Compressibility of general mixed-state signals

Masato Koashi
SOKEN (The Graduate University for Advanced Studies, Japan)

- Introduction
- Quantum data compression
  - Fixed length, asymptotically faithful compression
  - Blind vs visible scenario
  - Variable length, faithful compression
- Quantum teleportation
- Structure of general mixed-state signals

A fundamental question in the information theory

Quantifying the randomness of a probabilistic source

source → ABCDBCDBCABCDBC….

source → AAAAAABAAAAACA….

↓ Compression (coding)

01001001...

↓ Decompression (decoding)

AAAAAABAAAAACA….

How many bits (per letter) are required to describe the sequence?

Fixed-length, asymptotically faithful coding

Characterization of a source

$\{p_i, i\}$

probability ↗ ↖ letter

source → A or B

$p_A = 1/3$
$p_B = 2/3$

A sequence of n letters independently drawn from the source

BABBAABBBBABBAB (n-i.i.d. sequence)

↓ block coding

L_n bits (fixed-length)
010010010

↓ decoding

BABBAABBBBABBAB

With success probability $1 - e_n$

Requirement: "Asymptotically faithful" $\lim_{n\to\infty} e_n = 0$
(vanishing errors in large block length limit)

Compression rate $\equiv \lim_{n\to\infty} L_n/n$ (How many bits are used per letter?)

Minimum of this rate: optimal compression rate $R_{\rm opt}^{\rm AF}$

AEP (Asymptotic equipartition property)

Source $\{p_i, i\}$ n-i.i.d. sequence $i_1 i_2 i_3 \ldots i_n$

A particular sequence $i_1 i_2 i_3 \ldots i_n (\equiv \lambda)$ appears with probability p_λ

$$p_\lambda = p_{i_1} p_{i_2} p_{i_3} \cdots p_{i_n}$$

Consider a statistical variable $X = -\frac{1}{n}\log_2 p_\lambda = \frac{1}{n}\sum_{k=1}^{n} -\log_2 p_{i_k}$

This is the average of $-\log_2 p_i$ over n samples

Law of large numbers

When n is large, $X \sim \langle X \rangle = \sum_i -p_i \log_2 p_i \equiv H(\{p_i\})$

In almost all cases, we encounter a sequence with $p_\lambda \sim 2^{-nH}$

↓

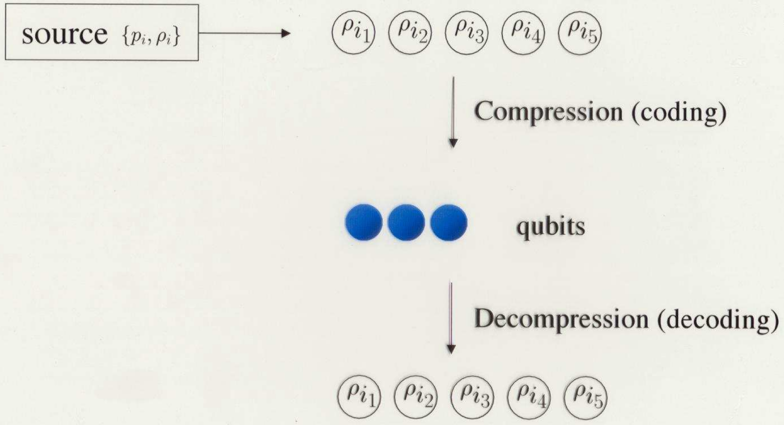
Evenly distributed $\sim 2^{nH}$ (typical) sequences
(other atypical sequences appear with negligible probability)

↓

optimal compression rate $R_{\rm opt}^{\rm AF} = H(\{p_i\})$ bits (per letter)

A fundamental question in quantum information theory

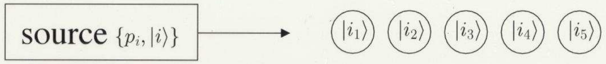
How many qubits (per system) are required to reproduce the state?



How to quantify quantum information?

