

QIT

Janik Schüttler

HS20

1 Classical Formalism

Boolean algebra

- Boolean algebra: a set of propositions and all their combinations under the three logical operations. If non-empty, always contains the tautology 1 and self-contradiction 0.
- propositions/ events: entities we assign probabilities to
- disjoint propositions: events which cannot be true at the same time
- atoms: set of propositions such that any proposition in the Boolean algebra can be written as the OR of a set of atoms. Always exists for finite Boolean algebras. Any Boolean algebra is equivalent to the powerset of the set of atoms.
- subalgebras: when regarding a proposition as tautology
- random variable

Boolean probability $\Pr[A|C]$, $C \neq 0$, fullfills:

- $\Pr[A|C] \geq 0$ (axiom 1, positivity)
- $\Pr[A|C] = 1$ iff $C \implies A$ (axiom 2, norm.)
- $\Pr[A \vee B|C] = \Pr[A|C] + \Pr[B|C]$ for $A \wedge B = 0$ (axiom 3, addition rule)
- $\Pr[A \wedge B|C] = \Pr[A|B \wedge C] \Pr[B|C]$ (axiom 4, product rule, consistency of sub-algebras)
- $\Pr[A \vee B|C] = \Pr[A|C] \Pr[B|C] - \Pr[A \wedge B|C]$
- $\Pr[\bigvee_i A_i|C] \leq \sum_i \Pr[A_i|C]$ (union bound)
- $\Pr[A] = \sum_i \Pr[A|B_i] \Pr[B_i]$ for $\bigvee_i B_i = 1$ (law of total probability)
- $\Pr[A|B \wedge C] = \frac{\Pr[B|A \wedge C]}{\Pr[B|C]} \Pr[A|C]$

Representational probability

- $P_X : \mathcal{X} \rightarrow [0, 1]$, $P_X(x) := \Pr[X = x]$
- $P_{XY}(x, y) := \Pr[X = x \wedge Y = y]$
- $P_{X|Y=y} : \mathcal{X} \rightarrow [0, 1]$, $P_{X|Y=y}(x) := \frac{P_{XY}(x, y)}{P_Y(y)}$
- $P_{X|Y}(x, y) = P_{X|Y}(x|y) = P_{X|Y=y}(x)$
- $P_X(x) = \sum_y P_{XY}(x, y) = \sum_y P_{X|Y=y}(x) P_Y(y)$
- linearity: $P_Y(y) = \sum_{x \in \mathcal{X}} \mathbf{1}[f(x) = y] P_X(x)$

Convexity

- convex set: closed under convex combinations:
 $s, r \in \mathcal{S} \implies \lambda s + (1 - \lambda)r \in \mathcal{S}$, $\lambda \in [0, 1]$
- convex hull: a set's convex combinations
- extreme points: cannot be written as nontrivial convex combination of other points
- convex function: $f(\lambda x_1 + (1 - \lambda)x_2) \leq \lambda f(x_1) + (1 - \lambda)f(x_2)$. Set of points above f is convex.
- Jensen's inequality: $\langle f(X) \rangle \geq f(\langle X \rangle)$

$$\text{Prob}(n) := \{(p_1, \dots, p_n) \in \mathbb{R}^n : p_i \geq 0, \sum p_i = 1\}$$

$$\text{Events}(n) := \{(e_1, \dots, e_n) \in \mathbb{R}^n : e_i \in \{0, 1\}\}$$

$$\text{Tests}(n) := \{(t_1, \dots, t_n) \in \mathbb{R}^n : 0 \leq t_i \leq 1\}$$

$$\begin{aligned} \text{States}(d) &:= \{\sigma \in L(\mathbb{C}^d) : \sigma \geq 0, \text{Tr}[\sigma] = 1\} \\ &= \text{Hull}(\{|\varphi\rangle\langle\varphi| : |\varphi\rangle \in L(\mathbb{C}^d)\}) \end{aligned}$$

$$\text{Events}(d) := \{\Gamma \in L(\mathbb{C}^d) : 0 \geq \Gamma \leq \mathbb{1}\}$$

$$\begin{aligned} \text{POVMs}(n, d) &:= \{\{\Lambda(x)\}_{x=1}^n : \Lambda(x) \in \text{Effects}(d), \\ &\quad \sum \Lambda(x) = \mathbb{1}\} \end{aligned}$$

