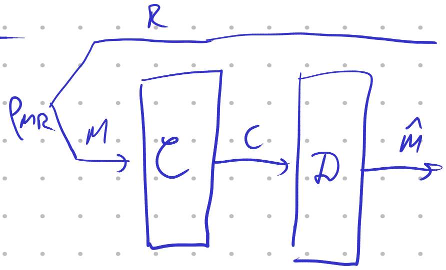
Mini-Course: Quantum Information Theory

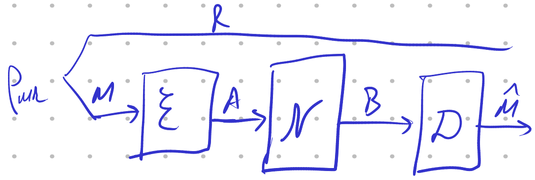
Intro

Compression



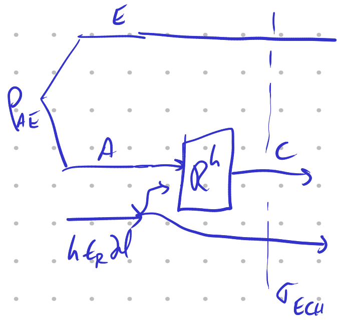
Want ① Low error rate
② $\log|C|$ as small as possible.

Channel coding:



Want: ① low error rate
② $\log|M|$ as big as possible.

Randomness extraction & Decoupling



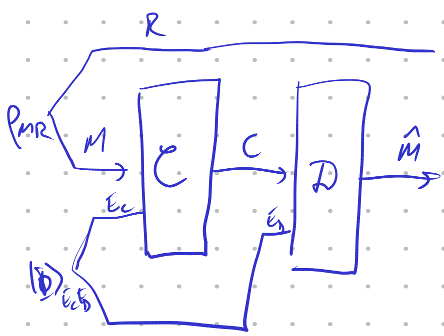
Want ① $\sigma_{ECH} \approx \frac{\mathbb{1}_C}{|C|} \otimes \sigma_E \otimes \frac{\mathbb{1}_H}{|H|}$.

uniform on C

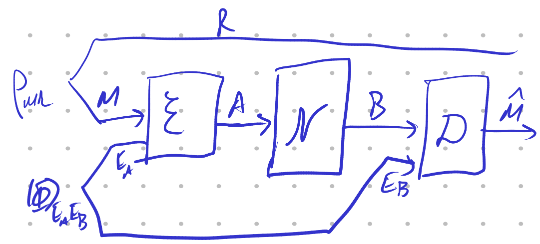
② $\log|C|$ as big as possible.

Entanglement assistance

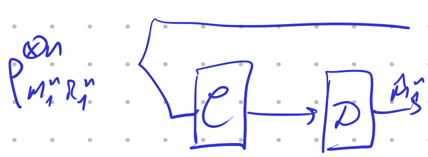
Compression

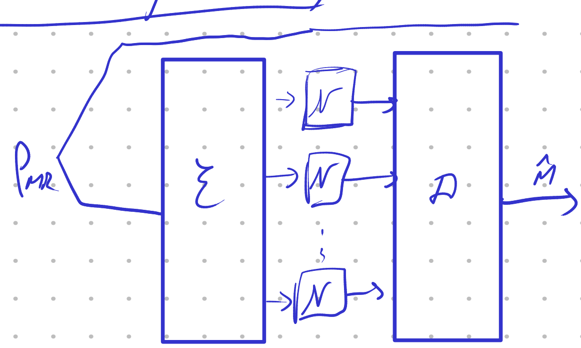


Channel coding



iid (independent & identically distributed)





Mathematical Background

Density operators (aka "quantum probability distribution")

- We have state $|\psi_i\rangle \in \mathcal{H}$ with probability p_i. $\{(p_i, |\psi_i\rangle) : i \in I\}$.
- Measure in basis $\{|\varphi_j\rangle : j \in J\}$.

