Introduzione alla teoria dell'informazione classica e quantistica

Sviluppo del teorema di codifica sorgente di Shannon e di Schumacher nella teoria dell'informazione

Simone Bisogno, Francesco Mogavero

18 Settembre 2019

Università degli Studi di Salerno
Dipartimento di informatica

Informazione quantistica e computazione quantistica

Contenuti

Contenuti

Contenuti sezione

Entropia classica

Entropia classica

Fissato $t \geq 1$, sia X una sorgente (o registro) che emette caratteri

- Alfabeto sorgente: $\mathcal{X} = \{x_1, x_2, \ldots, x_t\}$,
- Distribuzione di probabilità:
  $P(\mathcal{X}) = \{p(x_1), p(x_2), \ldots, p(x_t)\}$

L'entropia della sorgente X (o *entropia di Shannon*) è

$$H(X) \stackrel{\text{def}}{=} - \sum_{\substack{i=1 \\ p(x_i)>0}}^{t} p(x_i) \log_2 p(x_i).$$

$\forall$ sorgente X risulta $H(X) \in [0, log_2 t]$

- $H(X) = 0 \iff X$ è sorgente costante
- $H(X) = log_2 t \iff$ X sorgente uniforme

Contenuti

Contenuti sezione

Il problema della codifica sorgente

Obiettivo: minimizzare # bit per codifica sequenze di M sorgenti

Siano $t \geq 1$, X variabile aleatoria

$$X \stackrel{\text{def}}{=} \begin{pmatrix} x_1, & x_2, & \dots & , x_t \\ p(x_1), & p(x_2), & \dots, & p(x_t) \end{pmatrix} : t \geq 1$$

Consideriamo la sequenza di M caratteri $w = X_1 X_2 \dots X_M$

- $X_i = X, \forall i \in [1, M] \implies w = X \dots X$

Funzioni di codifica e decodifica

$$\begin{aligned} c\colon \mathcal{X}^M &\to \{0,1\}^N \\ w &\mapsto c(w), \end{aligned} \tag{1}$$

$$\begin{aligned} d\colon \{0,1\}^N &\to \mathcal{X}^M \\ \gamma &\mapsto d(\gamma). \end{aligned} \tag{2}$$

Correttezza: $\forall w \in \mathcal{X}^M \;\; d(c(w)) = w$

Per rappresentare tutti i possibili messaggi, $N = \lceil M \log_2 |\mathcal{X}| \rceil$ bit

N riducibile a $M \cdot H(X)$

- viene introdotto un errore di codifica-decodifica
- risparmio sostanziale
- si adatta alla casualità della sorgente
- se $N < M \cdot H(X)$, la probabilità di errore cresce

Sequenze ϵ-tipiche

Definiamo $\mathcal{T}_{M,\epsilon}(X) \subseteq \mathcal{X}^M$ di sequenze ϵ-tipiche emissibili dalla sorgente

$$\mathcal{T}_{M,\epsilon}(X) \stackrel{\text{def}}{=} \{w \in \mathcal{X}^M : 2^{-M(H(X)+\epsilon)} \leq p(w) \leq 2^{-M(H(X)-\epsilon)}\}$$

da cui consegue la definizione equivalente

$$\mathcal{T}_{M,\epsilon}(X) \stackrel{\text{def}}{=} \{w \in \mathcal{X}^M : \left|\frac{1}{M} \sum_{i=1}^{M} \log_2 \frac{1}{p(x_i)} - H(X)\right| \leq \epsilon\}$$

Proprietà $\mathcal{T}_{M,\epsilon}(X)$

1. Sia $\epsilon \geq 0$. $\forall \delta > 0$, M sufficientemente grande

$$P(\mathcal{T}_{M,\epsilon}(X)) \stackrel{\text{def}}{=} \sum_{w \in \mathcal{T}_{M,\epsilon}(X)} p(w) \geq 1 - \delta$$

o equivalentemente

$$P(\overline{\mathcal{T}_{M,\epsilon}(X)}) \stackrel{\text{def}}{=} \sum_{w \notin \mathcal{T}_{M,\epsilon}(X)} p(w) \leq \delta.$$

- Al crescere di M, anche la probabilità di avere sequenze emesse dalle M sorgenti cresce

2. Siano $\epsilon > 0, \delta > 0$. Per M sufficientemente grande

$$(1-\delta)2^{M(H(X)-\epsilon)} \leq |\mathcal{T}_{M,\epsilon}(X)| \leq 2^{M(H(X)+\epsilon)}$$

Per minimizzare N, fissiamo $\epsilon > 0, \delta > 0$

- dalla proprietà 1), $\exists M_0 \leq M$

Si costruisce c in modo che, considerato nel sottodominio delle sequenze ϵ-tipiche, debba essere iniettivo

- non è più garantita la condizione di correttezza dell'algoritmo di codifica $d(c(w)) = w$

Legame tra M, ϵ e δ

Il numero delle sorgenti emittenti M e i parametri ϵ e δ sono legati tra loro

- fissati due, il terzo è univocamente determinato

ϵ rappresenta l'ampiezza dell'insieme delle sequenze ϵ-tipiche

- la cardinalità di $\mathcal{T}_{M,\epsilon}(X)$ è direttamente proporzionale

δ rappresenta la propabilità di errore massima tollerata

Si considera un canale *ideale*: nessun errore esterno

L'errore di codifica-decodifica è legato esclusivamente alla generazione di sequenze non ϵ-tipiche:

$$P(e_{cd}(c)) \leq P\left(\overline{\mathcal{T}_{M,\epsilon}(X)}\right)$$

$P(e_{cd}(c))$ è limitata superiormente da δ

Servono $M(H(x) + \epsilon) \simeq MH(X)$ bit per codificare in maniera iniettiva $\mathcal{T}_{M,\epsilon}(X)$

Dimostrazione dell'enunciato

Correttezza $\forall \epsilon > 0, \delta > 0, M > M_0$, bastano $MH(X)$ bit per codificare $\mathcal{T}_{M,\epsilon}(X)$ mantenendo la probabilità d'errore inferiore a δ

Ottimalità fissato ϵ come sopra, se c codifica impiegando meno di $MH(X)$ bit, per $M \to \infty \implies P(e_{cd}(c)) \to 1$

Algoritmo di codifica, definizione formale

Scelti $\epsilon > 0, \delta > 0, M > M_0$, si sceglie un numero minimo di bit per codifica carattere $\mathcal{A} \geq H(X) + 2\epsilon$

- $N \stackrel{\text{def}}{=} \lfloor M \cdot \mathcal{A} \rfloor > M(H(X) + \epsilon)$
- $|\mathcal{T}_{M,\epsilon}(X)| \leq 2^{M(H(X)+\epsilon)} \implies |\mathcal{T}_{M,\epsilon}(X)| \leq 2^N$
  - bastano N bit per codificare una sequenza ϵ-tipica

Si costruisce c in modo che a ogni sequenza ϵ-tipica corrisponda una codifica binaria univoca