Independence

- A, B independent iff $\Pr[A \wedge B] = \Pr[A] \Pr[B]$
- A, B conditionally independent iff $\Pr[A \wedge B|C] = \Pr[A|C] \Pr[B|C]$
- pairwise independence not sufficient for independence of more than 2 events
- Markov inequality $\Pr[X \geq \epsilon] \leq \frac{1}{\epsilon} \langle X \rangle$
- Chebychev inequality $\Pr[(Y - y)^2 \geq \epsilon] \leq \frac{1}{\epsilon} \sigma^2$
- LLN & CLT for $Z_n = \sum_i X_i$ with X_i iid

$$\lim_{n \rightarrow \infty} \Pr[|Z_n - \mu| > \epsilon] = 0 \quad \forall \epsilon \quad (\text{wLLN})$$

$$\Pr\left[\lim_{n \rightarrow \infty} Z_n = \mu\right] = 1 \quad (\text{sLLN})$$

$$\lim_{n \rightarrow \infty} \Pr\left[\sqrt{n} \frac{Z_n - \mu}{\sigma} \leq y\right] = \Phi(y) \quad (\text{CLT})$$

- convergence speed from Chebychev, Hoeffding bound, Berry-Esseen theorem:

$$\Pr[(Z_n - \mu)^2 < \epsilon] \leq O(n^{-1})$$

$$\Pr[|Z_n - \mu| \geq \epsilon] \leq 2 \exp\left(-\frac{2n\epsilon^2}{(b-a)^2}\right)$$

$$|\Pr[Y_n \leq y] - \Phi(y)| \leq \frac{Ct}{\sigma^3 \sqrt{n}}$$

2 Quantum Formalism

Quantum probability theory

$$\Pr[\Lambda]_\rho = \text{Tr}[\Lambda\rho]$$

$$\rho \in L(H), \quad \rho \geq 0 \quad \text{Tr}[\rho] = 1 \quad (\text{density op})$$

$$\Lambda \in L(H) \quad \lambda \geq 0 \quad \Lambda \leq \mathbb{1} \quad (\text{effect})$$

- POVM $\{\Lambda(x)\}_{x=1}^n$
- Hilbert-Schmidt inner product
- states are complex hull of pure states
- decomposition of density matrix into ensemble of states is non-unique
- indeterminacy of measurement Λ is partly due to quantum nature and partly because a state is a mixture of pure state (ensemble character). Due to non-uniqueness division cannot be made.
- Gleason's theorem: $P(\mathbb{1}) = 1, P(0) = 0, P(\Pi_j + \Pi_k) = P(\Pi_j) + P(\Pi_k)$ for $\Pi_j\Pi_k = 0$ imply $P(\Pi) = \text{Tr}[\text{Tr}\rho]$

Composite systems

- product state $|\varphi\rangle_A \otimes |\psi\rangle_B$
- entangled states are non-trivial convex combinations of product states
- maximally entangled states

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |b_k\rangle_A \otimes |b_k\rangle_B$$

$$|\Omega\rangle_{AB} = \sum_{k=0}^{d-1} |b_k\rangle_A \otimes |b_k\rangle_B$$

- Bell basis in 2D $|\Phi_{ij}\rangle = (\mathbb{1} \otimes X^j Z^k) |\Phi\rangle_{AB}$

$$|\Phi_{00}\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi_{01}\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Phi_{10}\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Phi_{11}\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

- Bell basis in dD $|\Phi_{ij}\rangle = (\mathbb{1} \otimes U_B^j V_B^k) |\Phi\rangle_{AB}$
- Weyl-Heisenberg operators ($\omega = e^{2\pi i/d}$)

$$U = \sum_{k=0}^{d-1} |k+1\rangle \langle k|, \quad V = \sum_{k=0}^{d-1} \omega^k |k\rangle \langle k|$$

- partial trace with basis $|b_k\rangle$ of system B: $\text{Tr}_B[|\Psi\rangle \langle \Psi|_{AB}] = \sum_{k=1}^{d_B} \langle b_k| |\Psi\rangle_{AB} \langle \Psi| |b_k\rangle$
- marginal/ reduced state $\rho_A = \text{Tr}_B[\rho_{AB}]$
- unitary actions & measurements on B does not affect A (and vice versa)
- cq states $\rho_{ZA} = \sum_z P_Z(z) \langle b_k| |b_k\rangle_Z \otimes \rho_A(z)$

