4-2. Distinguishability

Trace distance
  Trace norm and polar decomposition
  Minimum-error discrimination
Fidelity
  Fidelity and distinguishability
  No-cloning theorem
Relation between fidelity and trace distance
**Distinguishability**

Measure of distinguishability between two states \( D(\hat{\rho}, \hat{\sigma}) \)

A quantity describing how we can distinguish between the two states in principle.

The distinguishability should never be improved by a quantum operation.

Examples

\[
\begin{align*}
\frac{1}{2}\|\hat{\rho} - \hat{\sigma}\| \\
1 - F(\hat{\rho}, \hat{\sigma})
\end{align*}
\]

Monotonicity under quantum operations

\[
D(\hat{\rho}, \hat{\sigma}) \geq D(\chi(\hat{\rho}), \chi(\hat{\sigma}))
\]
Distinguishability

A quantity describing how we can distinguish between the two states in principle.

Measure of distinguishability

Quantum channel (CPTP map)

The distinguishability should never be improved by a quantum operation.

• Attach an ancilla
• Apply a unitary
• Discard the ancilla

Monotonicity under quantum operations

$D(\hat{\rho}, \hat{\sigma}) \geq D(\chi(\hat{\rho}), \chi(\hat{\sigma}))$
Trace norm

\[ \|\hat{A}\| = \|\hat{A}\|_1 \equiv \text{Tr}|\hat{A}| = \text{Tr}\sqrt{\hat{A}^\dagger \hat{A}} \]

In particular, when \( \hat{A} \) is normal (diagonalizable),

\[ \text{Tr}(|\hat{A}|) = \sum_j |\lambda_j| \quad \lambda_j: \text{Eigenvalues of } \hat{A} \]

\[ \|\hat{A}\| = \max_{\hat{U}} |\text{Tr}(\hat{A}\hat{U})| \]

\[ |\hat{A}| = \sum_j \nu_j |j\rangle \langle j| \quad \|\hat{A}\| = \sum_j \nu_j \]

\[ \text{Tr}(\hat{A}\hat{U}) = \text{Tr}(\hat{V}|\hat{A}|\hat{U}) = \sum_j \nu_j \langle j|\hat{U}\hat{V}|j\rangle \]

\[ |\langle j|\hat{U}\hat{V}|j\rangle| \leq 1 \text{ for any } \hat{U} \]

\[ \hat{U} = \hat{V}^\dagger \rightarrow |\langle j|\hat{U}\hat{V}|j\rangle| = 1 \]

Polar decomposition

number \( \alpha = e^{i\theta}|\alpha| \)

linear operator \( \hat{A} = \hat{V}|\hat{A}| \)

unitary \rightarrow \text{positive}

\[ |\hat{A}| \equiv \sqrt{\hat{A}^\dagger \hat{A}} \]

\[ \hat{V} \equiv \hat{A}|\hat{A}|^{-1} \]

(when \( \hat{A} \) is invertible)

\[ \hat{V}^\dagger \hat{V} = |\hat{A}|^{-1}\hat{A}^\dagger \hat{A}|\hat{A}|^{-1} = \hat{1} \]
**Trace distance** \[ \| \cdot \| : \text{trace norm} \]

\[ \frac{1}{2} \| \hat{\rho} - \hat{\sigma} \| \]

Zero when \( \hat{\rho} = \hat{\sigma} \) (the same state)

Unity when \( \hat{\rho} \hat{\sigma} = 0 \) (perfectly distinguishable)

**Monotonicity**

\[ \| \hat{\rho} - \hat{\sigma} \| \geq \| \chi(\hat{\rho}) - \chi(\hat{\sigma}) \| \]

- Attach an ancilla
  \[ \hat{\rho} \rightarrow \hat{\rho} \otimes \hat{\tau} \quad \hat{\sigma} \rightarrow \hat{\sigma} \otimes \hat{\tau} \]
  \[ \| \hat{\rho} \otimes \hat{\tau} - \hat{\sigma} \otimes \hat{\tau} \| = \| (\hat{\rho} - \hat{\sigma}) \otimes \hat{\tau} \| = \| \hat{\rho} - \hat{\sigma} \| \times \| \hat{\tau} \| = \| \hat{\rho} - \hat{\sigma} \| \]

- Apply a unitary
  \[ \hat{\rho} \rightarrow \hat{U} \hat{\rho} \hat{U}^\dagger \quad \hat{\sigma} \rightarrow \hat{U} \hat{\sigma} \hat{U}^\dagger \]
  \[ \| \hat{U} \hat{\rho} \hat{U}^\dagger - \hat{U} \hat{\sigma} \hat{U}^\dagger \| = \| \hat{U} (\hat{\rho} - \hat{\sigma}) \hat{U}^\dagger \| = \| \hat{\rho} - \hat{\sigma} \| \]

- Discard the ancilla
  \[ \hat{\rho} \rightarrow \text{Tr}_R(\hat{\rho}) \quad \hat{\sigma} \rightarrow \text{Tr}_R(\hat{\sigma}) \]
  \[ \| \text{Tr}_R(\hat{\rho}) - \text{Tr}_R(\hat{\sigma}) \| = \max_{\hat{V}_A} \left| \text{Tr} [\text{Tr}_R(\hat{\rho} - \hat{\sigma}) \hat{V}_A] \right| \]
  \[ = \max_{\hat{V}_A} \left| \text{Tr} [(\hat{\rho} - \hat{\sigma})(\hat{V}_A \otimes \hat{1}_R)] \right| \leq \max_{\hat{U}_{AR}} \left| \text{Tr} [(\hat{\rho} - \hat{\sigma}) \hat{U}_{AR}] \right| \]
  \[ = \| \hat{\rho} - \hat{\sigma} \| \]
Measurements and quantum operations

Any measurement has a description in terms of a quantum operation.

