

$S_{\min}$  is additive if one of the two channels is:

- ▶ entanglement breaking<sup>5</sup>
  - ▶  $(\Phi \otimes I)(\rho)$  is separable for all  $\rho$
  - ▶ This class contains  $N$ ,  $D$  and other popular channels.
- ▶ a unital channel on qubits<sup>6</sup>
  - ▶  $\Phi$  is unital if  $\Phi(\mathbb{1}) = \mathbb{1}$
  - ▶ Qubit channels have input and output dimension 2
  - ▶ These are exactly<sup>7</sup> the channels we consider later, restricted to qubits!

---

<sup>5</sup>Shor 2002

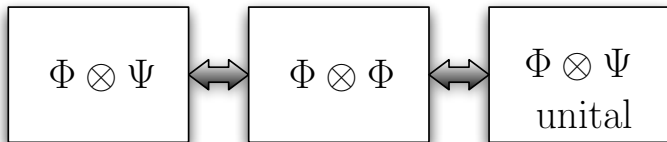
<sup>6</sup>King 2002

<sup>7</sup>Tregub 1986, Landau and Streater 1993

## Equivalent conjectures

The following are equivalent:

1.  $\mathcal{S}_{\min}(\Phi \otimes \Psi) = \mathcal{S}_{\min}(\Phi) + \mathcal{S}_{\min}(\Psi)$  is true for any  $\Phi, \Psi$ .
2.  $\mathcal{S}_{\min}(\Phi \otimes \Phi) = 2\mathcal{S}_{\min}(\Phi)$  is true for any  $\Phi$ .<sup>8</sup>
3.  $\mathcal{S}_{\min}(\Phi \otimes \Psi) = \mathcal{S}_{\min}(\Phi) + \mathcal{S}_{\min}(\Psi)$  is true for any **unital**  $\Phi, \Psi$ .<sup>9</sup>



<sup>8</sup>Fukuda and Wolf 2007

<sup>9</sup>Fukuda 2007

# Fukuda's Argument

To show that additivity of  $S_{\min}$  is equivalent on two channels:

1. From a channel  $\Phi$  construct a unital channel  $\Phi'$  such that

$$S_{\min}(\Phi) = S_{\min}(\Phi')$$

and

$$S_{\min}(\Phi \otimes \Psi) = S_{\min}(\Phi' \otimes \Psi).$$

2. Assuming additivity for unital channels,

$$\begin{aligned} S_{\min}(\Phi \otimes \Psi) &= S_{\min}(\Phi' \otimes \Psi') \\ &= S_{\min}(\Phi') + S_{\min}(\Psi') \\ &= S_{\min}(\Phi) + S_{\min}(\Psi). \end{aligned}$$

# Outline

Additivity

Mixed Unitary Channels

Construction

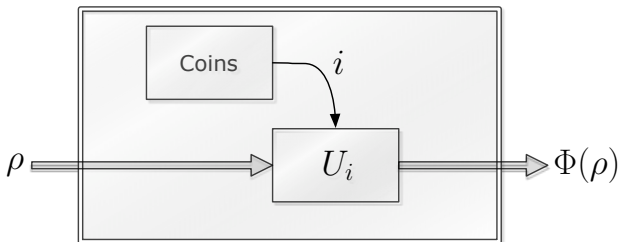
Sketch of Proof

# Random Mixed-unitary channels

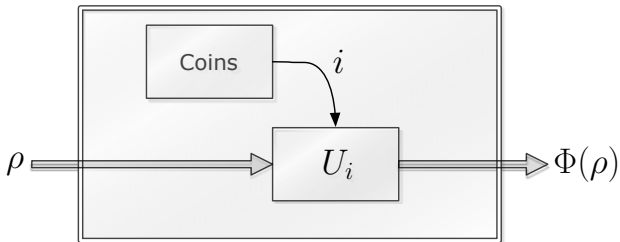
## Definition

A channel  $\Phi$  is *mixed-unitary* if there exists a probability distribution  $p_i$  and unitaries  $U_i$  such that

$$\Phi(X) = \sum_i p_i U_i X U_i^*.$$



# Why you should care about mixed-unitary channels



- ▶ Exactly the channels reversible using information measured from the environment<sup>10</sup>
- ▶ Need at most  $d^4$  unitaries in a decomposition<sup>11</sup>
- ▶ Strict subset of the unital channels<sup>12</sup>