Bloch sphere

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\varphi} |1\rangle$$

$$\mathbf{n}_\psi = (\sin \theta \cos \varphi, \sin \theta \sin \varphi, \cos \theta)^T$$

$$\psi = |\psi\rangle \langle \psi| = \frac{1}{2}(\mathbb{1} + \mathbf{n} \cdot \boldsymbol{\sigma})$$

$$|\mathbf{n}_\psi^\perp\rangle = |-\mathbf{n}_\psi\rangle$$

$$|\langle \varphi | \psi \rangle|^2 = \frac{1}{2}(1 + \mathbf{n}_\varphi \cdot \mathbf{n}_\psi)$$

$$\Pr[\Lambda_{\mathbf{n}}]_{\mathbf{m}} = \text{Tr}[\Lambda_{\mathbf{m}}\rho_{\mathbf{m}}] = \frac{1}{2}(1 + \mathbf{n} \cdot \mathbf{m})$$

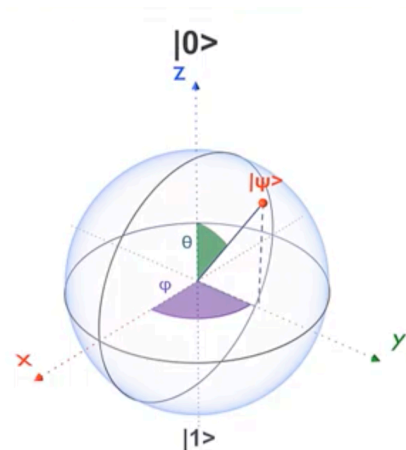
$$\lambda_\pm = \frac{1}{2}(1 \pm |\mathbf{n}|)$$

$$\mathbf{n}_{|0\rangle} = (0, 0, +1), \quad \theta = 0, \varphi = 0$$

$$\mathbf{n}_{|1\rangle} = (0, 0, -1), \quad \theta = \pi, \varphi = 0$$

$$\mathbf{n}_{|+\rangle} = (+1, 0, 0), \quad \theta = \pi/2, \varphi = 0$$

$$\mathbf{n}_{|-\rangle} = (-1, 0, 0), \quad \theta = \pi/2, \varphi = \pi$$



Entanglement has the property that for the composite system AB there exists a measurement for which the outcome is certain. However, any nontrivial measurement of A/B alone results in a uniform outcome distribution. The full system is deterministic, parts of the system are completely uncertain.

Separable vs. entangled A pure state $|\theta\rangle_{AB}$ is

- separable/ a product state iff there exists $|\varphi\rangle_A, |\psi\rangle_B$ st $|\theta\rangle_{AB} = |\varphi\rangle_A \otimes |\psi\rangle_B$
- entangled otherwise: $|\theta\rangle_{AB} = \sum_k |\varphi_k\rangle_A \otimes |\psi_k\rangle_B$

A mixed state θ_{AB} is

- separable iff there exists $p_k \in [0, 1], \rho_A(k), \rho_B(k)$ st $\theta_{AB} = \sum_k p_k \rho_A(k) \otimes \rho_B(k)$
- separable iff there exists $p_k \in [0, 1], |\varphi_k\rangle_A, |\psi_k\rangle_B$ st $\theta_{AB} = \sum_k p_k |\varphi_k\rangle_A \langle \varphi_k|_A \otimes |\psi_k\rangle_B \langle \psi_k|_B$
- entangled otherwise

Operator-state isomorphism

$$V : L(\mathcal{H}_A, \mathcal{H}_B) \rightarrow \mathcal{H}_A \otimes \mathcal{H}_B$$

$$M_{B|A} \mapsto (\mathbb{1}_A \otimes M_{B|A'}) |\Omega\rangle_{AA'}$$

$$V^{-1} : |\Psi\rangle_{AB} \mapsto_{AA'} \langle \Omega | \Psi \rangle_{A'B}$$

- $V(|\varphi\rangle_B \langle \psi|_A) = |\bar{\psi}\rangle_A \otimes |\varphi\rangle_B$
- $M_{B|A} |\Omega\rangle_{AA'} = \sum M_{ij} |ij\rangle_{BA'} \in \mathcal{H}_A \otimes \mathcal{H}_B$ for $M_{B|A} = \sum M_{ij} |i\rangle_B \langle j|_A \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$
- ${}_{AA'} \langle \Omega | \Omega \rangle_{A'B} = \mathbb{1}_{B|A} = \sum_i |b_i\rangle_B \langle b_i|_A$
- $\mathbb{1}_A \otimes M_{B|A'} |\Omega\rangle_{AA'} = (M_{B|A'})^T \otimes \mathbb{1}_{A'} |\Omega\rangle_{BB'}$
- V is an isometry

Quantum channels are completely positive, trace-preserving, linear maps/ superoperators.