$$\Pr[\text{measure } j] = \sum_i p_i \, |\langle \varphi_j | \psi_i \rangle|^2$$

$$= \sum_i p_i \, \langle \varphi_j | \psi_i \rangle\langle \psi_i | \varphi_j \rangle$$

$$= \langle \varphi_j | \underbrace{\left(\sum_i p_i \, |\psi_i\rangle\langle \psi_i| \right)}_{\rho \in L(\mathcal{H},\mathcal{H}) \text{ : density operator}} |\varphi_j\rangle.$$

$\rho \in \mathrm{Pos}(\mathcal{H}) = \{A : \forall |\psi\rangle, \langle \psi | A | \psi \rangle \geq 0\}$

- Ex: Uniform distribution over basis $\{|\psi_i\rangle\}$ $\rightarrow$ $\rho = \sum \frac{1}{d} |\psi_i\rangle\langle\psi_i| = \frac{1}{d} \underbrace{\sum_i |\psi_i\rangle\langle\psi_i|}_{\mathbb{1} \text{ (identity)}}$

$$|0\rangle\langle 0| + |1\rangle\langle 1| = \mathbb{1}$$

$$|+\rangle\langle +| + |-\rangle\langle -| = \mathbb{1}.$$

- Ex: Pure state $|\psi\rangle$, $\rho = |\psi\rangle\langle\psi|$ $\rightarrow$ rank one.

Trace

- Given an $n \times n$ matrix M, $\mathrm{Tr}[M] = \sum_i M_{ii}$
- Basis independent $\Rightarrow$ works for any $M \in L(\mathcal{H},\mathcal{H})$ w/o specifying a basis.
- Cyclic. $\mathrm{Tr}[AB] = \mathrm{Tr}[BA]$ ($\forall$ density operator ρ, $\mathrm{Tr}[\rho] = \mathrm{Tr}[\sum_i p_i |\psi_i\rangle\langle\psi_i|]$ $= \sum p_i \mathrm{Tr}[\underbrace{|\psi_i\rangle}_{A}\underbrace{\langle\psi_i|}_{B}]$ $= \sum p_i \mathrm{Tr}\langle\psi_i|\psi_i\rangle$ $= 1.$)

Hence: $\Pr[\text{measure } j] = \langle\varphi_j|\rho|\varphi_j\rangle = \mathrm{Tr}[\underbrace{\langle\varphi_j|\rho}_{A}\underbrace{|\varphi_j\rangle}_{B}] = \mathrm{Tr}[\underbrace{|\varphi_j\rangle\langle\varphi_j|}_{\in \mathrm{Pos}(\mathcal{H})}\rho]$

$$\sum_j |\varphi_j\rangle\langle\varphi_j| = \mathbb{1}$$

More generally: Can view any set $\{M_j : M_j \in \mathrm{Pos}(\mathcal{H})\}$ w/ $\sum_j M_j = \mathbb{1}$ as a measurement.

("POVM": Positive operator valued measurement)

$$\Pr[\text{outcome } M_j] = \mathrm{Tr}[M_j \rho]$$

$$\sum_j \Pr[\text{outcome } M_j] = \sum_j \mathrm{Tr}[M_j \rho] = \mathrm{Tr}[(\textstyle\sum_j M_j)\rho] = \mathrm{Tr}[\rho] = 1.$$

$|\psi_i\rangle \quad |\varphi_j\rangle$

$M_i = \frac{1}{2}|\psi_i\rangle\langle\psi_i|$ $\quad \{\frac{1}{2}|\psi_1\rangle\langle\psi_1|, \ldots, \frac{1}{2}|\psi_{I_{max}}\rangle\langle\psi_{I_{max}}|,$

$M_{j+I_{max}} = \frac{1}{2}|\varphi_j\rangle\langle\varphi_j|$ $\quad \frac{1}{2}|\varphi_1\rangle\langle\varphi_1|, \ldots, \frac{1}{2}|\varphi_{I_{max}}\rangle\langle\varphi_{I_{max}}|\}.$