Quantum data compression (pure states)

Schumacher, PRA **51**, 2738 (1995).



$$\rho \equiv \sum_i p_i |i\rangle\langle i| \xrightarrow[\text{diagonalize}]{} \sum_j q_j |b_j\rangle\langle b_j|$$

Typical subspace

spanned by $|b_{i_1}\rangle|b_{i_2}\rangle|b_{i_3}\rangle \cdots |b_{i_n}\rangle$ with $X \equiv \frac{1}{n}\sum_{k=1}^{n} -\log_2 q_{i_k} \sim H(\{q_i\})$

# of such states
(dimension) $\sim 2^{nH(\{q_i\})}$

$H(\{q_j\}) = -\mathrm{Tr}[\rho \log_2 \rho] \equiv S(\rho)$
von Neumann etntropy

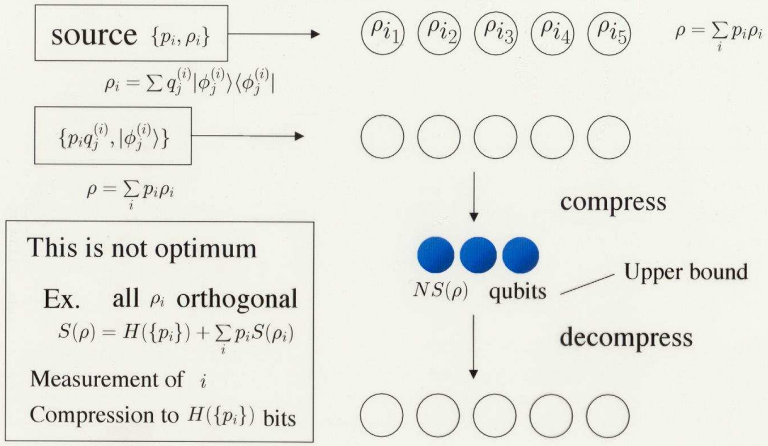
Transfer to
$nS(\rho)$ qubits

Atypical subspace

Probability of finding the state in this subspace is negligible when $n \to \infty$

optimal compression rate $R_{\mathrm{opt}}^{\mathrm{AF}} = S(\rho)$ qubits (per letter)

Quantum data compression (mixed states)



$\rho = \sum_i p_i \rho_i$

$\rho_i = \sum q_j^{(i)} |\phi_j^{(i)}\rangle\langle\phi_j^{(i)}|$

$\rho = \sum_i p_i \rho_i$

This is not optimum

Ex. all ρ_i orthogonal
$S(\rho) = H(\{p_i\}) + \sum_i p_i S(\rho_i)$

Measurement of i

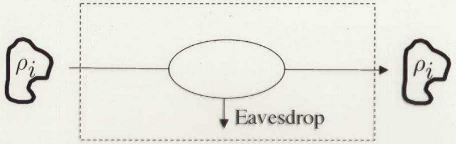
Compression to $H(\{p_i\})$ bits

Lower bound $I_{\mathrm{LH}} = S(\rho) - \sum_i p_i S(\rho_i)$ =classical information accessible through the ensemble

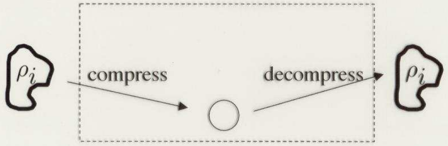
Levitin-Holevo function

The operations that do not disturb $\{\rho_i\}$

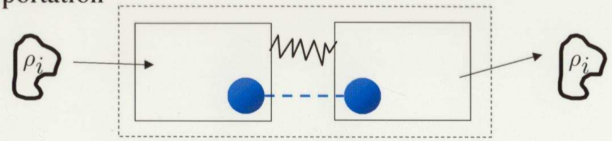
Quantum cryptography



Compression

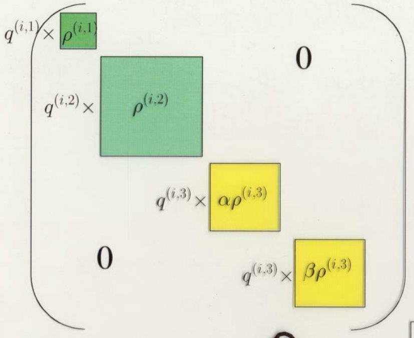


Teleportation



Principle

$\rho_i =$



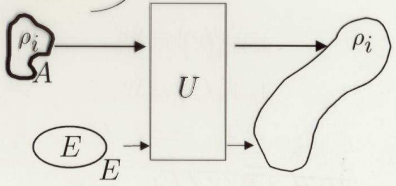
$$\rho_{\mathrm{J}}^{(i,3)} = \rho^{(i,3)}$$