- trace preserving: $\text{Tr}[\mathcal{E}_{B|A}[\rho_A]] = 1$ for $\text{Tr}[\rho_A] = 1$
- positivity: $\mathcal{E}_{B|A}[\rho_A] \geq 0$ for $\rho_A \geq 0$
- complete positivity: $\mathcal{E}_{B|A} \otimes \mathcal{I}_R$ positive f any \mathcal{H}_R
- necessity of completely positivity: $(\mathcal{I}_A \otimes \mathcal{T}_B) \Phi_{AB}$ has eigenvector $\frac{1}{\sqrt{2}}(|jk\rangle - |kj\rangle)$ with negativ eigenvalue $-1/2$
- adjoint \mathcal{E}^* : $\text{Tr}[\Lambda \mathcal{E}[\rho]] = \text{Tr}[\mathcal{E}^*[\Lambda] \rho]$
- unital \mathcal{E} : $\mathcal{E}[\mathbb{1}] = \mathbb{1}$
- \mathcal{E} trace-preserving $\iff \mathcal{E}^*$ unital

Important quantum channels

$$\rho \rightarrow (1-p)\rho + p \text{diag}[\rho] \quad (\text{dephasing})$$

$$= (1-p/2)\rho + \frac{p}{2} Z \rho Z$$

$$\rho \rightarrow (1-p)\rho + p\pi \quad (\text{depolarizing})$$

$$\sqrt{1-3p/4} \mathbb{1}, \sqrt{p/4} \sigma_k, k = x, y, z$$

$$\rho \rightarrow (1-p)\rho + p|?\rangle \langle ?| \quad (\text{erasure})$$

$$\sqrt{1-p}(|0\rangle \langle 0| + |1\rangle \langle 1|), \sqrt{p}|?\rangle \langle 0|, \sqrt{p}|?\rangle \langle 1|$$

$$\rho \rightarrow K_0^\dagger \rho K_0 + K_1^\dagger \rho K_1 \quad (\text{amplitude damping})$$

$$\sqrt{p}|0\rangle \langle 1|, |0\rangle \langle 0| + \sqrt{1-p}|1\rangle \langle 1|$$

Quantum instrument performs a measurement and stores the outcome + post-measurement state

$$Q_{XB|A} : \rho_A \mapsto \sum |x\rangle \langle x| \otimes M_{B|A}(x) \rho_A M_{B|A}^*(x)$$

- Given POVM $\{\Lambda_A(x)\}$, a qinstrument's Kraus operators $K_{B|A}(x)$ must satisfy

$$\Lambda_A(x) = K_{B|A}^*(x) K_{B|A}(x)$$

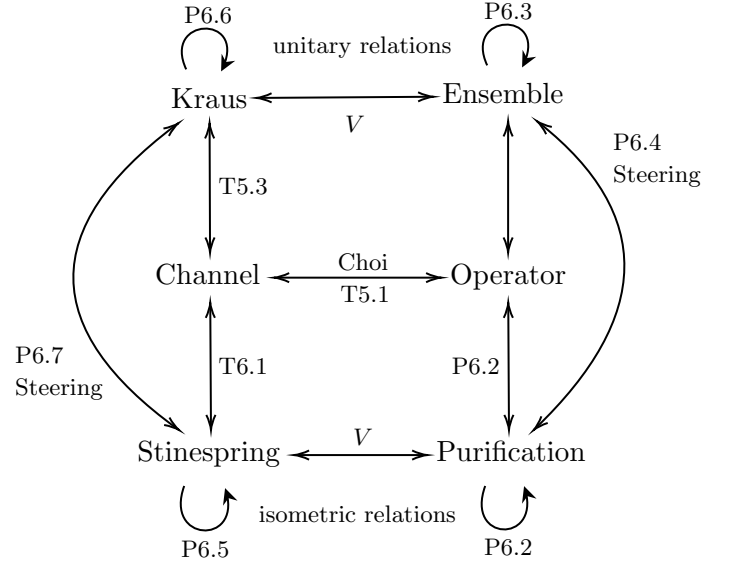
- $\text{Tr}_B \circ Q_{XB|A}[\rho_A]$ = measurement result only without post-measurement state of ρ_A
- $\text{Tr}_X \circ Q_{XB|A}[\rho_A]$ = post-measurement state of ρ_A only, forgetting the outcome. A Kraus representation. Thereby, every qchannel can be regarded as a measurement by some POVM followed by forgetting the measurement results.