Partial Trace

- Sps we have $|\psi\rangle_{AE} \in \mathcal{H}_A \otimes \mathcal{H}_E$. Sps we have a measurement on A: $\{M_j : M_j \in Pos(\mathcal{H}_A)\}$

$\sum M_j = \mathbb{1}$.

$$\sum_j M_j \otimes \mathbb{1}_E = \left(\sum M_j\right) \otimes \mathbb{1}_E = \mathbb{1}_A \otimes \mathbb{1}_E = \mathbb{1}_{AE}.$$

$$\Pr[\text{outcome } j] = \mathrm{Tr}\left[(M_j \otimes \mathbb{1}_E)|\psi\rangle\langle\psi|\right] = \sum_{a,e} \langle a| \otimes \langle e| \left((M_j \otimes \mathbb{1})|\psi\rangle\langle\psi|\right)|a\rangle \otimes |e\rangle$$

$$= \sum_a \langle a| \Big(M_j \underbrace{\sum_e (\mathbb{1}_A \otimes \langle e|)|\psi\rangle\langle\psi|(\mathbb{1}_A \otimes |e\rangle)}_{\mathrm{Tr}_E[|\psi\rangle\langle\psi|] \in L(\mathcal{H}_A, \mathcal{H}_A)}\Big)|a\rangle \qquad \left(\mathrm{Tr}[M] = \sum_i \langle i|M|i\rangle\right)$$

$$= \mathrm{Tr}\Big[M_j \underbrace{\mathrm{Tr}_E[|\psi\rangle\langle\psi|]}_{\text{density operator on } A}\Big].$$

Quantum Channels

$$\mathcal{H}_A \otimes \mathcal{H}_{A'} \cong \mathcal{H}_B \otimes \mathcal{H}_E$$

"Everything is unitary" $\quad |\psi\rangle_A \in \mathcal{H}_A \quad U_{AA'\to BE}\left(|\psi\rangle_A \otimes |0\rangle_{A'}\right) \in \mathcal{H}_B \otimes \mathcal{H}_E$

$$\rho_A = \sum p_i |\psi_i\rangle\langle\psi_i| \mapsto \sum p_i\, U(|\psi_i\rangle \otimes |0\rangle)(\langle\psi_i| \otimes \langle 0|)U^\dagger$$

$$= U\Big(\underbrace{\sum p_i |\psi_i\rangle\langle\psi_i|}_{\rho} \otimes |0\rangle\langle 0|\Big)U^\dagger.$$

$$\xrightarrow{\text{trace out } E} \mathrm{Tr}_E\left[U\left(\sum p_i |\psi_i\rangle\langle\psi_i| \otimes |0\rangle\langle 0|\right)U^\dagger\right] = \sum_e \underbrace{(\mathbb{1}_B \otimes \langle e|)}_{L(\mathcal{H}_B \otimes \mathcal{H}_E, \mathcal{H}_B)} \underbrace{U}_{L(\mathcal{H}_A \otimes \mathcal{H}_{A'}, \mathcal{H}_B \otimes \mathcal{H}_E)} \underbrace{(\mathbb{1}_A \otimes |0\rangle)}_{\in L(\mathcal{H}_A, \mathcal{H}_A \otimes \mathcal{H}_{A'})} \rho_A \underbrace{(\mathbb{1}_A \otimes \langle 0|)U^\dagger(\mathbb{1}_B \otimes |e\rangle)}_{N_e^\dagger}$$

$$N_e \in L(\mathcal{H}_A, \mathcal{H}_B)$$

$$= \sum_e N_e \rho_A N_e^\dagger.$$

Note that: $\displaystyle \sum_e N_e^\dagger N_e = \sum_e (\mathbb{1}_A \otimes \langle 0|)U^\dagger(\mathbb{1}_B \otimes |e\rangle)(\mathbb{1}_B \otimes \langle e|)U(\mathbb{1}_A \otimes |0\rangle)$