<sup>10</sup>Gregoratti and Werner 2003

<sup>11</sup>Buscemi 2006

<sup>12</sup>Landau and Streater 1993

## Examples of mixed-unitary channels

- ▶ Composing two mixed-unitary channels  $\Phi, \Psi$ :

$$\Phi(\Psi(\rho)) = \sum_{ij} p_i q_j U_i V_j \rho V_j^* U_i^*$$

- ▶ Depolarizing channel  $N(\rho) = \mathbb{1}/d$ :

$$N(\rho) = \frac{1}{4} \left[ I\rho I + X\rho X + Z\rho Z + XZ\rho(XZ)^* \right] = \frac{\mathbb{1}}{2}$$

- ▶ Dephasing channel  $D(|i\rangle\langle j|) = \delta_{ij}|i\rangle\langle j|$ :

$$D(\rho) = \frac{1}{2} \left[ I\rho I + Z\rho Z \right]$$

# Not everything is mixed-unitary

- ▶  $\Phi(\rho) = |0\rangle\langle 0|$  is not unital.
- ▶ The channel  $\Phi(\rho) = \frac{1}{d-1}(\text{tr}(\rho)\mathbb{1} - \rho^\top)$  for  $d = 3$  is unital but not mixed-unitary.
  - ▶ This is the Werner-Holevo counterexample to the (recently falsified) maximum output  $p$ -norm conjecture!

## Open Problem

*Characterize the unital channels that are not mixed unitary.*

# Outline

Additivity

Mixed Unitary Channels

Construction

Sketch of Proof

# The result

## Theorem

*The additivity conjecture*

$$S_{\min}(\Phi \otimes \Psi) = S_{\min}(\Phi) + S_{\min}(\Psi)$$

*holds for all channels  $\Phi, \Psi$  if and only if it holds for all mixed-unitary channels  $\Phi, \Psi$ .*

- ▶ This generalizes Fukuda's result on unital channels
- ▶ Can be extended to two copies of the same channel using the construction of Fukuda and Wolf

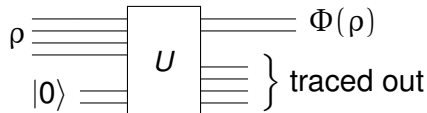
# Overview

Proof strategy:

- ▶ Given a channel  $\Phi$ , find an approximation  $\Phi'$  that is mixed-unitary
- ▶ Reduction of additivity to mixed-unitary case follows from the approximation scheme
  
- ▶ Features of the approximation:
  1. Approximation error is  $O(\log m/m)$ , where  $m$  is the dimension of the ancillary space added.
  2. Given a circuit, approximation can be constructed efficiently

# Quantum channels

$$\text{Let } \Phi(\rho) = \text{tr}_B U(\rho \otimes |0\rangle\langle 0|)U^*$$

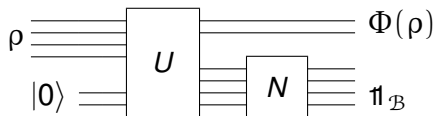


Only two operations that are not mixed-unitary:

1. Partial trace
2. Ancillary qubits in  $|0\rangle$  state

# Approximating the partial trace

- ▶ Replace  $\text{tr}_{\mathcal{B}}$  with the completely noisy channel on  $\mathcal{B}$



- ▶ The resulting output is  $\Phi(\rho) \otimes I_{\mathcal{B}}$

## Proof (sleeping allowed)

$$\begin{aligned}
 (I \otimes N)(\sigma) &= \sum_{i,j} (I \otimes |i\rangle\langle j|) \sigma (I \otimes |j\rangle\langle i|) \\
 &= \sum_i (I \otimes |i\rangle) \left[ \sum_j (I \otimes \langle j|) \sigma (I \otimes |j\rangle) \right] (I \otimes \langle i|) \\
 &= \sum_i (I \otimes |i\rangle) [\text{tr}_{\mathcal{B}} \sigma] (I \otimes \langle i|) \\
 &= \text{tr}_{\mathcal{B}} \sigma \otimes \sum_i |i\rangle\langle i| \\
 &= \text{tr}_{\mathcal{B}} \sigma \otimes \mathbb{1}
 \end{aligned}$$

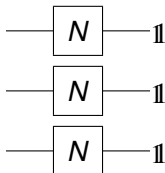
- ▶ Replacing  $\sigma$  with  $U(\rho \otimes |0\rangle\langle 0|)U^*$  finishes the proof

## Depolarizing is mixed-unitary

The depolarizing channel can be written as

$$N(\rho) = \int U\rho U^* dU = \frac{1}{d^2} \sum_{i=1}^{d^2} W_i \rho W_i^* = \mathbb{1}/d$$

for a suitable choice of operators  $W_i$ .