We may apply rules and bounds for quantum operations to measurements.
Monotonicity of trace distance and measurements

The equality is always achieved by the orthogonal measurement on a basis diagonalizing \( \hat{\rho} - \hat{\sigma} \).

Total variation distance between the probabilities of the outcomes never exceeds the trace distance.

\[
\sum_j |p_{\rho}(j) - p_{\sigma}(j)| = \sum_j \lambda_j
\]

\[
2 \| \hat{\rho} - \hat{\sigma} \| \leq \frac{1}{2} \| \hat{\rho}_{cl} - \hat{\sigma}_{cl} \| = \frac{1}{2} \sum_j |p_{\rho}(j) - p_{\sigma}(j)|
\]
Minimum-error discrimination

\( \hat{\rho} \) or \( \hat{\sigma} \)

50% 50%

probability of error: \( p_{\text{err}} = \frac{1}{2} p_{\rho}(1) + \frac{1}{2} p_{\sigma}(0) \)

total variation distance:

\[
\frac{1}{2} \sum_{j=0,1} |p_{\rho}(j) - p_{\sigma}(j)| = \frac{1}{2} |1 - p_{\rho}(1) - p_{\sigma}(0)| + \frac{1}{2} |p_{\rho}(1) - [1 - p_{\sigma}(0)]| = 1 - 2p_{\text{err}}
\]

The minimum error probability:

\[
p_{\text{err}}^{(\text{min})} = \frac{1}{2} \left( 1 - \frac{1}{2} \|\hat{\rho} - \hat{\sigma}\| \right)
\]

An operational meaning of the trace distance
Discrimination between two pure states

\[ \frac{1}{2} \| \hat{\rho}_0 - \hat{\rho}_1 \| = \cos 2\theta = \sqrt{1 - s^2} \]

The inner product determines the distinguishability of two pure states.
Fidelity

\[ F(\hat{\rho}, \hat{\sigma}) \equiv \max |\langle \phi_\rho | \phi_\sigma \rangle|^2 \]

\[ \text{Tr}_R[|\phi_\rho\rangle\langle\phi_\rho|] = \hat{\rho} \quad \text{(purifications)} \]
\[ \text{Tr}_R[|\phi_\sigma\rangle\langle\phi_\sigma|] = \hat{\sigma} \]

\[ F(\hat{\rho}, \hat{\sigma}) = 1 \iff \hat{\rho} = \hat{\sigma} \quad F(\hat{\rho}, \hat{\sigma}) = 0 \iff \hat{\rho}\hat{\sigma} = 0 \]

\[ F(|\varphi\rangle\langle\varphi|, |\psi\rangle\langle\psi|) = |\langle \varphi | \psi \rangle|^2 \]

\[ F(\hat{\rho}, |\psi\rangle\langle\psi|) = \langle \psi | \hat{\rho} | \psi \rangle \]

**proof:**

\[ F = \max_{|u\rangle} |\text{Tr}_R[u A \langle \psi | \phi_\rho \rangle_{AR}]|^2 \]
\[ = \| A \langle \psi | \phi_\rho \rangle_{AR} \|^2 \]

**Operational meaning of the fidelity (to a pure state)**

\[ \begin{array}{c}
\hat{\rho} \\
\text{Is it } |\psi\rangle \text{?}
\end{array} \]

\[ \begin{array}{c}
F \\
YES \\
1 - F \\
NO
\end{array} \]
Fidelity

\[ F(\hat{\rho}, \hat{\sigma}) \equiv \max |\langle \phi_\rho | \phi_\sigma \rangle|^2 \]

\[ F(\hat{\rho}, \hat{\sigma}) = \| \sqrt{\hat{\rho}} \sqrt{\hat{\sigma}} \|^2 \]