$$\rho_{\mathrm{K}}^{(i,3)} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$$

$$\mathcal{H} = \sum_l \mathcal{H}_{\mathrm{J}}^{(l)} \otimes \mathcal{H}_{\mathrm{K}}^{(l)}$$

$$\rho_i = \sum_l q^{(i,l)} \rho_{\mathrm{J}}^{(i,l)} \otimes \rho_{\mathrm{K}}^{(l)}$$

$$U = \sum_l 1_{\mathrm{J}}^{(l)} \otimes U_{\mathrm{KE}}^{(l)}$$



source $\{p_i, \rho_i\}$

$$\mathcal{H} = \sum_l \mathcal{H}_{\mathrm{J}}^{(l)} \otimes \mathcal{H}_{\mathrm{K}}^{(l)}$$

$$\rho_i = \sum_l q^{(i,l)} \rho_{\mathrm{J}}^{(i,l)} \otimes \rho_{\mathrm{K}}^{(l)}$$

$$\rho = \sum_i p_i \rho_i = \sum_l p^{(l)} \rho_{\mathrm{J}}^{(l)} \otimes \rho_{\mathrm{K}}^{(l)}$$

$$S(\rho) = H(\{p^{(l)}\}) + \sum_l p^{(l)} S(\rho_{\mathrm{J}}^{(l)}) + \sum_l p^{(l)} S(\rho_{\mathrm{K}}^{(l)})$$
$$\equiv I_{\mathrm{C}} + I_{\mathrm{NC}} + I_{\mathrm{R}}$$

System K is redundant.

$$\rho_i = \sum_l q^{(i,l)} \rho_{\mathrm{J}}^{(i,l)} \otimes \rho_{\mathrm{K}}^{(l)} \quad \overset{\text{freely}}{\Longleftrightarrow} \quad \sigma_i \equiv \sum_l q^{(i,l)} \rho_{\mathrm{J}}^{(i,l)}$$

Compressibility of $\{p_i, \rho_i\}$ is equal to that of $\{p_i, \sigma_i\}$

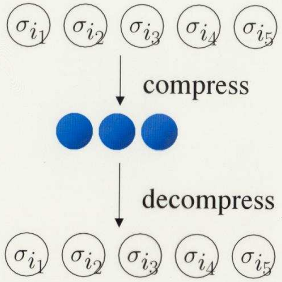
$\{p_i, \rho_i\}$ can be compressed into

$$S(\sigma) = H(\{p^{(l)}\}) + \sum_l p^{(l)} S(\rho_{\mathrm{J}}^{(l)})$$
$$= I_{\mathrm{C}} + I_{\mathrm{NC}}$$

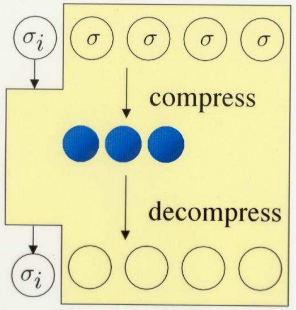
(qubits per letter)

Can we do better?

source $\{p_i, \sigma_i\}$



Consider any asymptotically faithful compression scheme.