Si considera $\mathcal{G}_M : |\mathcal{G}_M| \leq 2^N$

- $\mathcal{G}_M \stackrel{\text{def}}{=} \{w \in \mathcal{X}^M : d(c(w)) = w\}$

Per costruzione di c, $\mathcal{T}_{M,\epsilon}(X) \subseteq \mathcal{G}_M$

Probabilità errore codifica-decodifica:

$$P(e_{cd}(c)) \stackrel{\text{def}}{=} P(\overline{\mathcal{G}_M}) = \sum_{w \notin \mathcal{G}_M} p(w)$$

$$\begin{aligned}
&\mathcal{T}_{M,\epsilon}(X) \subseteq \mathcal{G}_M \implies \\
&P(\mathcal{G}_M) \geq P(\mathcal{T}_{M,\epsilon}(X)) \implies \\
&P(\overline{\mathcal{G}_M}) \leq P(\overline{\mathcal{T}_{M,\epsilon}(X)}) \leq \delta \implies \\
&P(\overline{\mathcal{G}_M}) \leq \delta \quad \square
\end{aligned}$$

Scelto ϵ, se si vuole mantenere un errore c-d al più δ si deve considerare un M sufficientemente grande

Ottimalità

Si consideri, invece, $\mathcal{A} \leq H(X) + \epsilon$

Sia $c : \mathcal{X}^M \supseteq \mathcal{S} \to \{0,1\}^N$ iniettiva

- $\forall \epsilon > 0, M > 0, \mathcal{G}_M \subseteq (\Sigma^M \setminus \mathcal{T}_{M,\epsilon}(X)) \cup (\mathcal{G}_M \cap \mathcal{T}_{M,\epsilon}(X))$

Di conseguenza

$$
\begin{aligned}
&P(\mathcal{G}_M) = \\
&= \textstyle\sum_{w \in \mathcal{G}_M} p(w) = \\
&= \textstyle\sum_{w = a_1 \ldots a_M \in \mathcal{G}_M} p(a_1) \ldots p(a_M) \leq \\
&\leq (1 - \textstyle\sum_{w = a_1 \ldots a_M \in \mathcal{T}_{M,\epsilon}(X)} p(a_1) \ldots p(a_M)) + \\
&(\textstyle\sum_{w = a_1 \ldots a_M \in \mathcal{G}_M \cap \mathcal{T}_{M,\epsilon}(X)} p(a_1) \ldots p(a_M)).
\end{aligned}
$$

Dal secondo termine e dalla definizione di $\mathcal{T}_{M,\epsilon}(X)$ segue

$$\begin{aligned}
&\sum_{w=a_1\ldots a_M\in\mathcal{G}_M\cap\mathcal{T}_{M,\epsilon}(X)} p(a_1)\ldots p(a_M) \leq \\
&\leq \sum_{w=a_1\ldots a_M\in\mathcal{G}_M\cap\mathcal{T}_{M,\epsilon}(X)} 2^{-M(H(X)-\epsilon)} \leq \\
&\leq \sum_{w=a_1\ldots a_M\in\mathcal{G}_M} 2^{-M(H(X)-\epsilon)} = \\
&= 2^{-M(H(X)-\epsilon)}|\mathcal{G}_M|.
\end{aligned}$$

Torniamo alla definizione di $P(\mathcal{G}_M)$

$$P(\mathcal{G}_M) \leq (1 - \sum_{w=a_1\ldots a_M\in\mathcal{T}_{M,\epsilon}(X)} p(a_1)\ldots p(a_M)) + 2^{-M(H(X)-\epsilon)}|\mathcal{G}_M|.$$

Poiché, per definizione, $|\mathcal{G}_M| \leq 2^N$, $N = \lfloor M\cdot\mathcal{A}\rfloor$, e per scelta di $\mathcal{A}$, segue

$$|\mathcal{G}_M| \leq 2^N = 2^{\lfloor M\cdot\mathcal{A}\rfloor} \leq 2^{M(H(X)-\epsilon)}$$

Al crescere di M, osserviamo l'espressione data di $P(\mathcal{G}_M)$

Da $|\mathcal{G}_M| \leq 2^{M(H(X)-\epsilon)}$ si ottiene

$$\lim_{M\to\infty} 2^{-M(H(X)-\epsilon)}|\mathcal{G}_M| = 0,$$

dunque

$$\begin{aligned}
&\lim_{M\to\infty} P(\mathcal{G}_M) \leq \\
&\leq \lim_{M\to\infty}(1 - \sum_{w=a_1\ldots a_M\in\mathcal{T}_{M,\epsilon}(X)} p(a_1)\ldots p(a_M)) = \\
&= 1 - \lim_{M\to\infty} \sum_{w=a_1\ldots a_M\in\mathcal{T}_{M,\epsilon}(X)} p(a_1)\ldots p(a_M))
\end{aligned}$$

Al crescere di M, le sequenze emesse sono quasi certamente ϵ-tipiche, per cui

$$\lim_{M\to\infty} P(\mathcal{G}_M) = 0 \quad \square$$

Conclusioni Th. codifica sorgente

Codificare con un numero di bit utilizzato $N < H(X) + \epsilon$ non è sufficiente per codificare un qualunque sottoinsieme di sequenze emissibili mantenendo limitata la probabiltà di errore di codifica-decodifica

$N = H(X)$ valore ideale per avere una codifica con errore limitato minimizzando la quantità di bit necessaria

Contenuti

Contenuti sezione

Entropia quantistica

Generalizzazione entropia di Shannon agli stati quantistici

Entropia quantistica di von Neumann:

$$S(\rho) = -\operatorname{Tr}(\rho \log_2 \rho) = -\sum_x \lambda_x \log_2 \lambda_x$$

Entropia quantistica, alcune proprietà

- non negativa
- $\rho \in \mathcal{H}_d$, $S(\rho) \leq \log_2 d$
- ρ matrice densità, P distribuzione di probabilità: $S(\rho) = -\operatorname{Tr}(\rho \log_2 \rho) = H(P)$

Misura ed entropia

Le misure alterano l'entropia

- misura proiettiva: $\rho' = \sum_i P_i \rho P_i$

Teorema: *la misura proiettiva aumenta l'entropia*

Contenuti

Contenuti sezione

Il problema quantistico della codifica sorgente

B. Schumacher, *Quantum coding* (1995)

Γ, Π algoritmi di codifica e decodifica

- Γ codifica sequenze prodotte da M stati quantistici di M sistemi quantistici i.i.d. in N qubit
- Π riporta gli N qubit negli M stati iniziali

Unità d'informazione: stato puro di un sistema quantistico sorgente

Dato l'ensemble $\{p_x, | \psi_x \rangle\}$, una sorgente quantistica è una matrice densità ρ definita in $\mathcal{H}_{Sorg}$

$$\rho \stackrel{\text{def}}{=} \sum_x p_x | \psi_x \rangle\langle \psi_x | .$$

Nel th. di Schumacher consideriamo $\rho_i, i \in [1, M]$ sorgenti uguali

1. $$\rho_1 = \cdots = \rho_M$$
2. $$\underbrace{| \psi \rangle \otimes \cdots \otimes | \psi \rangle}_{M \text{ volte}} = | \psi \rangle^{\otimes M}.$$
3. $$\rho^{\otimes M} = \underbrace{\rho \otimes \cdots \otimes \rho}_{M \text{volte}}.$$