Any purification can be written as

\[ |\phi_\rho \rangle = \sum_k \sqrt{\hat{\rho}} |k\rangle \otimes \hat{U}_R |k\rangle_R \]

\[ = \sum_k \sqrt{\rho} \hat{U}' |k\rangle \otimes |k\rangle_R \]

\[ F(\hat{\rho}, \hat{\sigma}) = \max _{\hat{U}, \hat{V}} \left| \sum_{kl} \langle k | \hat{U}^\dagger \sqrt{\rho} \sqrt{\sigma} \hat{V} |l\rangle \times R \langle k | l \rangle_R \right|^2 \]

\[ = \max _{\hat{U}, \hat{V}} \left| \text{Tr}(\hat{U}^\dagger \sqrt{\rho} \sqrt{\sigma} \hat{V}) \right|^2 \]

\[ = \max _{\hat{V}} \left| \text{Tr}(\sqrt{\rho} \sqrt{\sigma} \hat{V}) \right|^2 \]
Monotonicity of fidelity

\[ F(\hat{\rho}, \hat{\sigma}) \equiv \max |\langle \phi_\rho | \phi_\sigma \rangle|^2 = \| \sqrt{\hat{\rho}} \sqrt{\hat{\sigma}} \|^2 = \left( \text{Tr} \sqrt{\hat{\sigma}} \sqrt{\hat{\rho}} \sqrt{\hat{\sigma}} \right)^2 \]

\[ 1 - F(\hat{\rho}, \hat{\sigma}) \] is a measure of distinguishability. (not a distance)

Monotonicity

\[ F(\hat{\rho}, \hat{\sigma}) \leq F(\chi(\hat{\rho}), \chi(\hat{\sigma})) \]

- Attach an ancilla  
\[ \hat{\rho} \rightarrow \hat{\rho} \otimes \hat{\tau} \quad \hat{\sigma} \rightarrow \hat{\sigma} \otimes \hat{\tau} \]
\[ F(\hat{\rho} \otimes \hat{\tau}, \hat{\sigma} \otimes \hat{\tau}) = \| \sqrt{\hat{\rho}} \sqrt{\hat{\sigma}} \|^2 \| \tau \|^2 = F(\hat{\rho}, \hat{\sigma}) \]

- Apply a unitary  
\[ \hat{\rho} \rightarrow \hat{U} \hat{\rho} \hat{U}^\dagger \quad \hat{\sigma} \rightarrow \hat{U} \hat{\sigma} \hat{U}^\dagger \]
\[ F(\hat{U} \hat{\rho} \hat{U}^\dagger, \hat{U} \hat{\sigma} \hat{U}^\dagger) = \| \hat{U} \sqrt{\hat{\rho}} \sqrt{\hat{\sigma}} \hat{U}^\dagger \|^2 = \| \sqrt{\hat{\rho}} \sqrt{\hat{\sigma}} \|^2 = F(\hat{\rho}, \hat{\sigma}) \]

- Discard the ancilla  
\[ \hat{\rho} \rightarrow \text{Tr}_R(\hat{\rho}) \quad \hat{\sigma} \rightarrow \text{Tr}_R(\hat{\sigma}) \]

Choose purifications achieving the maximum

\[ F(\hat{\rho}, \hat{\sigma}) = |\langle \tilde{\phi}_\rho | \tilde{\phi}_\sigma \rangle|^2 \]

They are also purifications of \( \text{Tr}_R(\hat{\rho}), \text{Tr}_R(\hat{\sigma}) \)

\[ F(\text{Tr}_R(\hat{\rho}), \text{Tr}_R(\hat{\sigma})) \geq |\langle \tilde{\phi}_\rho | \tilde{\phi}_\sigma \rangle|^2 = F(\hat{\rho}, \hat{\sigma}) \]

\[ \hat{\rho} \]

\[ \text{Tr}_R(\hat{\rho}) \]

\[ R \]

\[ |\tilde{\phi}_\rho \rangle \]
Operational meaning of the fidelity?

\[ F(\hat{\rho}, \hat{\sigma}) \leq F(\hat{\rho}_{cl}, \hat{\sigma}_{cl}) = \left( \sum_j \sqrt{p_\rho(j)} \sqrt{p_\sigma(j)} \right)^2 \]

No clear operational meaning ...

The equality is always achieved by the orthogonal measurement on a basis “diagonalizing \( \sqrt{\hat{\rho}} / \sqrt{\hat{\sigma}} \).”

\[ \mathcal{H} = (\text{Ran } \hat{\sigma}) \oplus (\text{Ker } \hat{\sigma}) \]

Diagonalize the positive operator \( \hat{\sigma}^{-1/2} |\sqrt{\hat{\rho}} \sqrt{\hat{\sigma}}| \hat{\sigma}^{-1/2} \)

Proof:

\[ \sqrt{\mu_j} \hat{\sigma}^{1/2} |j\rangle = |\sqrt{\hat{\rho}} \sqrt{\hat{\sigma}}| \hat{\sigma}^{-1/2} |j\rangle \]

\[ \mu_j \langle j | \hat{\sigma} | j \rangle = \langle j | \hat{\sigma}^{-1/2} |\sqrt{\hat{\rho}} \sqrt{\hat{\sigma}}|^2 \hat{\sigma}^{-1/2} |j\rangle = \langle j | \hat{\rho} | j \rangle \]

\[ \sum_j \sqrt{\mu_j} \langle j | \hat{\sigma} | j \rangle = \sum_j \langle j | \hat{\sigma}^{1/2} |\sqrt{\hat{\rho}} \sqrt{\hat{\sigma}}| \hat{\sigma}^{-1/2} |j\rangle = \text{Tr} |\sqrt{\hat{\rho}} \sqrt{\hat{\sigma}}| = \sqrt{F(\hat{\rho}, \hat{\sigma})} \]
Fidelity