This operation preserves

$$\sigma_i \equiv \sum_l q^{(i,l)} \rho_{\mathrm{J}}^{(i,l)}$$
$$\downarrow$$
$$U = \sum_l \mathbf{1}_{\mathrm{J}}^{(l)} \otimes U_{\mathrm{E}}^{(l)}$$

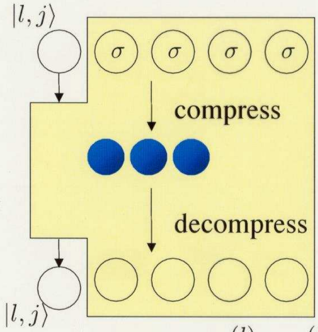
Replace the source with orthogonal pure states

$$\sigma = \sum_l p^{(l)} \rho_{\mathrm{J}}^{(l)}$$

$$\rho_{\mathrm{J}}^{(l)} = \sum_j q_j^{(l)} |l, j\rangle\langle l, j|$$

$$\boxed{\{p^{(l)} q_j^{(l)}, |l, j\rangle\}}$$

Averaged state is still σ



$$U = \sum_l \mathbf{1}_{\mathrm{J}}^{(l)} \otimes U_{\mathrm{E}}^{(l)}$$

Transfer of letter (l, j)

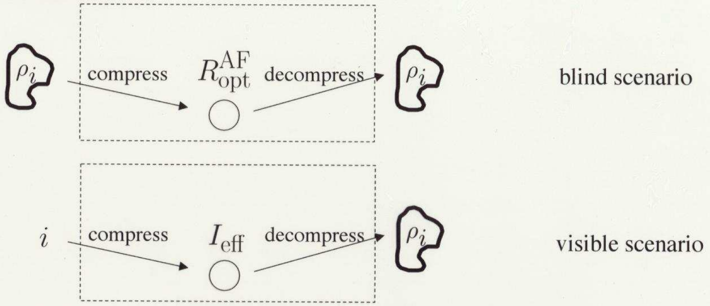
$S(\sigma)$ bits of information can be sent.
↓
$S(\sigma)$ qubits are optimum.

$$\boxed{R_{\mathrm{opt}}^{\mathrm{AF}} = I_{\mathrm{C}} + I_{\mathrm{NC}}}$$

$$S(\rho) = \sum_l p^{(l)} \left[-\log_2 p^{(l)} + S(\rho_{\mathrm{J}}^{(l)}) + S(\rho_{\mathrm{K}}^{(l)}) \right]$$
$$\equiv \boxed{I_{\mathrm{C}} + I_{\mathrm{NC}}} + I_{\mathrm{R}}$$

Koashi and Imoto, PRL **87**, 017902 (2001).

Information defect



$$I_{\rm eff} \geq I_{\rm LH} \equiv S(\hat{\rho}) - \sum_i p_i S(\hat{\rho}_i)$$

$$\Delta_{\rm b-v} \equiv R_{\rm opt}^{\rm AF} - I_{\rm eff} \leq I_{\rm C} + I_{\rm NC} - I_{\rm LH}$$
$$= \sum_i p_i S(\hat{\rho}_i) - \sum_l p^{(l)} S(\hat{\rho}_{\rm K}^{(l)}) = \sum_i p_i S(\hat{\sigma}_i)$$

$\Delta_{\rm b-v} = 0$ if $\{\sigma_i\}$ are all pure.

$\Delta_{\rm b-v}$ can be nonzero even when $\{\sigma_i\}$ commute.
(classical data)

Variable-length, faithful coding

source $\{p_i, i\}$ $\quad i \xrightarrow[\text{coding}]{} \underset{L \text{ bits}}{010010} \xrightarrow[\text{decoding}]{} i$ with success probability 1.

(length can be varied)

$R_{\rm opt}^{(1)}$: Minimum of expected length $\langle L \rangle$

n-i.i.d. sequence $\xrightarrow[\text{block coding}]{} \underset{L_n \text{ bits}}{01001100010} \xrightarrow[\text{decoding}]{}$

$R_{\rm opt}^{(n)}$: Minimum of expected length per letter, $\langle L_n \rangle / n$

By definition, $R_{\rm opt}^{(1)} \geq R_{\rm opt}^{(2)} \geq \cdots \geq R_{\rm opt}^{(n)} \geq \cdots$

optimal compression rate $\quad R_{\rm opt}^{(\infty)} \equiv \lim_{n\to\infty} R_{\rm opt}^{(n)}$

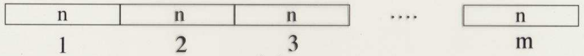
Variable-length, faithful coding $\quad R_{\rm opt}^{(\infty)}$

more powerful more strict

v.s.