$$= (\mathbb{1}_A \otimes \langle 0|)\cancel{U^\dagger}\Big(\mathbb{1}_B \otimes \underbrace{\sum_e |e\rangle\langle e|}_{\mathbb{1}}\Big)\cancel{U}(\mathbb{1}_A \otimes |0\rangle)$$

$$= \mathbb{1}_A.$$

→ Quantum channel: $\mathcal{N}(\rho) = \sum_j N_j \rho N_j^\dagger$ s.t. $\sum N_j^\dagger N_j = \mathbb{1}$.

"CPTP map" ⟶ completely positive ⇝ $X \in \mathrm{Pos}(\mathcal{H}_A \otimes \mathcal{H}_R)$ $(\mathcal{N} \otimes \mathbb{1}_R)(X) \in \mathrm{Pos}(\mathcal{H}_B \otimes \mathcal{H}_R)$

& trace preserving → $\mathrm{Tr}[\mathcal{N}(X)] = \mathrm{Tr}[X]$.

$X \in L(\mathcal{H}_A)$ $\qquad \mathcal{N}: L(\mathcal{H}_A) \to L(\mathcal{H}_B)$

Ex: - Erasure channel: $\mathcal{N}(\rho) = (1-\varepsilon)\rho + \varepsilon |\perp\rangle\langle\perp|$

$$= \left(\sqrt{1-\varepsilon}\,\mathbb{1}\right)\rho\left(\sqrt{1-\varepsilon}\,\mathbb{1}\right) + \sum_i \left(\sqrt{\varepsilon}\,|\perp\rangle\langle i|\right)\rho\left(|i\rangle\langle\perp|\sqrt{\varepsilon}\right).$$

- Depolarizing channel: $\mathcal{N}(\rho) = (1-\varepsilon)\rho + \varepsilon \frac{\mathbb{1}}{d}$

$$= \left(\sqrt{1-\varepsilon}\,\mathbb{1}\right)\rho\left(\sqrt{1-\varepsilon}\,\mathbb{1}\right) + \frac{\varepsilon}{4}\left(\mathbb{1}\rho\mathbb{1} + X\rho X + Y\rho Y + Z\rho Z\right)$$

Purification

- Sps we have ρ_A: $\exists$ a purification $|\psi\rangle_{AR}$ s.t. $\mathrm{Tr}_R[|\psi\rangle\langle\psi|] = \rho_A$

$$|\Phi\rangle_{AR} := \sum \frac{1}{\sqrt{d_A}} |i\rangle_A \otimes |i\rangle_R. \quad \longrightarrow \quad \mathrm{Tr}_R[|\Phi\rangle\langle\Phi|] = \frac{\mathbb{1}_A}{d_A}.$$

Trick: $\quad X_A \in L(\mathcal{H}_A) \qquad (X_A \otimes \mathbb{1}_R)|\Phi\rangle_{AR} = (\mathbb{1}_A \otimes X_R^T)|\Phi\rangle_{AR}$.

Given ρ_A, $\quad |\psi\rangle_{AR} = \sqrt{d_A}\left(\sqrt{\rho_A} \otimes \mathbb{1}_R\right)|\Phi\rangle_{AR}$.

$\hookrightarrow \rho_A = \sum p_i |\psi_i\rangle\langle\psi_i| \rightarrow f(\rho_A) = \sum f(p_i)\,|\psi_i\rangle\langle\psi_i|$.

$$\mathrm{Tr}_R[|\psi\rangle\langle\psi|] = \mathrm{Tr}_R\left[\sqrt{d_A}\left(\sqrt{\rho_A} \otimes \mathbb{1}_R\right)|\Phi\rangle\langle\Phi|\left(\sqrt{\rho_A} \otimes \mathbb{1}_R\right)\sqrt{d_A}\right]$$
$$= d_A \sqrt{\rho_A}\,\mathrm{Tr}_R[|\Phi\rangle\langle\Phi|]\sqrt{\rho_A}$$
$$= \cancel{d_A}\sqrt{\rho_A}\,\frac{\mathbb{1}_A}{\cancel{d_A}}\sqrt{\rho_A} = \rho_A.$$