Multiplicativity

\[ F(\hat{\rho}_1 \otimes \hat{\rho}_2, \hat{\sigma}_1 \otimes \hat{\sigma}_2) = F(\hat{\rho}_1, \hat{\sigma}_1)F(\hat{\rho}_2, \hat{\sigma}_2) \]

Proof: \[ \| \sqrt{\hat{\rho}_1 \otimes \hat{\rho}_2} \sqrt{\hat{\sigma}_1 \otimes \hat{\sigma}_2} \|^2 = \| \sqrt{\hat{\rho}_1} \sqrt{\hat{\sigma}_1} \otimes \sqrt{\hat{\rho}_2} \sqrt{\hat{\sigma}_2} \|^2 \]
\[ = \| \sqrt{\hat{\rho}_1} \sqrt{\hat{\sigma}_1} \|^2 \times \| \sqrt{\hat{\rho}_2} \sqrt{\hat{\sigma}_2} \|^2 \]

This property is not shared by the trace distance.

Applications

Basic principle for a quantum cryptography scheme called B92 protocol.

\[ F(\langle \phi | \phi \rangle, \langle \psi | \psi \rangle) \leq F(\chi(\langle \phi | \phi \rangle), \chi(\langle \psi | \psi \rangle)) \]
\[ = F(\langle \phi | \phi \rangle, \langle \psi | \psi \rangle)F(\hat{\rho}, \hat{\sigma}) \]
\[ |\langle \phi | \psi \rangle|^2 [1 - F(\hat{\rho}, \hat{\sigma})] \leq 0 \]

\[ |\langle \phi | \psi \rangle| > 0 \quad \Rightarrow \quad \hat{\rho} = \hat{\sigma} \]

Basic principle for a quantum cryptography scheme called B92 protocol.

\[ \begin{cases} \rho = |\phi \rangle \langle \phi | \\ \sigma = |\psi \rangle \langle \psi | \end{cases} \quad \Rightarrow \quad \langle \phi | \psi \rangle = 0, 1 \]

No-cloning theorem
Fidelity and trace distance

\[ 1 - \sqrt{F(\hat{\rho}, \hat{\sigma})} \leq \frac{1}{2} \| \hat{\rho} - \hat{\sigma} \| \leq \sqrt{1 - F(\hat{\rho}, \hat{\sigma})} \]

Proof:

There exists a measurement that preserves the fidelity:

\[ \sqrt{F(\hat{\rho}, \hat{\sigma})} = \sum_j \sqrt{p_\rho(j)} \sqrt{p_\sigma(j)} \]

\[ \frac{1}{2} \| \hat{\rho} - \hat{\sigma} \| \geq \frac{1}{2} \sum_j |p_\rho(j) - p_\sigma(j)| \]

\[ = \frac{1}{2} \sum_j \left| \sqrt{p_\rho(j)} - \sqrt{p_\sigma(j)} \right| \left( \sqrt{p_\rho(j)} + \sqrt{p_\sigma(j)} \right) \]

\[ \geq \frac{1}{2} \sum_j \left| \sqrt{p_\rho(j)} - \sqrt{p_\sigma(j)} \right|^2 = 1 - \sum_j \sqrt{p_\rho(j)} \sqrt{p_\sigma(j)} \]

\[ = 1 - \sqrt{F(\hat{\rho}, \hat{\sigma})} \]
Fidelity and trace distance

\[ 1 - \sqrt{F(\hat{\rho}, \hat{\sigma})} \leq \frac{1}{2} \| \hat{\rho} - \hat{\sigma} \| \leq \sqrt{1 - F(\hat{\rho}, \hat{\sigma})} \]

Proof:

There exists a pair of purifications satisfying

\[ F(\hat{\rho}, \hat{\sigma}) = |\langle \tilde{\phi}_\rho | \tilde{\phi}_\sigma \rangle|^2 \equiv s^2 \]

\[ \frac{1}{2} \left\| |\tilde{\phi}_\rho \rangle \langle \tilde{\phi}_\rho | - |\tilde{\phi}_\sigma \rangle \langle \tilde{\phi}_\sigma | \right\| = \sqrt{1 - s^2} = \sqrt{1 - F(\hat{\rho}, \hat{\sigma})} \]

Consider the quantum operation of discarding the subsystem used for purifying.

\[ |\tilde{\phi}_\rho \rangle \rightarrow \hat{\rho} \]
\[ |\tilde{\phi}_\sigma \rangle \rightarrow \hat{\sigma} \]

\[ \frac{1}{2} \left\| |\tilde{\phi}_\rho \rangle \langle \tilde{\phi}_\rho | - |\tilde{\phi}_\sigma \rangle \langle \tilde{\phi}_\sigma | \right\| \geq \frac{1}{2} \| \hat{\rho}_0 - \hat{\rho}_1 \| \]
5. Communication resources

Classical channel
Quantum channel
Entanglement
  How does the state evolve under LOCC?
  Properties of maximally entangled states
  Bell basis
Quantum dense coding
Quantum teleportation
  Entanglement swapping
Resource conversion protocols and bounds
Classical channel