Fixed-length, asymptotically faithful coding $\quad R_{\rm opt}^{\rm AF}$

Repeating n-block variable-length coding for m times



Expected length per letter is $R_{\rm opt}^{(n)}$

Law of large numbers

When m becomes large, length per letter is almost always close to $R_{\rm opt}^{(n)}$

$\downarrow$

Fixed-length, asymptotically faithful coding with rate $R_{\rm opt}^{(n)}$

$$R_{\rm opt}^{(n)} \geq R_{\rm opt}^{\rm AF}$$

$$R_{\rm opt}^{(\infty)} \geq R_{\rm opt}^{\rm AF}$$

Classical case

source $\{p_i, i\}$

$$H(\{p_i\}) \leq R_{\rm opt}^{(1)} \leq H(\{p_i\}) + 1$$

Applying this to the n-i.i.d. case,

$$nH(\{p_i\}) \leq nR_{\rm opt}^{(n)} \leq nH(\{p_i\}) + 1$$

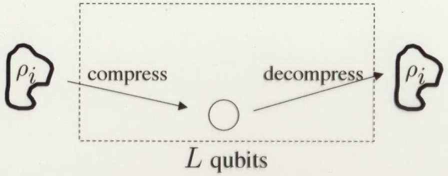
$$H(\{p_i\}) \leq R_{\rm opt}^{(n)} \leq H(\{p_i\}) + 1/n,$$

$$R_{\rm opt}^{(\infty)} = H(\{p_i\}) = R_{\rm opt}^{\rm AF}$$

Compressibility is the same for the two scenarios.

Quantum case

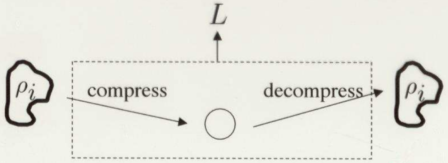
source $\mathcal{E} = \{p_i, \hat{\rho}_i\}$



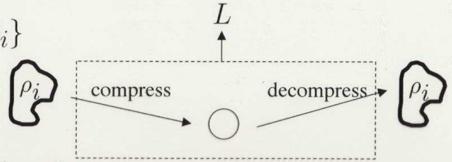
What do we mean by saying, “only L qubits are used this time.” ?

“OK, the rest of N-L qubits can be used in any other independent task.”

Information of L comes out of the compression machine.



$\mathcal{E} = \{p_i, \hat{\rho}_i\}$



$$\mathcal{H}_{\rm A} = \bigoplus_l \mathcal{H}_{\rm J}^{(l)} \otimes \mathcal{H}_{\rm K}^{(l)} \qquad \hat{U} = \bigoplus_l \hat{1}_{\rm J}^{(l)} \otimes \hat{U}_{\rm KE}^{(l)}$$

$$\hat{\rho}_i = \bigoplus_l p^{(i,l)} \hat{\rho}_{\rm J}^{(i,l)} \otimes \hat{\rho}_{\rm K}^{(l)} \qquad \hat{\rho} = \bigoplus_l p^{(l)} \hat{\rho}_{\rm J}^{(l)} \otimes \hat{\rho}_{\rm K}^{(l)},$$

Consider another source $\mathcal{E}' = \{q_\lambda, \hat{\sigma}_\lambda\}$ $\quad \lambda \equiv (l, j)$

$$q_\lambda = (\dim \mathcal{H}_{\rm J}^{(l)})^{-1} p^{(l)} \qquad \hat{\sigma}_\lambda = |a_j\rangle_{\rm J}^{(l)}{}_{\rm J}^{(l)}\langle a_j| \otimes \hat{\rho}_{\rm K}^{(l)} \qquad \hat{\sigma} = \bigoplus_l p^{(l)} (\dim \mathcal{H}_{\rm J}^{(l)})^{-1} \hat{1}_{\rm J}^{(l)} \otimes \hat{\rho}_{\rm K}^{(l)}$$

The form $\hat{U} = \bigoplus_l \hat{1}_{\rm J}^{(l)} \otimes \hat{U}_{\rm KE}^{(l)}$ implies that it can faithfully compress the new source with the same expected length.