Fact: Given two purification $|\psi\rangle_{AR}$, $|\varphi\rangle_{AR}$ of ρ_A, $\exists U_R$ st. $|\psi\rangle_{AR} = (\mathbb{1}_A \otimes U_R)|\varphi\rangle_{AR}$.

Stinespring dilation: Purifying channels

- Sps we have a channel $\mathcal{N}_{A\to B}$ $\quad \rho_A \mapsto \sum_i N_i \rho N_i^\dagger$. $\quad \exists V_{A\to BE}$ s.t. $\mathcal{N}(\rho) = \mathrm{Tr}_E[V\rho V^\dagger]$

Let $\quad V = \sum_i N_i \otimes |i\rangle_E$

$$\mathrm{Tr}_E[V\rho V^\dagger] = \mathrm{Tr}_E\Big[\underbrace{\big(\textstyle\sum_i N_i\otimes|i\rangle_E\big)\,\rho\,\big(\sum_j N_j^\dagger\otimes\langle j|\big)}\Big]$$

$$= \sum_k \langle k|_E \;\; |k\rangle_E$$

$$= \sum_i N_i\,\rho\, N_i^\dagger .$$

Distance measures

- Give two ρ_A & σ_A, how close are they?

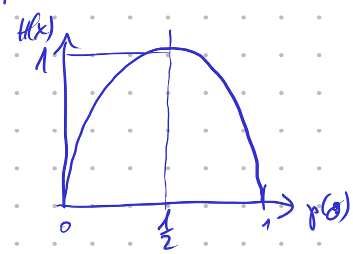
  Trace distance: $\|\rho_A-\sigma_A\|_1 := \mathrm{Tr}\big[|\rho_A-\sigma_A|\big]$.

  Fact: Best prob of guessing $= \frac{1}{2}+\frac{1}{4}\|\rho_A-\sigma_A\|_1$.

Information Measures

- Surprisal of an event $\mathcal{E}$.
- Def: $S(\mathcal{E}) := -\log_2 \Pr[\mathcal{E}]$.
- Def [Entropy]: $H(X)_p := \mathbb{E}_x\big[S(X=x)\big]$ $\quad p_x$: prob. distribution over $\mathcal{X}$.

  $$= -\sum_x p_x(x)\log p_x(x).$$



$$0 \le H(X) \le \log|\mathcal{X}|.$$

- Conditional entropy: $H(X|Y) = \mathbb{E}_y\big[H(X|Y=y)\big] = -\sum_{x,y} p(x,y)\log p(x|y)$. $\qquad H(X|Y)\ge 0$

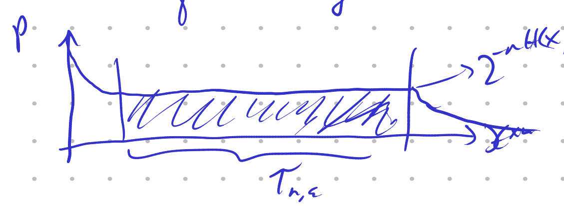
  Fact: $H(X|Y) = H(XY) - H(Y)$. $\qquad$ (Cover & Thomas)

- Mutual information: $I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$

- Asymptotic equipartition property (AEP)

  X_1^n iid. $\exists$ a typical set $T_{n,\varepsilon} = \{x_1^n : 2^{-n(H(X)+\varepsilon)} \le p(x_1^n) \le 2^{-n(H(X)-\varepsilon)}\}$.

  1. $\Pr[X_1^n \in T_{n,\varepsilon}] \to 1$ as $n\to\infty$
  2. $2^{+n(H(X)-\varepsilon)} \le |T_{n,\varepsilon}| \le 2^{n(H(X)+\varepsilon)}$ for n large.