Ideal classical channel: faithful transfer of any signal chosen from \( d \) symbols

Parallel use of channels

\[
\begin{align*}
0 & \quad \quad \quad 0 \\
1 & \quad \quad \quad 1 \\
a & \quad \quad \quad a \\
b & \quad \quad \quad b \\
c & \quad \quad \quad c \\
0a & \quad \quad \quad 0a \\
0b & \quad \quad \quad 0b \\
0c & \quad \quad \quad 0c \\
1a & \quad \quad \quad 1a \\
1b & \quad \quad \quad 1b \\
1c & \quad \quad \quad 1c
\end{align*}
\]

\( d \)-symbol ideal classical channel
\( d' \)-symbol ideal classical channel

Measure of usefulness

\( d \)-symbol ideal classical channel \( \rightarrow \) \( (\log d) \) bits

Additive for ideal channels
Quantum channel

\[ \alpha |0\rangle + \beta |1\rangle \]

Ideal quantum channel: faithful transfer of any state of an $d$-level system (Hilbert space of dimension $d$)

Parallel use of channels

\( (dd') \)-level system

Measure of usefulness

d-level ideal quantum channel \( \rightarrow \) \((\log d)\) qubits

Additive for ideal channels
Can classical channels substitute a quantum channel?

**NO** (with no other resources)

Suppose that it was possible …

- Any size of classical channel
- Classical info can be copied
- The same procedure should result in the same state.

This amounts to the cloning of unknown quantum states, which is forbidden.
Can a quantum channel substitute a classical channel?

Of course yes.

But not so bizarre (with no other resources).

**n-qubit ideal quantum channel can only substitute a n-bit classical channel.**

(Holevo bound)

Suppose that transfer of an d-level system can convey any signal from s symbols faithfully.

\[ j = 1, 2, \ldots, s \]

\[ \dim \mathcal{H} = d \]

Recall that any measurement must be described by a POVM.

\[ \text{Tr} \left( \hat{F}_j \hat{\rho}_j \right) = 1 \quad \sum_{j' = 1}^{s} \hat{F}_{j'} \leq \hat{1} \]

\[ s = \sum_{j=1}^{s} \text{Tr} \left( \hat{F}_j \hat{\rho}_j \right) \leq \sum_{j=1}^{s} \text{Tr} \left( \hat{F}_j \hat{1} \right) = \text{Tr} \left( \sum_{j=1}^{s} \hat{F}_j \right) \leq \text{Tr} \hat{1} = d \]
Difference between quantum and classical channels

We have seen that a quantum channel is more powerful than a classical channel.

Can we pin down what is missing in a classical channel?

I’ve already bought a classical channel, but now I want to use a quantum channel. Do I have to buy the quantum channel?

Oh, you can buy this optional package for a cheaper price, and upgrade the classical channel to a quantum channel!
Operational definition of entanglement

“Correlations that cannot be created over classical channels”

**LOCC**: Local operations and classical communication

Alice has a subsystem A, and Bob has a subsystem B.

Operations (including measurements) on a local subsystem are allowed.

Communication between Alice and Bob only uses classical channels.

Separable states: The states that can be created under LOCC from scratch.

Entangled states: The states that cannot be created under LOCC from scratch.
Entangled states and separable states

\[ |\phi\rangle_A \otimes |\psi\rangle_B \quad \sum_k \alpha_k |\phi_k\rangle_A \otimes |\psi_k\rangle_B \]

Separable states \quad \text{Entangled states}

Are there any procedure to distinguish between the two classes?

\[ \rightarrow \text{Schmidt decomposition} \quad |\Phi\rangle_{AB} = \sum_{i=1}^{s} \sqrt{p_i} |a_i\rangle_A |b_i\rangle_B \]

Schmidt number

Number of nonzero coefficients in Schmidt decomposition = The rank of the marginal density operators

\{p_j\} : The eigenvalues of the marginal density operators (the same for A and B)

Symmetry between A and B

\[ \hat{\rho}_A, \hat{\rho}_B \] The same set of eigenvalues

\[ s = \text{Rank}(\hat{\rho}_A) = \text{Rank}(\hat{\rho}_B) \]

Separable states \quad Schmidt number = 1 \quad p_1 = 1

Entangled states \quad Schmidt number > 1 \quad p_1 \geq p_2 > 0
How does the state evolve under LOCC?

Any LOCC procedure can be made a sequential one:

Alice applies local operations
Alice communicates to Bob
Bob applies local operations
Bob communicates to Alice
Alice …..