$$R_{\rm opt}^{(1)}(\mathcal{E}) \geq R_{\rm opt}^{(1)}(\mathcal{E}')$$

$$\begin{aligned} R_{\rm opt}^{(1)}(\mathcal{E}') \geq R_{\rm opt}^{\rm AF}(\mathcal{E}') &= H(\{p^{(l)}\}) + \sum_l p^{(l)} \log_2 \dim \mathcal{H}_{\rm J}^{(l)} \\ &= I_{\rm C}(\mathcal{E}) + D_{\rm NC}(\mathcal{E}) \end{aligned}$$

Quantum case

source $\mathcal{E} = \{p_i, \hat{\rho}_i\}$

$$I_{\rm C}(\mathcal{E}) + D_{\rm NC}(\mathcal{E}) \leq R_{\rm opt}^{(1)}(\mathcal{E}) \leq I_{\rm C}(\mathcal{E}) + D_{\rm NC}(\mathcal{E}) + 2$$

Applying this to the n-i.i.d. case,

$$I_{\rm C}(\mathcal{E}) + D_{\rm NC}(\mathcal{E}) \leq R_{\rm opt}^{(n)}(\mathcal{E}) \leq I_{\rm C}(\mathcal{E}) + D_{\rm NC}(\mathcal{E}) + 2/n$$

$$R_{\rm opt}^{(\infty)}(\mathcal{E}) = I_{\rm C}(\mathcal{E}) + D_{\rm NC}(\mathcal{E})$$

The quantum part ($\mathcal{H}_{\rm J}^{(l)}$) is incompressible.

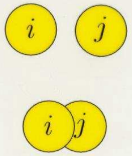
$$R_{\rm opt}^{\rm AF}(\mathcal{E}) = I_{\rm C}(\mathcal{E}) + I_{\rm NC}(\mathcal{E})$$

$$R_{\rm opt}^{(\infty)} - R_{\rm opt}^{\rm AF} = \sum_l p^{(l)} [\log_2 \dim \mathcal{H}_{\rm J}^{(l)} - S(\hat{\rho}_{\rm J}^{(l)})]$$

$R_{\rm opt}^{(\infty)} = R_{\rm opt}^{\rm AF}$ if all $\hat{\rho}_i$ commute.

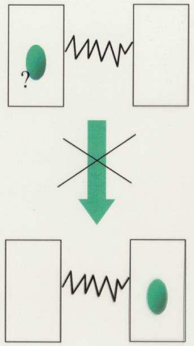
Nature of information and compressibility

Information	classical $([\hat{\rho}_i, \hat{\rho}_j] = 0)$	quantum
pure $(S(\hat{\sigma}_i) = 0)$	$R_{\rm opt}^{(\infty)} = R_{\rm opt}^{\rm AF} = I_{\rm eff}$	$R_{\rm opt}^{(\infty)} \geq R_{\rm opt}^{\rm AF} = I_{\rm eff}$
mixed	$R_{\rm opt}^{(\infty)} = R_{\rm opt}^{\rm AF} \geq I_{\rm eff}$	$R_{\rm opt}^{(\infty)} \geq R_{\rm opt}^{\rm AF} \geq I_{\rm eff}$

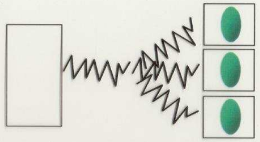


$R_{\rm opt}^{(\infty)}$	$R_{\rm opt}^{\rm AF}$	$I_{\rm eff}$
variable-length faithful	fixed length asymptotically faithful	
blind		visible

Transfer of quantum states through a classical channel

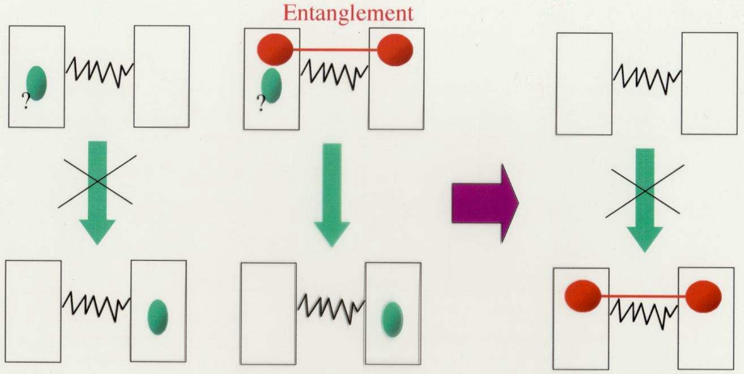


Why?