Quantum Case

$\rho_A = \sum p(a) |a\rangle\langle a|$. $H(A)_\rho$ = entropy of eigenvalues

$$= -\sum p(a) \log p(a)$$
$$= -\mathrm{Tr}[\rho_A \log \rho_A].$$

Conditional entropy: ρ_{AB} $H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$

Can be negative! $\rho_{AB} = |\Phi\rangle\langle\Phi|_{AB}$

$$H(A|B)_\rho = H(AB) - H(B)$$
$$= 0 - 1 = -1.$$

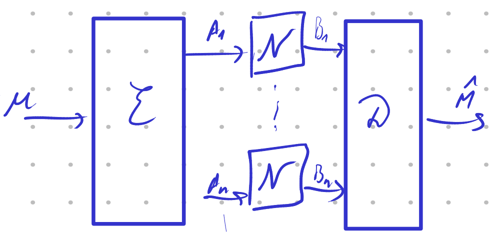
Mutual information: $I(A;B)_\rho := H(A) - H(A|B) \geq 0$ $[H(A|B) \leq H(A)]$

Back to info theory problems

Channel coding

Classical data

$M \in \mathcal{M}$

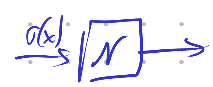


- Want: $\forall m \in \mathcal{M}$,
  $\Pr[\hat{M} \neq M] \leq$ small. ($\to 0$ as $n \to \infty$)
- Rate: $R = \frac{\log |\mathcal{M}|}{n}$
- Achievable rate: $\exists \mathcal{E}_n, \mathcal{D}_n$ s.t. $\Pr[\hat{M} \neq M] \to 0$ as $n \to \infty$
  $R_n \to R$ as $n \to \infty$.

- Capacity of $\mathcal{N}$ = supremum of achievable rates.

Thm [HSW]: $C_{HSW}(\mathcal{N}) = \max_{\rho_{XB}} I(X;B)_\rho$ is achievable.

$\rho_{XB} = \sum p(x) |x\rangle\langle x|_X \otimes \mathcal{N}(\sigma(x))$.

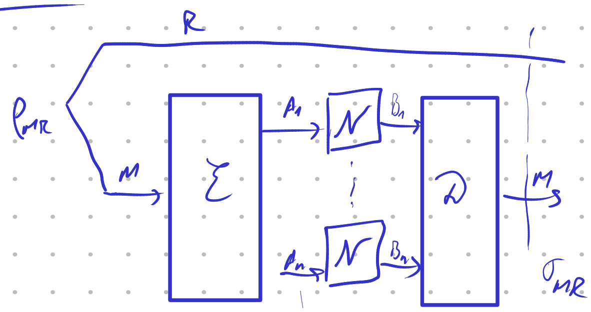


"Additivity conjecture": Is this the capacity?

Answer: No! [Hastings '08]: $\exists$ channel $\mathcal{N}$ st. $C_{HSW}(\mathcal{N}^{\otimes 2}) > 2C_{HSW}(\mathcal{N})$.

$\hookrightarrow$ existence proof only!

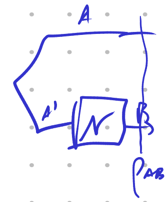
Quantum data



$\forall \rho_{MR}$,
Want: $\|\sigma_{MR} - \rho_{MR}\|_1 \leq$ small,

Thm [LSD]: The rate

$$C_{LSD}(\mathcal{N}) = \max_{\rho} \left(-H(A|B) \right) \quad \text{is achievable.}$$



$C_{LSD}(\mathcal{N}) \neq$ capacity

$\mathcal{N}_1$, $\mathcal{N}_2$

- Mark Wilde. "From Classical to Quantum Shannon Theory"
- Marco Tomamichel, "Quantum info. processing w/ finite resources: mathematical foundations"