When Alice operates

outcome \( j \)

|\( \psi \rangle_{AB} \) \( \sim \) \( \hat{\rho} \)

Probability \( p_j > 0 \)

|\( \psi_j \rangle_{AB} \) \( \sim \) \( \hat{\rho}_j \)

\[ \sum_j p_j \hat{\rho}_j = \hat{\rho} \]

\( \hat{\rho} \geq p_j \hat{\rho}_j \)

Ran(\( \hat{\rho} \)) \supset Ran(\( \hat{\rho}_j \))

Rank(\( \hat{\rho} \)) \geq Rank(\( \hat{\rho}_j \))

Schmidt number never increases under LOCC (even probabilistically)

Schmidt number >1 \( \rightarrow \) Impossible to create under LOCC

If a concave functional \( S \) only depends on the eigenvalues,

\[ S(\hat{\rho}) \geq \sum_j p_j S(\hat{\rho}_j) \]

Any such functional of the marginal density operator (e.g., von Neumann entropy) is monotone decreasing under LOCC on average.
Maximally entangled states (MES) "ideal" entangled states

\[ \sum_{k=1}^{d} \frac{1}{\sqrt{d}} |k\rangle_A \otimes |k\rangle_B \]

An MES with Schmidt number \( d \)

Putting two MESs together

MES with Schmidt number \( d \)

\[ \left( \sum_{j=1}^{d} \frac{1}{\sqrt{d}} |j\rangle_A \otimes |j\rangle_B \right) \otimes \left( \sum_{k=1}^{d'} \frac{1}{\sqrt{d'}} |k\rangle_{A'} \otimes |k\rangle_{B'} \right) = \sum_{j,k} \frac{1}{\sqrt{dd'}} |j\rangle_A |\rangle_{A'} \otimes |j\rangle_B |\rangle_{B'} \]

MES with Schmidt number \( dd' \)

Measure of entanglement

MES with Schmidt number \( d \) \( \xrightarrow{\text{(log } d\text{) ebits}} \)

\[ |\Phi_+\rangle = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) \quad 1\text{ ebit} \]

Additive for MESs
Ebits and bits are mutually exclusive

Schmidt number never increases under LOCC.

Classical channels cannot increase (ideal) entanglement.

The outcome can be correctly predicted with probability at least $1/d$.

Transfer of $s$ symbols

Success probability 1

Transfer of $s$ symbols

Success probability $1/d$

$s \leq d$
Ebits and bits are mutually exclusive

Schmidt number never increases under LOCC.

Classical channels cannot increase (ideal) entanglement.

d-symbol ideal classical channel
The outcome can be correctly predicted with probability at least $1/d$.

Transfer of 3 symbols
♥ ♦ ♠
Which is on my mind?

Success probability 1
That must be ♥!!

Transfer of 3 symbols
♥ ♦ ♠
Which is on my mind?

Success probability 1/2
That must be ♥!!

Entanglement cannot assist (ideal) classical channels
Resource conversion protocols

Conversion to ebits

Entanglement sharing
- 1 qubit $\rightarrow$ 1 ebit

Conversion to bits

Quantum dense coding
- 1 qubit + 1 ebit $\rightarrow$ 2 bits

Conversion to qubits

Quantum teleportation
- 2 bits + 1 ebit $\rightarrow$ 1 qubit

Restrictions
- bits alone $\rightarrow$ no ebits
- ebits alone $\rightarrow$ no bits
- 1 qubit alone $\rightarrow$ no more than 1 bit
Properties of maximally entangled states $|\Phi\rangle_{AB} = \sum_{k=1}^{d} \frac{1}{\sqrt{d}} |k\rangle_A \otimes |k\rangle_B$

(I) Convertibility via local unitary $|\Phi'\rangle_{AB} = (\mathbf{1}_A \otimes \hat{U}_B) |\Phi\rangle_{AB}$

(II) Pair of local states (relative states) $\frac{1}{\sqrt{d}} |\phi\rangle_A = B \langle \phi^* | |\Phi\rangle_{AB} \rightarrow |\phi^*\rangle_B = \sum_k \alpha_k |k\rangle_B$

B measurement $p = 1/d$

(III) Pair of local operations $(\hat{M}_A \otimes \mathbf{1}_B) |\Phi\rangle_{AB} = (\mathbf{1}_A \otimes \hat{M}_B^T) |\Phi\rangle_{AB}$

(IV) Orthonormal basis (Bell basis) $\langle \Phi_j | \Phi_k \rangle = \delta_{jk} \ (j, k = 1, \ldots d^2)$

There exists an orthonormal basis composed of MESs.
Bell basis for a pair of qubits

\(d = 2\)

\( |\Phi_+\rangle = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) \)

\( |\Phi_-\rangle = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B) = \hat{Z}_B |\Phi_+\rangle \)

\( |\Psi_+\rangle = \frac{1}{\sqrt{2}} (|1\rangle_A |0\rangle_B + |0\rangle_A |1\rangle_B) = \hat{X}_A |\Phi_+\rangle \)

\( |\Psi_-\rangle = \frac{1}{\sqrt{2}} (|1\rangle_A |0\rangle_B - |0\rangle_A |1\rangle_B) = (\hat{X}_A \otimes \hat{Z}_B) |\Phi_+\rangle \)

\( \hat{X} \equiv \hat{\sigma}_x = |1\rangle\langle 0| + |0\rangle\langle 1| \)