Funzioni di codifica e decodifica

$$\Gamma : \mathcal{H}_{Sorg}^{\otimes M} \to \mathcal{H}^{\otimes N} \qquad | \psi^{\otimes M} \rangle \mapsto \Gamma(| \psi^{\otimes M} \rangle) \tag{3}$$

$$\Pi : \mathcal{H}^{\otimes N} \to \mathcal{H}_{Sorg}^{\otimes M} \qquad | \gamma \rangle^{\otimes N} \mapsto \Pi(| \gamma \rangle^{\otimes N}). \tag{4}$$

Si considerano Γ e Π come porte logiche

- Γ: M registri in input in parallelo, ognuno di essi preparato in accordo allo stato ρ_i
- Π: N registri in input, inversa di Γ

Per codificare $\mathcal{H}_{Sorg}^{M}$ in qubit in maniera *iniettiva* e *invertibile* sono necessari almeno $N \geq \lceil M \log_2 dim(H_\rho) \rceil$ qubit

- si può abbassare N a circa $M\, S(\rho)$
- viene introdotto una probabilità di errore c-d *arbitrariamente* bassa
  - nel caso quantistico, si parla di abbassamento della *fedeltà* del canale quantistico $\Phi = \Pi \circ \Gamma$
- serve un sottospazio ϵ-tipico di $\mathcal{H}_{Sorg}^{\otimes M}$ relativo a ρ
- Γ trasforma iniettivamente ogni sequenza del sottospazio ϵ-tipico in una successione di N qubit distinta

Obiettivo

Si dimostra che è possibile definire un algoritmo Γ che usi $N \simeq M\,S(\rho)$ qubit

- perdita di fedeltà limitata superiormente da un parametro δ

Se Γ usa meno di $M\,S(\rho)$ qubit, al crescere di M la fedeltà tende a zero

Fedeltà tra due stati quantistici

Dati $\rho, \sigma \in \mathcal{H}$, la fedeltà $F(\rho, \sigma)$ tra ρ e σ si esprime come

$$F(\rho, \sigma) \stackrel{\text{def}}{=} \|\sqrt{\rho}\sqrt{\sigma}\| = \mathsf{Tr}\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}$$

Per alcuni autori,

$$F(\rho, \sigma) \stackrel{\text{def}}{=} \left(\mathsf{Tr}\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}\right)^2$$

Fedeltà tra due stati quantistici, proprietà

- $F(\rho, \sigma) = F(\sigma, \rho)$
- $0 \leq F(\rho, \sigma) \leq 1$
- $\rho = |\, \psi \bigtimes \psi \,| \implies F(|\, \psi \bigtimes \psi \,|, \sigma) = \langle\, \psi \,|\, \sigma \,|\, \psi \,\rangle$

Fedeltà di un canale

$\mathcal{H}_A, \mathcal{H}_B$, $\Phi : \mathcal{H}_A \to \mathcal{H}_B$

Φ è una matrice con $\dim \mathcal{H}_B$ righe e $\dim \mathcal{H}_A$ colonne

Condizioni sul canale Φ:

1. lineare completamente positiva
2. preserva la traccia

Fedeltà media di ensemble

Siano $\mathcal{H}_A = \mathcal{H}_B \stackrel{\text{def}}{=} \mathcal{H}_1$, $\Phi : \mathcal{H}_1 \to \mathcal{H}_1$ canale quantistico, ρ_1 uno stato di $\mathcal{H}_1$, $\{p_i, |\, \psi_i \,\rangle\} \ : i \in \{1 \dots k\}$ ensemble di ρ_1

$$\hat{F}(\Phi, \rho_1) \stackrel{\text{def}}{=} \sum_{i=1}^{k} p_i \, F(|\, \psi_i \,\rangle_1 \,,\ \Phi \mid \psi_i \,\rangle_1)$$

oppure, per la definizione di fedeltà per uno stato puro

$$\hat{F}(\Phi, \rho_1) = \sum_{i=1}^{k} \ p_i \, {}_1\langle\, \psi_i \mid \ \ [\Phi \mid \psi_i \,\rangle_1] \ \ \mid \psi_i \,\rangle_1$$

Dimostrazione dell'enunciato

La sorgente quantistica che emette un singolo stato è definita come la matrice densità ρ associata ad uno *Hilbert* $\mathcal{H}_{Sorg}$ e derivata dall'ensemble $\{p_x, | \psi_x \rangle\}$

$$\rho = \sum_x p_x | \psi_x \times \psi_x | .$$

Per semplicità, si diagonalizzi ρ:

$$\rho = \sum_{i=1}^{t} p_i | \psi_i \times \psi_i |$$

dove $t = dim(\mathcal{H}_{Sorg})$. In tal modo, gli autovettori di ψ_i sono una base ortogonale per lo spazio, mentre gli autovalori $\{p_i\}$ sono una distribuzione di probabilità classica

Dimostrazione dell'enunciato

La matrice densità associata alla sorgente che emette messaggi di M stati sorgente (un messaggio di lunghezza M) è

$$\rho^{\otimes M} = \underbrace{\rho \otimes \cdots \otimes \rho}_{M \text{ volte}}$$

- Il numero di autovettori di $\rho^{\otimes M}$ è t^M
  - $| \psi^{\otimes M} \rangle = | \psi \rangle_1 \otimes \ldots \otimes | \psi \rangle_M$, con $| \psi \rangle_i$ autovettore di ρ_i
- I cui autovalori sono
  - $\lambda_{|\psi^{\otimes M} \rangle} = \lambda_{|\psi \rangle_1} \cdot \ldots \cdot \lambda_{|\psi \rangle_M}$, con $\lambda_{|\psi \rangle_i}$ autovalore di ρ_i
  - $\lambda_{|\psi^{\otimes M} \rangle}$ probabilità che l'autovettore $| \psi^{\otimes M} \rangle$ venga trasmesso

Definizione del problema

Si intende realizzare una coppia di algoritmi

- Γ di codifica
- Π di decodifica

$$\begin{aligned} \Gamma &: \mathcal{H}_{Sorg}^{\otimes M} \to \mathcal{H}^{\otimes N} \\ &| \psi^{\otimes M} \rangle \mapsto \Gamma(| \psi^{\otimes M} \rangle) \end{aligned} \tag{5}$$

$$\begin{aligned} \Pi &: \mathcal{H}^{\otimes N} \to \mathcal{H}_{Sorg}^{\otimes M} \\ &| \gamma \rangle^{\otimes N} \mapsto \Pi(| \gamma \rangle^{\otimes N}) \end{aligned} \tag{6}$$

che minimizzino il numero di qubit usati mantenendo una fedeltà media d'ensemble accettabile

Γ e Π possono essere implementati come due porte logiche
La composizione $\Pi \cdot \Gamma$, associata all'applicazione dell'algoritmo di codifica e poi di decodifica, è un **canale di comunicazione quantistico di codifica-decodifica** $\Phi = \Pi \cdot \Gamma$