Wave function could be measured.

Signals could be sent faster than light...



Quantum teleportation

Entanglement can never be increased over a classical channel

$d = 2$

One qubit in a completely unknown state

Teleported via one ebit

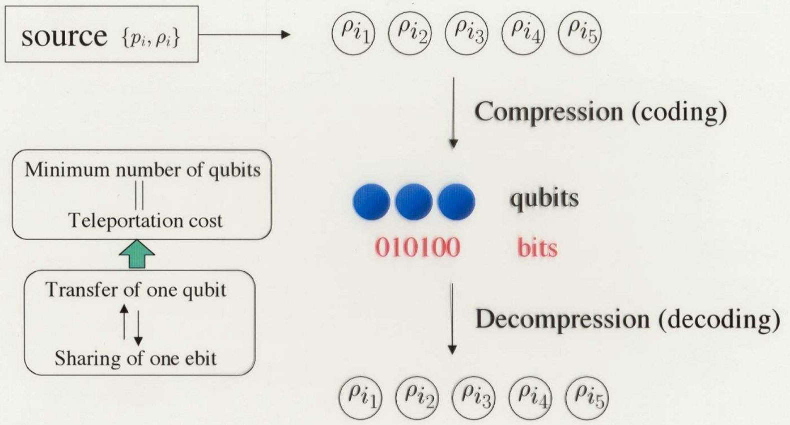
Bell pair $\frac{1}{\sqrt{2}}(|\leftrightarrow\rangle_A|\leftrightarrow\rangle_B + |\updownarrow\rangle_A|\updownarrow\rangle_B)$

Open question

How many ebits are required to teleport partially known state?

source $\{p_i, \rho_i\}$

A fundamental question in quantum information theory



source $\{p_i, \rho_i\}$ → ρ_{i_1} ρ_{i_2} ρ_{i_3} ρ_{i_4} ρ_{i_5}

Compression (coding)

qubits

010100 bits

Decompression (decoding)

ρ_{i_1} ρ_{i_2} ρ_{i_3} ρ_{i_4} ρ_{i_5}

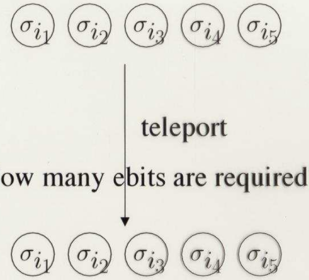
Minimum number of qubits
||
Teleportation cost

Transfer of one qubit
↑↓
Sharing of one ebit

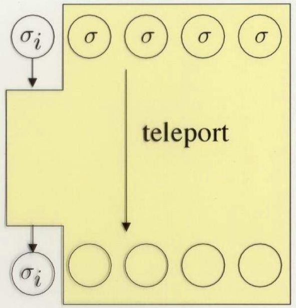
Barnum, Hayden, Jozsa, Winter,
Proc. R. Soc. Lond. A **457**, 2019 (2001) (quant-ph/0011072)

Teleportation cost

source $\{p_i, \sigma_i\}$



How many ebits are required?



This operation preserves

$$\sigma_i \equiv \sum_l q^{(i,l)} \rho_{\mathrm{J}}^{(i,l)}$$

$$\downarrow$$

$$U = \sum_l \mathbf{1}_{\mathrm{J}}^{(l)} \otimes U_{\mathrm{E}}^{(l)}$$

Consider any asymptotically faithful teleportation scheme.