\( \hat{Z} \equiv \hat{\sigma}_z = |0\rangle\langle 0| - |1\rangle\langle 1| \)
Bell basis

$$\beta \equiv \exp(2\pi i / d) \quad (\beta^d = 1, \beta^{-1} = \bar{\beta})$$

Basis \( \{ |0\rangle, |1\rangle, \ldots, |d-1\rangle \} \quad (|d\rangle \equiv |0\rangle) \)

$$\hat{X} \equiv \sum_{j=0}^{d-1} |j+1\rangle \langle j| \quad \hat{Z} \equiv \sum_{j=0}^{d-1} \beta^j |j\rangle \langle j| \quad \text{(Unitary)}$$

$$\hat{X}^T = \hat{X}^{-1} \quad \hat{Z}^T = \hat{Z}$$

$$\hat{Z}^d = \hat{X}^d = \hat{1} \quad \text{Eigenvalues: } 1, \beta, \beta^2, \ldots, \beta^{d-1}$$

$$\hat{Z} \hat{X} = \beta \hat{X} \hat{Z} \quad \hat{Z}^m \hat{X}^l = \beta^{lm} \hat{X}^l \hat{Z}^m$$

$$|\Phi_{0,0}\rangle \equiv \frac{1}{\sqrt{d}} \sum_{k=1}^{d} |k\rangle_A \otimes |k\rangle_B$$

$$(\hat{X}_A \otimes \hat{X}_B)|\Phi_{0,0}\rangle = |\Phi_{0,0}\rangle$$

$$(\hat{Z}_A \otimes \hat{Z}_B^{-1})|\Phi_{0,0}\rangle = |\Phi_{0,0}\rangle$$

Bell basis: \( \{ |\Phi_{l,m}\rangle \} \quad (l = 0, 1, \ldots, d-1; \ m = 0, 1, \ldots, d-1) \)

$$|\Phi_{l,m}\rangle \equiv (\hat{X}_A^l \otimes \hat{Z}_B^m)|\Phi_{0,0}\rangle$$

$$\langle \hat{X}_A \otimes \hat{X}_B |\Phi_{l,m}\rangle = \beta^{-m} |\Phi_{l,m}\rangle$$

$$\langle \hat{Z}_A \otimes \hat{Z}_B^{-1} |\Phi_{l,m}\rangle = \beta^l |\Phi_{l,m}\rangle$$

$$\begin{align*}
\end{align*} \quad \text{All states are orthogonal.}$$
**Quantum dense coding**

1 qubit + 1 ebit → 2 bits
n qubits + n ebits → 2n bits

(Dimension d) + (Schmidt number d) → $(d^2)$ symbols

**MES**

Convertibility via local unitary

**Orthonormal basis (Bell basis)**

$d^2$ symbols $(l, m)$

$\hat{U}_{A}^{(l,m)} \rightarrow |\Phi_{l,m}\rangle$

| $\Phi_{l,m}$ Measurement on the Bell basis |
| (Bell measurement) → $(l, m)$ |
Creating entanglement by nonlocal measurement

\[ |\Phi_{0,0}\rangle_{AB} \otimes |\Phi_{0,0}\rangle_{A'C} = \sum_{j,k} \frac{1}{\sqrt{d^2}} |jk\rangle_{AA'} \otimes |jk\rangle_{BC} \]

measurement

\[ |\Psi\rangle_{AA'} \leftarrow \begin{cases} A \hline A' \end{cases} \rightarrow \begin{cases} B \hline C \end{cases} \]

(More precisely, obtaining an outcome corresponding to a POVM element \( \mu |\Psi\rangle \langle \Psi| \))

Relative state of \( |\Psi\rangle_{AA'} \)

\[ \begin{pmatrix} |\Psi\rangle_{AA'} \\ |\Psi^*\rangle_{BC} \end{pmatrix} \]

The same entanglement
\[ \hat{\rho}_A \equiv \text{Tr}_{A'} |\Psi\rangle \langle \Psi| \]
\[ \hat{\rho}_B \equiv \text{Tr}_{C} |\Psi^*\rangle \langle \Psi^*| \]

\[ A \langle j | \hat{\rho}_A | j' \rangle_A = B \langle j | \hat{\rho}_B | j' \rangle_B \]
\( \hat{\rho}_A, \hat{\rho}_B \) : the same set of eigenvalues

When \( |\Psi\rangle_{AA'} \) is an entangled state, (e.g., Bell measurement)

Initially no entanglement

entangled

Such a measurement cannot be implemented over LOCC.
Entanglement swapping

\[ |\Phi_{0,0}\rangle_B \otimes |\Phi_{0,0}\rangle_{A'C} = \sum_{j,k} \frac{1}{\sqrt{d^2}} |jk\rangle_{AA'} \otimes |jk\rangle_{BC} \]

Bell measurement

\[ |\Phi_{0,0}\rangle_{AA'} \]

A maximally entangled state

It should be written as

\[ \left( \hat{U}_B^{(l,m)} \right)^{-1} |\Phi_{0,0}\rangle_{BC} \]
Entanglement swapping

Classical channel (2\log d \ bits)

\[ (l, m) \quad \longrightarrow \quad \hat{U}_B^{(l, m)} \]

Bell measurement

Final state

\[ |\Phi_{0,0}\rangle_{BC} \]