Dimostrazione dell'enunciato - Obiettivi

Soluzione basic

- Volendo rappresentare con un distinto stato di N qubit tutti i possibili messaggi di M stati, sono necessari almeno $N \geq \lceil M \cdot \log_2 \left(dim(\mathcal{H}_{Sorg}) \right) \rceil$ qubit

Teorema di Schumacher

- **Definisce un algoritmo di codifica** che abbassa il numero di qubit necessari fino a $N \simeq M \cdot S(\rho)$ con fedeltà media d'ensemble limitata inferiormente
- Con un numero di qubit $N < M \cdot S(\rho)$ la medesima fidelity, al crescere di M, si abbassa fino a 0 in **qualunque algoritmo** di codifica ideabile

Per raggiungere questo scopo **viene utilizzato** il *sottospazio* ϵ*-tipico* di $\mathcal{H}_{Sorg}^{\otimes M}$ relativo a ρ

Il sottospazio ϵ-tipico

Dati $\epsilon > 0$ ed $M \geq 1$, il sottospazio ϵ-*tipico* di $\mathcal{H}_{Sorg}^{\otimes M}$ relativo a ρ ha per *base* l'insieme degli autovettori di $\rho^{\otimes M}$ il cui autovalore $\lambda_{|\psi\rangle^{\otimes M}}$ soddisfa l'equazione

$$2^{-M(S(\rho)+\epsilon)} \leq \lambda \leq 2^{-M(S(\rho)-\epsilon)}$$

- $\mathcal{T}_{M,\epsilon}(\rho) \subseteq \mathcal{H}_{Sorg}^{\otimes M}$ il sottospazio ϵ-*tipico*
- $\{|v_1^{\otimes M}\rangle, \ldots, |v_l^{\otimes M}\rangle : l \geq 1\}$ i suoi vettori di base
- $\mathcal{P}_{M,\epsilon}(\rho) \stackrel{\text{def}}{=} |v_1^{\otimes M}\rangle\langle v_1^{\otimes M}| + \cdots + |v_l^{\otimes M}\rangle\langle v_l^{\otimes M}|$ è il proiettore a $\mathcal{T}_{M,\epsilon}(\rho)$

$\mathcal{T}_{M,\epsilon}(\rho)$ e $\overline{\mathcal{T}_{M,\epsilon}(\rho)}$ sono in somma diretta

Il sottospazio ϵ-*tipico*

Si cerca ora di stabilire:

1. **P($\mathcal{T}_{M,\epsilon}(\rho)$): la probabilità che un vettore w di $\rho^{\otimes M}$ sia in $\mathcal{T}_{M,\epsilon}(\rho)$**
2. La dimensione del sottospazio ϵ-*tipico* $dim(\mathcal{T}_{M,\epsilon}(\rho))$

Il sottospazio ϵ-*tipico* - Calcolo di $P(\mathcal{T}_{M,\epsilon}(\rho))$

Per calcolare il valore di $P(\mathcal{T}_{M,\epsilon}(\rho))$ si utilizzano alcuni risultati

- $\mathrm{Tr}\left(\mathcal{P}_{M,\epsilon}(\rho)\ \rho^{\otimes M}\right) = \sum_{|w\rangle^{\otimes M}=|w_1\rangle\otimes\cdots\otimes|w_M\rangle\in\mathcal{T}_{M,\epsilon}(\rho)} \lambda_w = \sum_{|w\rangle^{\otimes M}=|w_1\rangle\otimes\cdots\otimes|w_M\rangle\in\mathcal{T}_{M,\epsilon}(\rho)} p_{w_1}\cdots p_{w_M}$.

$$P(\mathcal{T}_{M,\epsilon}(\rho)) = \mathrm{Tr}\left(\mathcal{P}_{M,\epsilon}(\rho)\ \rho^{\otimes M}\right)$$

- Sia ρ una matrice densità e $P = \{p_1, \ldots, p_t\} : t \geq 1$ la distribuzione di probabilità classica associata a ρ. Risulta

$$S(\rho) = H(P)$$

Da ciò consegue che

- Ogni sorgente quantistica **è simile** a una sorgente classica $\mathcal{X}$ avente distribuzione di probabilità pari all'insieme degli autovalori di ρ

Il sottospazio ϵ-*tipico* - Calcolo di $P(\mathcal{T}_{M,\epsilon}(\rho))$

Sia X una sorgente classica simile a ρ

È possibile sfruttare anche nel caso quantistico alcune considerazioni legate ai concetti di entropia, di sorgente e di sottospazio tipico valevoli nel mondo classico

$$
\begin{aligned}
&P(\mathcal{T}_{M,\epsilon}(\rho)) = \mathsf{Tr}\left(\mathcal{P}_{M,\epsilon}(\rho)\ \rho^{\otimes M}\right) = \\
&\sum_{|\psi\ \rangle^{\otimes M} = |\psi_1\ \rangle \otimes \cdots \otimes |\psi_M\ \rangle \in \mathcal{T}_{M,\epsilon}(\rho)} p_{w_1} \cdots p_{w_M} = \\
&\sum_{w = w_1 \ldots w_M \in \mathcal{T}_{M,\epsilon}(X)} p_{w_1} \cdots p_{w_M} = \\
&P(\mathcal{T}_{M,\epsilon}(X))
\end{aligned}
$$

Il sottospazio ϵ-*tipico* - Calcolo di $P(\mathcal{T}_{M,\epsilon}(\rho))$

Dunque

$$P(\mathcal{T}_{M,\epsilon}(\rho)) = \mathrm{Tr}\left(\mathcal{P}_{M,\epsilon}(\rho)\ \rho^{\otimes M}\right) = P(\mathcal{T}_{M,\epsilon}(X))$$

Per quanto stabilito nel teorema classico, dato $\epsilon > 0$, $\forall \delta > 0$ e per M intero sufficientemente grande
$(\exists M_0 \in \mathcal{N} :\ \forall M \in \mathcal{N},\ M \geq M_0)$

$$P(\mathcal{T}_{M,\epsilon}(\rho)) = \mathrm{Tr}\left(\mathcal{P}_{M,\epsilon}(\rho)\ \rho^{\otimes M}\right) = P(\mathcal{T}_{M,\epsilon}(X)) \geq 1 - \delta$$

o, equivalentemente, sotto le medesime condizioni

$$P(\overline{\mathcal{T}_{M,\epsilon}(\rho)}) = \mathrm{Tr}\left(\overline{\mathcal{P}_{M,\epsilon}(\rho)}\ \rho^{\otimes M}\right) \leq \delta$$

ove $\overline{\mathcal{P}_{M,\epsilon}(\rho)} = \mathcal{I}_{\mathcal{H}_{Sorg}^{\otimes M}} - \mathcal{P}_{M,\epsilon}(\rho)$ è il proiettore al complemento ortogonale di $\mathcal{T}_{M,\epsilon}(\rho)$

Il sottospazio ϵ-*tipico* - Calcolo di $P(\mathcal{T}_{M,\epsilon}(\rho))$

Di conseguenza, come nel teorema classico, per $\epsilon > 0$ ed $M \to \infty$ risulta

$$P\Big(\mathcal{T}_{M,\epsilon}(\rho)\Big) = \lim_{M\to\infty} \mathrm{Tr}\left(\mathcal{P}_{M,\epsilon}(\rho)\, \rho^{\otimes M}\right) = 1$$