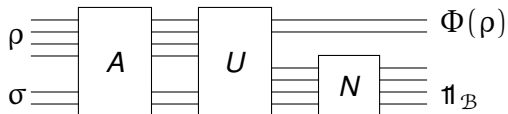
One such choice:

- ▶ apply Pauli  $X$  with probability  $1/2$  on each qubit
- ▶ followed by Pauli  $Z$  with probability  $1/2$  on each qubit

# Simulating ancillary qubits

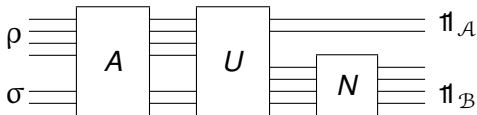
To simulate ancillary space:

- ▶ Add extra 'input' qubits
- ▶ Test that these qubits are in the  $|0\rangle$  state
  - ▶ If they are, do nothing
  - ▶ If not, send all input qubits to highly mixed state



# Intuition

If  $\sigma$  is far from  $|0\rangle\langle 0|$ , the output is (almost) completely mixed



- ▶ If the input is highly mixed, so is the output
- ▶ Mixed output has high entropy
  - ▶ i.e. any input minimizing the output entropy will have  $\sigma \approx |0\rangle\langle 0|$

# Mixed-unitaries do not reduce entropy

## Lemma

If  $\Phi$  is mixed-unitary, then  $S(\rho) \leq S(\Phi(\rho))$ .

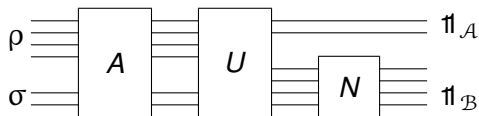
## Proof.

$$\begin{aligned} S(\Phi(\rho)) &= S\left(\sum_i p_i U_i \rho U_i^*\right) \\ &\geq \sum_i p_i S(U_i \rho U_i^*) \\ &= \sum_i p_i S(\rho) \\ &= S(\rho). \end{aligned}$$

□

## The problem

The ideal operation  $A$  is not unital, and so it is not mixed unitary.



- ▶ Mixing operation only needs to increase the entropy, not completely mix the states not of the form  $\rho \otimes |0\rangle\langle 0|$
- ▶ Solution: completely mix the subspace of states  $\mathcal{H} \otimes \{|0\rangle\}^\perp$
- ▶ This is where the approximation occurs.

## Mixing $\mathcal{H} \otimes \{|0\rangle\}^\perp$

- ▶ Let  $\{|e_k\rangle : 1 \leq k \leq d\}$  be a basis for this subspace
- ▶ Generalized Pauli operators:  $W_{a,b} = Z^b X^a$ , where

$$X|e_k\rangle = |e_{k+1}\rangle$$

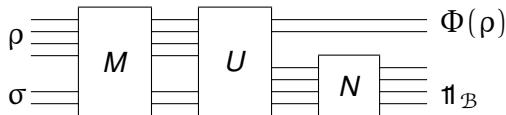
$$Z|e_k\rangle = \omega_{d-1}^k |e_k\rangle$$

$$X\rho = Z\rho = \rho, \text{ for } \rho \in \mathcal{H} \otimes \{|0\rangle\}.$$

- ▶ Completely depolarizing channel on this subspace is given by

$$M(X) = \frac{1}{(d-1)^2} \sum_{a,b} W_{a,b} X W_{a,b}^*.$$

# One final piece . . .



- ▶ Potential problem: entanglement between the subspaces  $\mathcal{H} \otimes \{|0\rangle\}$  and  $\mathcal{H} \otimes \{|0\rangle\}^\perp$  complicates the argument
- ▶ Solution: apply dephasing between these subspaces

# Dephasing

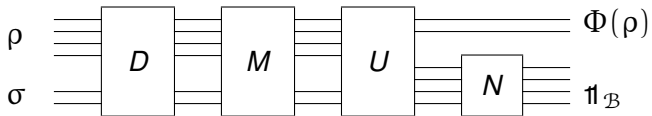
- ▶ Goal: take a density matrix  $\rho$  to  $p\sigma + (1 - p)\gamma$  with
  - ▶  $\sigma \in \mathcal{H} \otimes \{|0\rangle\}$
  - ▶  $\gamma \in \mathcal{H} \otimes \{|0\rangle\}^\perp$
- ▶ i.e. eliminate any terms  $|i\rangle\langle j|$  with  $|i\rangle, |j\rangle$  in different subspaces

$$V|i\rangle = \begin{cases} |i\rangle & \text{if } |i\rangle \in \sigma \in \mathcal{H} \otimes \{|0\rangle\} \\ -|i\rangle & \text{if } |i\rangle \in \sigma \in \mathcal{H} \otimes \{|0\rangle\}^\perp \end{cases}$$

- ▶ Apply  $V$  with probability 1/2:

$$D(|i\rangle\langle j|) = \frac{1}{2} \left[ |i\rangle\langle j| + V|i\rangle\langle j|V^* \right] = \begin{cases} |i\rangle\langle j| & \text{if } |i\rangle, |j\rangle \text{ in same subspace} \\ 0 & \text{otherwise} \end{cases}$$

# The final construction



- ▶ The result is random unitary, since all of the components are.