Replace the source with an entangled state ρ_{AB}

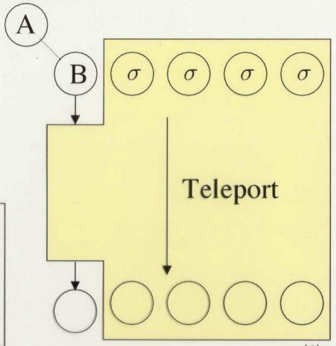
$$\sigma = \sum_l p^{(l)} \rho_{\mathrm{J}}^{(l)}$$

$$\rho_{\mathrm{J}}^{(l)} = \sum_j q_j^{(l)} |l, j\rangle\langle l, j|$$

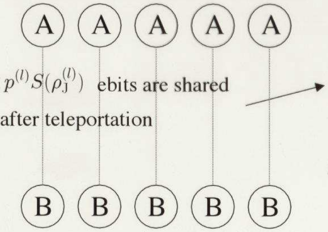
$$|\Psi^{(l)}\rangle_{AB} = \sum_j \sqrt{q_j^{(l)}} |l, j\rangle_A |l, j\rangle_B$$

$$\rho_{AB} = \sum_l p^{(l)} |\Psi^{(l)}\rangle_{AB} \langle \Psi^{(l)}|$$

ρ_{AB}
- $\sum_l p^{(l)} S(\rho_{\mathrm{J}}^{(l)})$ ebits
- Marginal state is σ
- Entangled in each $\mathcal{H}_{\mathrm{J}}^{(l)}$
- Mixture over index l



$$U = \sum_l \mathbf{1}_{\mathrm{J}}^{(l)} \otimes U_{\mathrm{E}}^{(l)}$$



$\sum_l p^{(l)} S(\rho_{\mathrm{J}}^{(l)})$ ebits are shared after teleportation → At least $\sum_l p^{(l)} S(\rho_{\mathrm{J}}^{(l)})$ ebits are required to teleport

$$S(\rho) = \sum_l p^{(l)} \left[-\log_2 p^{(l)} + S(\rho_{\mathrm{J}}^{(l)}) + S(\rho_{\mathrm{K}}^{(l)}) \right]$$

$$\equiv I_{\mathrm{C}} + \boxed{I_{\mathrm{NC}}} + I_{\mathrm{R}}$$

---

source $\{p_i, \rho_i\}$

$$\mathcal{H} = \sum_l \mathcal{H}_{\mathrm{J}}^{(l)} \otimes \mathcal{H}_{\mathrm{K}}^{(l)}$$

$$\rho = \sum_i p_i \rho_i = \sum_l p^{(l)} \rho_{\mathrm{J}}^{(l)} \otimes \rho_{\mathrm{K}}^{(l)}$$

$$\rho_i = \sum_l q^{(i,l)} \rho_{\mathrm{J}}^{(i,l)} \otimes \rho_{\mathrm{K}}^{(l)}$$

$$S(\rho) = \underbrace{H(\{p^{(l)}\})}_{\#\text{ of bits}} + \underbrace{\sum_l p^{(l)} S(\rho_{\mathrm{J}}^{(l)})}_{\#\text{ of qubits}} + \underbrace{\sum_l p^{(l)} S(\rho_{\mathrm{K}}^{(l)})}_{\text{redundant}}$$

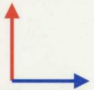
Koashi and Imoto, quant-ph/0104001.

Structure of quantum information

$$\mathcal{H} = \sum_l \mathcal{H}_{\mathrm{J}}^{(l)} \otimes \mathcal{H}_{\mathrm{K}}^{(l)}$$

$$\rho_i = \sum_l q^{(i,l)} \rho_{\mathrm{J}}^{(i,l)} \otimes \rho_{\mathrm{K}}^{(l)}$$

$$S(\rho) = H(\{p^{(l)}\}) + \sum_l p^{(l)} S(\rho_{\mathrm{J}}^{(l)}) + \sum_l p^{(l)} S(\rho_{\mathrm{K}}^{(l)})$$

2 pure states	Mixed states $\{p_i, \rho_i\}$	Extracting information	Stored in	Teleportation	
 orthogonal	l	intact	bits	free	classical
 nonorthogonal	$\mathcal{H}_{\mathrm{J}}^{(l)}$	disturbed	qubits	Consume ebits	nonclassical
 identical	$\mathcal{H}_{\mathrm{K}}^{(l)}$	no information	free	free	redundant