Al tendere di M all'infinito, dunque, tutti i messaggi di lunghezza M rientrano nel sottospazio ϵ-*tipico* $\mathcal{T}_{M,\epsilon}(\rho)$ di $\mathcal{H}_{Sorg}^{\otimes M}$ rispetto a ρ

Il sottospazio ϵ-*tipico*

Si cerca ora di stabilire:

1. $P(\mathcal{T}_{M,\epsilon}(\rho))$: la probabilità che un vettore w di $\rho^{\otimes M}$ sia in $\mathcal{T}_{M,\epsilon}(\rho)$

$$P(\mathcal{T}_{M,\epsilon}(\rho)) = \mathrm{Tr}\left(\mathcal{P}_{M,\epsilon}(\rho)\ \ \rho^{\otimes M}\right)$$

2. **La dimensione del sottospazio ϵ-*tipico*: $\dim(\mathcal{T}_{M,\epsilon}(\rho))$**

Il sottospazio ϵ-*tipico* - Calcolo di $dim(\mathcal{T}_{M,\epsilon}(\rho))$

Limitazione superiore:

$$
\begin{aligned}
&1 \geq P(\mathcal{T}_{M,\epsilon}(\rho)) = \\
&= \mathsf{Tr}\left(\mathcal{P}_{M,\epsilon}(\rho)\ \rho^{\otimes M}\right) = \\
&= \sum_{|\psi\rangle \in \mathcal{T}_{\mathcal{M},\epsilon}(\rho)} \lambda_\psi \geq \sum_{|\psi\rangle \in \mathcal{T}_{\mathcal{M},\epsilon}(\rho)} 2^{-M(S(\rho)+\epsilon)} = \\
&= 2^{-M(S(\rho)+\epsilon)} \sum_{|\psi\rangle \in \mathcal{T}_{\mathcal{M},\epsilon}(\rho)} 1 = \\
&= 2^{-M(S(\rho)+\epsilon)} \cdot dim(\mathcal{T}_{M,\epsilon}(\rho)).
\end{aligned}
$$

Risulta quindi

$$
l = dim(\mathcal{T}_{M,\epsilon}(\rho)) \leq 2^{M(S(\rho)+\epsilon)}
$$

Il sottospazio ϵ-*tipico* - Calcolo di $dim(\mathcal{T}_{M,\epsilon}(\rho))$

Limitazione inferiore:

$$
\begin{aligned}
&1-\delta \leq P(\mathcal{T}_{M,\epsilon}(\rho)) = \\
&= \mathrm{Tr}\left(\mathcal{P}_{M,\epsilon}(\rho)\ \rho^{\otimes M}\right) = \\
&= \sum_{|\psi\rangle \in \mathcal{T}_{\mathcal{M},\epsilon}(\rho)} \lambda_{\psi} \leq \sum_{|\psi\rangle \in \mathcal{T}_{\mathcal{M},\epsilon}(\rho)} 2^{-M(S(\rho)-\epsilon)} = \\
&= 2^{-M(S(\rho)-\epsilon)} \sum_{|\psi\rangle \in \mathcal{T}_{\mathcal{M},\epsilon}(\rho)} 1
\end{aligned}
$$

Dati $\epsilon > 0$ ed $\delta > 0$ la prima disequazione è valida per M sufficientemente grande ($M \geq M_0$). Risulta dunque, sotto le medesime condizioni, la limitazione inferiore

$$
l = dim(\mathcal{T}_{M,\epsilon}(\rho)) \geq (1-\delta)2^{M(S(\rho)-\epsilon)}
$$

Il sottospazio ϵ-*tipico* - Calcolo di $dim(\mathcal{T}_{M,\epsilon}(\rho))$

In conclusione, per parametri opportunamente scelti

$$(1-\delta)2^{M(S(\rho)-\epsilon)} \leq dim(\mathcal{T}_{M,\epsilon}(\rho)) \leq 2^{M(S(\rho)+\epsilon)}$$

Si giunge, anche in questo caso, ad una stretta correlazione col mondo classico

Il sottospazio ϵ-*tipico*

Sono stati stabiliti:

1. $P(\mathcal{T}_{M,\epsilon}(\rho))$: la probabilità che un vettore w di $\rho^{\otimes M}$ sia in $\mathcal{T}_{M,\epsilon}(\rho)$

$$P(\mathcal{T}_{M,\epsilon}(\rho)) = \mathsf{Tr}\left(\mathcal{P}_{M,\epsilon}(\rho)\ \ \rho^{\otimes M}\right)$$

2. La dimensione del sottospazio ϵ-*tipico*: $dim(\mathcal{T}_{M,\epsilon}(\rho))$

$$(1-\delta)2^{M(S(\rho)-\epsilon)} \leq dim(\mathcal{T}_{M,\epsilon}(\rho)) \leq 2^{M(S(\rho)+\epsilon)}$$

Dimostrazione dell'enunciato - Obiettivi

Teorema di Schumacher

- **Definisce un algoritmo di codifica** che abbassa il numero di qubit necessari fino a $N \simeq M \cdot S(\rho)$ con fedeltà media d'ensemble limitata inferiormente
- Con un numero di qubit $N < M \cdot S(\rho)$ la medesima fidelity, al crescere di M, si abbassa fino a 0 in **qualunque algoritmo** di codifica ideabile

Per raggiungere questo scopo viene utilizzato il *sottospazio* ϵ-*tipico* di $\mathcal{H}_{Sorg}^{\otimes M}$ relativo a ρ

Algoritmo di codifica Γ

0. Input: M registri in parallelo
   - Ciascuno preparato in accordo a ρ
1. Misurazione proiettiva che verifica se lo stato da codificare, $|\ \psi^{\otimes M}\ \rangle$, è nel sottospazio ϵ-*tipico*.
   - La misurazione proietta $|\ \psi^{\otimes M}\ \rangle$ nel sottospazio ϵ-*tipico*
2. Se $|\ \psi^{\otimes M}\ \rangle$ è ϵ-*tipico* allora il messaggio viene *mappato* in una parola codice (composto da N qubit) non usato in precedenza
   Altrimenti lo stato del sistema sorgente viene sostituito con un altro stato puro $|\ \psi^{\otimes M}\ \rangle'$, presente nel sottospazio ϵ-*tipico*, che viene infine *mappato* in N qubit

Algoritmo di codifica Γ

- Solo i messaggi presenti nel sottospazio ϵ-*tipico* vengono codificati in maniera iniettiva e decodificabile
- Ogni messaggio non presente nel sottospazio ϵ-*tipico* viene sostituito dall'algoritmo di codifica con uno presente nel sottospazio tipico
  Ciò causa un abbassamento della *fedeltà quantistica* del *canale di codifica-decodifica* che è stato ideato

In tutti i casi si considera il canale definito dall'algoritmo, $\Phi = \Pi\,\Gamma$ come privo di rumore

Algoritmo di decodifica Π

- Riceve in input N registri, ciascuno dei quali rappresenta un qubit
- Effettua il *mapping* inverso all'algoritmo di codifica, riportando lo stato del sistema in $\mathcal{H}_{Sorg}^{\otimes M}$