# Outline

Additivity

Mixed Unitary Channels

Construction

Sketch of Proof

# Approximation theorem

## Theorem

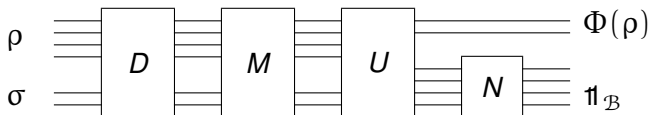
*Let  $\Phi'$  be the mixed-unitary approximation to a channel  $\Phi$  with input plus ancilla dimension  $d$ , then*

$$S_{\min}(\Phi) \geq S_{\min}(\Phi') - \log d \geq S_{\min}(\Phi) - O(\log d/d)$$

- ▶ By adding extra (unused) ancilla dimension to  $\Phi$ ,  $d$  can be increased to make the approximation arbitrarily good

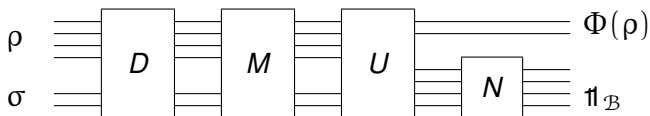
## Proof sketch ... (1 of 2)

Let  $\Phi'$  be the mixed unitary channel constructed from  $\Phi$ .



- ▶  $\Phi'(\rho \otimes |0\rangle\langle 0|) = \Phi(\rho) \otimes \mathbb{1}$
- ▶ Therefore,  $S_{\min}(\Phi') \leq S_{\min}(\Phi) + \log d$

## Proof sketch ... (2 of 2)



- ▶ If  $\sigma \in \mathcal{H} \otimes \{|0\rangle\}^\perp$ , then

$$S(\Phi'(\sigma)) > S(\mathbb{1}) - O(\log d/d) = \log d - O(\log d/d).$$

- ▶ For general input,  $D(\gamma) = q\rho \otimes |0\rangle\langle 0| + (1 - q)\sigma$ , so that

$$\begin{aligned} S_{\min}(\Phi') &= S(\Phi'(\gamma^*)) = S(\Phi'(D(\gamma^*))) \\ &\geq qS(\Phi'(\rho \otimes |0\rangle\langle 0|)) + (1 - q)S(\xi) \\ &> qS(\Phi(\rho) \otimes \mathbb{1}) + (1 - q)S(\mathbb{1}) - O(\log d/d) \\ &\geq S_{\min}(\Phi) + \log d - O(\log d/d) \end{aligned}$$

# Approximation theorem

## Theorem

*Let  $\Phi'$  be the mixed-unitary approximation to a channel  $\Phi$  with input plus ancilla dimension  $d$ , then*

$$S_{\min}(\Phi) \geq S_{\min}(\Phi') - \log d \geq S_{\min}(\Phi) - O(\log d/d)$$

- ▶ By adding extra (unused) ancilla dimension to  $\Phi$ ,  $d$  can be increased to make the approximation arbitrarily good

# Application to additivity

## Corollary

*The additivity conjecture*

$$S_{\min}(\Phi \otimes \Psi) = S_{\min}(\Phi) + S_{\min}(\Psi)$$

*holds for all  $\Phi, \Psi$  if and only if it holds for all mixed-unitary  $\Phi, \Psi$ .*

## Proof.

*Let  $\epsilon > 0$  and let the added dimension  $m$  be large enough, then assuming the additivity conjecture on mixed-unitary channels*

$$\begin{aligned} S_{\min}(\Phi \otimes \Psi) &\geq S_{\min}(\Phi' \otimes \Psi') - 2 \log d \\ &= S_{\min}(\Phi') + S_{\min}(\Psi') - 2 \log d \\ &\geq S_{\min}(\Phi) + S_{\min}(\Psi) - \epsilon. \end{aligned}$$

□

# Applications and open problems

This approximation scheme can also be used to show that

- ▶ Multiplicativity of the  $p$ -norm can also be restricted to mixed-unitary channels
- ▶ Distinguishing circuits is no easier if they implement mixed-unitary operations (**QIP**-complete).

Open problems:

- ▶ How far can such equivalences be extended?
- ▶ Can this be applied to other problems?