It is possible to creating entanglement over two subsystems without letting them directly interacted to each other.
Entanglement swapping

\[(l, m) \xrightarrow{\text{Classical channel (2log d bits)}} \hat{U}^{(l, m)}_B\]

Bell measurement

- \(|\phi\rangle_{A'}\)
- \((\hat{U}^{(l, m)}_B)^{-1}|\Phi_{0,0}\rangle_{BC}\)

Measurement

- |\phi^*\rangle_C

|\Phi_{0,0}\rangle_{BC}
Quantum teleportation

1 ebit + 2 bit $\rightarrow$ 1 qubit

n ebits + 2n bits $\rightarrow$ n qubits

$(d^2$ symbols) + (Schmidt number d) $\rightarrow$ (Dimension d)

Classical channel ($2\log d$ bits) $\rightarrow \hat{U}^{(l,m)}_B$

Bell measurement

$|\phi\rangle_{A'}$

$|\phi\rangle_B$
Quantum teleportation

If the cost of classical communication is neglected …

One can reserve the quantum channel by storing a quantum state.
One can use a quantum channel in the opposite direction.
A convenient way of quantum error correction (failure → retry).

Noisy quantum channel

|\phi\rangle \rightarrow \tilde{\rho} \rightarrow |\phi\rangle

Recovering
Failure → no recovery.

Noisy quantum channel

Noisy entanglement

Recovering
Resource conversion protocols

Conversion to ebits
Entanglement sharing
1 qubit $\rightarrow$ 1 ebit

Conversion to bits
Quantum dense coding
1 qubit + 1 ebit $\rightarrow$ 2 bits

Conversion to qubits
Quantum teleportation
2 bits + 1 ebit $\rightarrow$ 1 qubit

Restrictions
- bits alone $\rightarrow$ no ebits
- ebits alone $\rightarrow$ no bits
- 1 qubit alone $\rightarrow$ no more than 1 bit
Resource conversion protocols and bounds

We can do the following…

Conversion to ebits

Entanglement sharing

1 qubit $\rightarrow$ 1 ebit

$(\Delta q, \Delta e, \Delta c) = (-1, 1, 0)$

Conversion to bits

Quantum dense coding

1 qubit + 1 ebit $\rightarrow$ 2 bits

$(\Delta q, \Delta e, \Delta c) = (-1, -1, 2)$

Conversion to qubits

Quantum teleportation

2 bits + 1 ebit $\rightarrow$ 1 qubit

$(\Delta q, \Delta e, \Delta c) = (1, -1, -2)$
Resource conversion protocols and bounds

We can do the following...

**Restrictions**

- bits alone → no ebits
- ebits alone → no bits
- 1 qubit alone → no more than 1 bit

• The red region should be unreachable.

• From a point above the blue plane, the red region is accessible through ‘Teleportation’ and ‘Dense coding.’

• The region above the blue plane should be unreachable.
Resource conversion protocols and bounds

We can do the following...

Restrictions

- bits alone → no ebits
- ebits alone → no bits
- 1 qubit alone → no more than 1 bit

- The red region should be unreachable.
- From a point above the blue plane, the red region is accessible through ‘Dense coding’ and ‘Entanglement sharing.’

The region above the blue plane should be unreachable.

\[ \Delta c + \Delta q + \Delta e \leq 0 \]
Resource conversion protocols and bounds

We can do the following…

Conversion to ebits

Entanglement sharing (ES)

\[ (\Delta q, \Delta e, \Delta c) = (-1, 1, 0) \]

Conversion to bits

Quantum dense coding (QD)

\[ (\Delta q, \Delta e, \Delta c) = (-1, -1, 2) \]

Conversion to qubits

Quantum teleportation (QT)

\[ (\Delta q, \Delta e, \Delta c) = (1, -1, -2) \]

We cannot violate the following …

Entanglement alone never assists classical channels

+ QD, QT

\[ \Delta c + 2\Delta q \leq 0 \]

Classical channels alone cannot increase entanglement

+ QT, ES

\[ \Delta e + \Delta q \leq 0 \]

1-qubit channel alone can convey no more than 1 classical bit

+ ES, QD

\[ \Delta q + \Delta e + \Delta c \leq 0 \]
Resource conversion protocols and bounds

Teleportation

\[ \Delta q \]

\[ \Delta c \]

\[ \Delta e \]

\[ \Delta e + \Delta q \leq 0 \]

\[ \Delta c + 2\Delta q \leq 0 \]

Dense coding

\[ \Delta c + \Delta q + \Delta e \leq 0 \]

Entanglement sharing
Resource conversion protocols

Conversion to ebits
- Entanglement sharing
  - 1 qubit \rightarrow 1 ebit

Conversion to bits
- Quantum dense coding
  - 1 qubit + 1 ebit \rightarrow 2 bits

Conversion to qubits
- Quantum teleportation
  - 2 bits + 1 ebit \rightarrow 1 qubit

Restrictions
- bits alone \rightarrow no ebits
- ebits alone \rightarrow no bits
- 1 qubit alone \rightarrow no more than 1 bit