Algoritmo di codifica Γ - Misurazione proiettiva

Proietta tramite $\mathcal{P}_{M,\epsilon}(\rho)$, verificando se lo stato da codificare, $| \psi_i^{\otimes M} \rangle$, è nel sottospazio ϵ-*tipico*
Algebricamente ciò corrisponde a verificare una delle seguenti 3 condizioni (equivalenti):

1. $\mathcal{P}_{M,\epsilon}(\rho) \, | \psi^{\otimes M} \rangle \stackrel{?}{=} | \psi^{\otimes M} \rangle$
2. $\mathsf{Tr}\left(\mathcal{P}_{M,\epsilon}(\rho) \ \ | \psi^{\otimes M} \bigtimes \psi^{\otimes M} |\right) \stackrel{?}{=} 1$

Poiché $\mathsf{Tr}\left(| a \bigtimes b |\right) = \langle b \, | \, a \rangle$, ponendo $| a \rangle = (\mathcal{P}_{M,\epsilon}(\rho) \ | \psi^{\otimes M} \rangle)$ e $\langle b | = \langle \psi^{\otimes M} |$, la seconda equazione si riscrive come

3. $\langle \psi^{\otimes M} \, | \, \mathcal{P}_{M,\epsilon}(\rho) \, | \, \psi^{\otimes M} \rangle \stackrel{?}{=} 1$

Dimostrazione dell'enunciato - Correttezza ed ottimalità

L'algoritmo di Schumacher codifica con uno stato distinto di N qubit solo i messaggi in $\mathcal{T}_{M,\epsilon}(\rho)$ di $\mathcal{H}_{Sorg}^{\otimes M}$ rispetto a ρ

Correttezza.

- Usando almeno $N \simeq M \cdot S(\rho)$ qubit la **la fedeltà media d'ensamble** è limitata inferiormente dal valore $1 - 2 \cdot \delta$
  - La qualità della trasmissione non degrada eccessivamente

Ottimalità.

- Usando invece un numero qubit $N < M \cdot S(\rho)$ la medesima fidelity, al crescere di M, si abbassa fino a 0 in **qualunque algoritmo** di codifica ideabile

Dimostrazione della correttezza

Dato $\rho^{\otimes M}$, ed i parametri ϵ e δ, si dimostra che esiste un intero M_0 per il quale, se

1. si pone $M \geq M_0$ come parametro stante ad indicare la lunghezza fissa dei messaggi da codificare
2. si usano $N \geq M \cdot (S(\rho) + \epsilon)$ qubit per la codifica

risulta

$$\hat{F}\left(\Phi, \rho^{\otimes M}\right) \geq 1 - 2 \cdot \delta$$

Dimostrazione della correttezza

Dimostrazione.

Per scelta di $N \geq M \cdot (S(\rho) + \epsilon)$ e da $dim(\mathcal{T}_{M,\epsilon}(\rho)) \leq 2^{M(S(\rho)+\epsilon)}$

- È possibile codificare ogni vettore del sottospazio ϵ-*tipico* in maniera distinta

Sia

- $| \psi_i^{\otimes M} \rangle_{\forall i \in \{1,\ldots,t^M\}}$ il set degli autovettori di $\rho^{\otimes M}$

Definiamo

- $\Phi | \psi_i^{\otimes M} \rangle$ lo stato (espresso come matrice densità) che si ottiene dal canale Φ quando è codificato lo stato $| \psi_i^{\otimes M} \rangle$

Dimostrazione della correttezza

Per la costruzione del canale di codifica-decodifica, risulta

$$\Phi \mid \psi_i^{\otimes M} \rangle = \mid \psi_i^{\otimes M} \bigtimes \psi_i^{\otimes M} \mid \langle \psi_i^{\otimes M} \mid \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \rangle + \\ + \rho_{i,junk} \langle \psi_i^{\otimes M} \mid \overline{\mathcal{P}_{M,\epsilon}(\rho)} \mid \psi_i^{\otimes M} \rangle$$

$\rho_{i,junk}$ è il generico stato del sottospazio ϵ-*tipico* usato dall'algoritmo per sostituire $\mid \psi_i^{\otimes M} \rangle$ se $\mid \psi_i^{\otimes M} \rangle$ non fa parte del sottospazio tipico

- I calcoli che seguono sono indipendenti dalla scelta di $\rho_{i,junk}$

Dimostrazione della correttezza

Ragionando sul primo operando, si dimostra che

$$| \psi_i^{\otimes M} \bigtimes \psi_i^{\otimes M} | \langle \psi_i^{\otimes M} | \mathcal{P}_{M,\epsilon}(\rho) | \psi_i^{\otimes M} \rangle = \mathcal{P}_{M,\epsilon}(\rho) | \psi_i^{\otimes M} \bigtimes \psi_i^{\otimes M} | \mathcal{P}_{M,\epsilon}(\rho)$$

Pertanto, lo stato ricevuto si può riscrivere come

$$\Phi | \psi_i^{\otimes M} \rangle = \mathcal{P}_{M,\epsilon}(\rho) | \psi_i^{\otimes M} \bigtimes \psi_i^{\otimes M} | \mathcal{P}_{M,\epsilon}(\rho) + \rho_{i,junk} \langle \psi_i^{\otimes M} | \overline{\mathcal{P}_{M,\epsilon}(\rho)} | \psi_i^{\otimes M} \rangle$$

Dimostrazione della correttezza

Dalla definizione della *fedeltà media dell'ensemble* del canale di codifica-decodifica $\Phi = \Pi\,\Gamma$ rispetto alla sorgente $\rho^{\otimes M}$ (calcolata in base ai suoi autovettori ortogonali $\{|\,\psi_i\,\rangle\}\ \ i \in \{1, \ldots, t^M\}$) si ha

$$\hat{F}\left(\Phi, \rho^{\otimes M}\right) = \sum_{i=1}^{t^M} p_i \ \langle\, \psi_i^{\otimes M} \mid \ \left(\Phi \mid \psi_i^{\otimes M}\,\rangle\right) \ \mid \psi_i^{\otimes M}\,\rangle$$

Espandendo $\Phi \mid \psi_i^{\otimes M}\,\rangle$ si ha

$$\begin{aligned}
&\hat{F}\left(\Phi, \rho^{\otimes M}\right) = \\
&= \textstyle\sum_{i=1}^{t^M} \ p_i \ \langle\, \psi_i^{\otimes M} \mid \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M}\,\rangle \ \langle\, \psi_i^{\otimes M} \mid \mathcal{P}_{M,\epsilon}(\rho) \ \mid \psi_i^{\otimes M}\,\rangle + \\
&+ \textstyle\sum_{i=1}^{t^M} \ p_i \ \langle\, \psi_i^{\otimes M} \mid \ \rho_{i,junk} \mid \psi_i^{\otimes M}\,\rangle \ \langle\, \psi_i^{\otimes M} \mid \overline{\mathcal{P}_{M,\epsilon}(\rho)} \mid \psi_i^{\otimes M}\,\rangle
\end{aligned}$$

Dimostrazione della correttezza

La seconda sommatoria è reale e non regativa, dunque

$$\begin{aligned}
&\sum_{i=1}^{t^M} p_i \ \langle\, \psi_i^{\otimes M} \mid \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \,\rangle \ \langle\, \psi_i^{\otimes M} \mid \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \,\rangle + \\
&+ \sum_{i=1}^{t^M} p_i \ \langle\, \psi_i^{\otimes M} \mid \rho_{i,junk} \mid \psi_i^{\otimes M} \,\rangle \ \langle\, \psi_i^{\otimes M} \mid \overline{\mathcal{P}_{M,\epsilon}(\rho)} \mid \psi_i^{\otimes M} \,\rangle \geq \\
&\geq \sum_{i=1}^{t^M} p_i \ \langle\, \psi_i^{\otimes M} \mid \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \,\rangle \ \langle\, \psi_i^{\otimes M} \mid \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \,\rangle = \\
&= \sum_{i=1}^{t^M} p_i \ || \, \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \,\rangle \, ||^4
\end{aligned}$$

ove $|| \, \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \,\rangle \, ||$ è la *norma* del vettore $\left(\mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \,\rangle\right)$. Poiché $\forall x \in \mathcal{R} \ (x-1)^2 \geq 0$

ponendo $x = || \, \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \,\rangle \, ||^2$ risulta

$$\begin{aligned}
&|| \, \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \,\rangle \, ||^4 \geq \\
&\geq || \, 2 \, \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \,\rangle \, ||^2 - 1 = \\
&= 2 \, \langle\, \psi_i^{\otimes M} \mid \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \,\rangle - 1
\end{aligned}$$

Dimostrazione della correttezza

Mettendo tutto assieme

$$
\begin{aligned}
&\hat{F}\left(\Phi, \rho^{\otimes M}\right) \geq \\
&\geq \sum_{i=1}^{t^M} \left[p_i \; || \, \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \rangle \, ||^4 \right] \geq \\
&\geq \sum_{i=1}^{t^M} p_i \big(\; 2 \, \langle \, \psi_i^{\otimes M} \mid \mathcal{P}_{M,\epsilon}(\rho) \mid \psi_i^{\otimes M} \, \rangle - 1 \big) = \\
&= 2 \; \mathrm{Tr}\big(\, \mathcal{P}_{M,\epsilon}(\rho) \; \rho^{\otimes M} \big) - 1
\end{aligned}
$$

Poiché dato $\epsilon > 0$, $\forall \delta > 0$ e per M intero sufficientemente grande ($\exists M_0 \in \mathcal{N} : \; \forall M \in \mathcal{N}, \; M \geq M_0$) vale
$\mathrm{Tr}\left(\mathcal{P}_{M,\epsilon}(\rho) \; \rho^{\otimes M}\right) \geq 1 - \delta$

Si ottiene che, dato $\epsilon > 0$, $\delta > 0$, $\exists M_0 \in \mathcal{N} : \; \forall M \geq M_0$

$$\hat{F}\left(\Phi, \rho^{\otimes M}\right) \geq 2 \; \mathrm{Tr}(\mathcal{P}_{M,\epsilon}(\rho) \, \rho^{\otimes M}) - 1 \geq 2(1 - \delta) - 1 = 1 - 2 \, \delta$$

il che completa la prova di correttezza dell'algoritmo proposto

Dimostrazione dell'enunciato - Correttezza ed Ottimalità

Ottimalità.

- Usando invece un numero qubit $N < M \cdot S(\rho)$ la medesima fidelity, al crescere di M, si abbassa fino a 0 in **qualunque algoritmo** di codifica ideabile

Formalmente.

- Scelti gli stessi $\epsilon > 0$, $\delta > 0$ ed $M \geq M_0$, sia ora $N < M(S(\rho) - \epsilon)$
- Si dimostra che non esiste alcun canale di codifica-decodifica $\Phi' = \Pi' \, \Gamma'$ che, codificando con distinti stati di N qubit un qualunque sottospazio $\mathcal{A} \subset \mathcal{H}_{Sorg}^{\otimes M}$ mantenga una fedeltà media dell'ensemble sufficientemente elevata
  - Al contrario, al crescere di M, tende sempre a 0

Dimostrazione dell'ottimalità

Dimostrazione. Dato il siffatto N il sottospazio $\mathcal{A} \subset \mathcal{H}_{Sorg}^{\otimes M}$ dei messaggi codificati con stati distinti di N qubit da un generico algoritmo Γ' ha dimensione

$$l' = dim(\mathcal{A}) \leq 2^N < 2^{M(S(\rho)-\epsilon)}$$

dove gli l' vettori che formano la base di $\mathcal{A}$ sono scelti parte degli autovettori di $\rho^{\otimes M}$

Dimostrazione dell'ottimalità

Quando viene codificato e trasmesso un messaggio l'autovettore $| \psi \rangle_i^{\otimes M}$ di $\rho^{\otimes M}$ lungo il canale Φ' viene ottenuto dal decodificatore uno stato rappresentato dalla matrice densità γ_i

$$\Phi' \ | \psi_i^{\otimes M} \rangle = \gamma_i = \sum_{j=1}^{l'} \lambda_j \, | j^{\otimes M} \rangle\langle j^{\otimes M} |$$

con $| j^{\otimes M} \rangle\langle j^{\otimes M} | : \ j \in \{1, \ldots, l'\}$ base di $\mathcal{A}$ e $\lambda_j : \ j \in \{1, \ldots, l'\}$ distribuzione di probabilità

Dimostrazione dell'ottimalità

$$\mathcal{P}_{\mathcal{A}} \stackrel{\text{def}}{=} \sum_{j=1}^{l'} | j^{\otimes M} \rangle\langle j^{\otimes M} |$$

È il proiettore al sottospazio $\mathcal{A}$. La *fedeltà media dell'ensemble* del canale Φ' rispetto alla sorgente $\rho^{\otimes M}$ calcolata rispetto agli autovettori di $\rho^{\otimes M}$ è

$$\begin{aligned}
&\hat{F}\left(\Phi', \rho^{\otimes M}\right) = \\
&= \sum_{i=1}^{t^M} p_i \ \langle \psi_i^{\otimes M} | \ \left[\Phi' | \psi_i^{\otimes M} \rangle\right] \ | \psi_i^{\otimes M} \rangle = \\
&= \sum_{i=1}^{t^M} p_i \ \langle \psi_i^{\otimes M} | \ \left[\sum_{j=1}^{l'} \lambda_j | j^{\otimes M} \rangle\langle j^{\otimes M} |\right] \ | \psi_i^{\otimes M} \rangle \leq \\
&\leq \sum_{i=1}^{t^M} p_i \ \langle \psi_i^{\otimes M} | \ \left[| j^{\otimes M} \rangle\langle j^{\otimes M} |\right] \ | \psi_i^{\otimes M} \rangle = \\
&= \sum_{i=1}^{t^M} p_i \ \langle \psi_i^{\otimes M} | \ \mathcal{P}_{\mathcal{A}} \ | \psi_i^{\otimes M} \rangle = \\
&= \mathrm{Tr}\left(\rho^{\otimes M} \mathcal{P}_{\mathcal{A}}\right)
\end{aligned}$$

Dimostrazione dell'ottimalità

Per completare l'enunciato si prova che, scelti i parametri come illustrato in precedenza, con M sufficientemente grande, risulta

$$\mathrm{Tr}\left(\rho^{\otimes M}\mathcal{P}_{\mathcal{A}}\right) = 0$$

Per far ciò si scompone $\rho^{\otimes M}\mathcal{P}_{\mathcal{A}}$ nelle sue componenti presenti nel sottospazio ϵ-*tipico* e nel complemento ortogonale di quest'ultimo

$$\begin{aligned}
&\mathrm{Tr}\left(\rho^{\otimes M}\ \mathcal{P}_{\mathcal{A}}\right) = \\
&= \mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\right) = \\
&= \mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \mathcal{P}_{M,\epsilon}(\rho)\right) + \mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \overline{\mathcal{P}_{M,\epsilon}(\rho)}\right)
\end{aligned}$$

Dimostrazione dell'ottimalità

$$\begin{aligned}&\mathsf{Tr}\left(\rho^{\otimes M}\ \mathcal{P}_{\mathcal{A}}\right) = \\ &= \mathsf{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \mathcal{P}_{M,\epsilon}(\rho)\right) + \mathsf{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \overline{\mathcal{P}_{M,\epsilon}(\rho)}\right)\end{aligned}$$

Si trattano i due addendi separatamente

Primo addendo $Tr\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \mathcal{P}_{M,\epsilon}(\rho)\right)$.

Si dimostra che (la dimostrazione è omessa)
$\mathsf{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \mathcal{P}_{M,\epsilon}(\rho)\right) \leq\ 2^{-M(S(\rho)-\epsilon)}\ \mathsf{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \mathcal{P}_{M,\epsilon}(\rho)\right)$

Dimostrazione dell'ottimalità

Dimostrazione. Si assuma s.l.g. di operare nella base in cui $\rho^{\otimes M}$ e $\mathcal{P}_{M,\epsilon}(\rho)$ sono diagonali

$$\mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \mathcal{P}_{M,\epsilon}(\rho)\right) \leq 2^{-M(S(\rho)-\epsilon)}\ \mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \mathcal{P}_{M,\epsilon}(\rho)\right)$$

- Poiché gli autovalori di ogni operatore di proiezione assumono solo valore 0 oppure 1, sostituendo il valore 1 al posto di $\mathcal{P}_{M,\epsilon}(\rho)$ si ottiene una maggiorazione

$$\mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \mathcal{P}_{M,\epsilon}(\rho)\right) \leq 2^{-M(S(\rho)-\epsilon)}\ \mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \mathcal{P}_{M,\epsilon}(\rho)\right) \leq$$
$$\leq 2^{-M(S(\rho)-\epsilon)}\ \mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\right) = 2^{-M(S(\rho)-\epsilon)} \cdot l'$$

Dimostrazione dell'ottimalità

Dunque

$$\mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \mathcal{P}_{M,\epsilon}(\rho)\right)\ \leq\ 2^{-M(S(\rho)-\epsilon)}\cdot l'$$

Al crescere di M, per via della definizione di l'
$(l' = dim(\mathcal{A}) < 2^{M(S(\rho)-\epsilon)})$, risulta

$$\lim_{M\to\infty}\mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \mathcal{P}_{M,\epsilon}(\rho)\right)\ \leq\ \lim_{M\to\infty}2^{-M(S(\rho)-\epsilon)}\cdot l'\ =\ 0$$

Dimostrazione dell'ottimalità

Secondo addendo. $\mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \overline{\mathcal{P}_{M,\epsilon}(\rho)}\right)$
Si assuma s.l.g. di avere $\mathcal{P}_{\mathcal{A}}$ in forma diagonale

$$\mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \overline{\mathcal{P}_{M,\epsilon}(\rho)}\right) \leq \mathrm{Tr}\left(\rho^{\otimes M}\ \overline{\mathcal{P}_{M,\epsilon}(\rho)}\right)$$

Effettuando ulteriori passaggi algebrici

$$\begin{aligned}
&\mathrm{Tr}\left(\rho^{\otimes M}\,\overline{\mathcal{P}_{M,\epsilon}(\rho)}\right) = \mathrm{Tr}\left(\rho^{\otimes M}\ \left(\mathcal{I}_{\mathcal{H}_{Sorg}^{\otimes M}} - \mathcal{P}_{M,\epsilon}(\rho)\right)\right) = \\
&= \mathrm{Tr}\left(\rho^{\otimes M}\ -\ \rho^{\otimes M}\,\mathcal{P}_{M,\epsilon}(\rho)\right) = \mathrm{Tr}\,\rho^{\otimes M}\ -\ \mathrm{Tr}\left(\rho^{\otimes M}\,\mathcal{P}_{M,\epsilon}(\rho)\right) = \\
&= 1 -\ \mathrm{Tr}\left(\rho^{\otimes M}\,\mathcal{P}_{M,\epsilon}(\rho)\right)
\end{aligned}$$

Dimostrazione dell'ottimalità

In più, per $M \to \infty$ risulta

$$\lim_{M\to\infty} \mathrm{Tr}\left(\rho^{\otimes M}\, \overline{\mathcal{P}_{M,\epsilon}(\rho)}\right) = 1 - \lim_{M\to\infty} \mathrm{Tr}\left(\rho^{\otimes M}\, \mathcal{P}_{M,\epsilon}(\rho)\right) = 0$$

In conclusione, scelti ϵ, δ ed $M \geq M_0$

$$\begin{cases} \lim_{M\to\infty} \mathrm{Tr}\left(\rho^{\otimes M}\ \mathcal{P}_{\mathcal{A}}\right) = & \lim_{M\to\infty} \mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \mathcal{P}_{M,\epsilon}(\rho)\right) + \\ & + \lim_{M\to\infty} \mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \overline{\mathcal{P}_{M,\epsilon}(\rho)}\right) \\ \lim_{M\to\infty} \mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \mathcal{P}_{M,\epsilon}(\rho)\right) \ \leq \ \lim_{M\to\infty} 2^{-M(S(\rho)-\epsilon)} \cdot l' \ = \ 0 \\ \lim_{M\to\infty} \mathrm{Tr}\left(\mathcal{P}_{\mathcal{A}}\ \rho^{\otimes M}\ \overline{\mathcal{P}_{M,\epsilon}(\rho)}\right) \leq \ \lim_{M\to\infty} \mathrm{Tr}\left(\rho^{\otimes M}\, \overline{\mathcal{P}_{M,\epsilon}(\rho)}\right) = 0 \end{cases}$$

Dimostrazione dell'ottimalità

Dunque

$$\lim_{M\to\infty} \hat{F}\left(\Phi', \rho^{\otimes M}\right) \leq \lim_{M\to\infty} \mathrm{Tr}\left(\rho^{\otimes M}\ \mathcal{P}_{\mathcal{A}}\right) = 0$$

Il che completa la dimostrazione di ottimalità dell'algoritmo proposto

EOF

Grazie per l’attenzione!