- A POVM can have more than one Kraus op

$$\Lambda_A(x) = \sum_y M_{B|A}^*(x, y) M_{B|A}(x, y)$$

Transpose map \mathcal{T} / swap operator F

- transpose $\mathcal{T} : M \mapsto M^T, M \in L(\mathcal{H}_A, \mathcal{H}_B)$, ${}_B \langle b'_j | M | b_k \rangle_A | b'_j \rangle_B \langle b_k |_A \mapsto \langle b'_k | M | b_j \rangle | b_j \rangle_A \langle b'_k |_B$
- swap $F_{AA'} = \mathcal{T}_{A'}[\Omega_{AA'}] = (\mathcal{I}_A \otimes \mathcal{T}_{A'})[\Omega_{AA'}]$
- $F_{AB}(|\varphi\rangle_A \otimes |\psi\rangle_B) = |\psi\rangle_A \otimes |\varphi\rangle_B$
- $\text{Tr}_{A'}[F_{AA'}] = \mathbb{1}_A$
- $F_{AA'}^2 = \mathbb{1}_{AA'}$
- $\text{Tr}_{A'}[S_{A'}^T \Omega_{AA'}] = S_A$



Choi map relative to basis $\{b_i\}$ for $\mathcal{H}_A \simeq \mathcal{H}_B$ is

$$C : L(L(\mathcal{H}_A), L(\mathcal{H}_B)) \rightarrow L(\mathcal{H}_A \otimes \mathcal{H}_B)$$

$$\mathcal{E}_{B|A} \mapsto \mathcal{E}_{B|A'}[\Omega_{AA'}]$$

$$C^{-1}(M_{AB}) : \rho_A \mapsto \text{Tr}_A[\mathcal{T}_A[\rho_A] M_{AB}]$$

- C is an isomorphism with inverse C^{-1}
- C depends on basis $\{b_i\}$ chosen to define $|\Omega\rangle$
- $C(\text{identity channel}) = \Omega_{AB}$

Choi representation (\sim density operators)

- $\mathcal{E}_{B|A}$ is completely positive iff $C(\mathcal{E}_{B|A}) \geq 0$
- $\mathcal{E}_{B|A}$ is trace preserving iff $\text{Tr}_B[C(\mathcal{E}_{B|A})] = \mathbb{1}$
- set of channels is a convex set of positive operators on \mathcal{H}_{AB} , whose marginal on A corresponds to the identity. Extreme points are rank-one operators subject to the condition on the marginal.

Kraus representation (\sim ensembles)

- $\mathcal{E}_{B|A}$ is completely positive iff $\exists K_{B|A}(j)$ st

$$\mathcal{E}_{B|A}[S_A] = \sum_j K_{B|A}(j) S_A K_{B|A}^*(j)$$

- $\mathcal{E}_{B|A}$ is trace preserv iff $\sum_j K_{B|A}^*(j)K_{B|A}(j) = \mathbb{1}$
- $\{\Lambda(x) = K^*(x)K(x)\}_x$ is a POVM
- Kraus representations are not unique due to the non-uniqueness of the Choi operator.
- Minimal number of Kraus operators = Choi rank

Stinespring representation (\sim purifications)

- $\mathcal{E}_{B|A}$ is cp iff $\exists \mathcal{H}_R, V_{BR|A} \in L(\mathcal{H}_A, \mathcal{H}_B \otimes \mathcal{H}_R)$ st $\mathcal{E}_{B|A}[S_A] = \text{Tr}_R[V_{BR|A}S_A V_{BR|A}^*] \quad \forall S_A \in L(\mathcal{H}_A)$
- $\mathcal{E}_{B|A}$ is trace preserving iff $V_{BR|A}^* V_{BR|A} = \mathbb{1}_A$
- smallest possible $d_R \leq d_A d_B$
- qchannels = unitary operations involving additional systems which we do not have access to
- for any dilations $V_{BR|A}, V'_{BR|A}$ there exists a partial isometry $W_{R'|R}$ st $V'_{BR|A} = W_{R'|R} V_{BR|A}$

Purifications of ρ_A are normalized $|\psi\rangle_{AR} \in \mathcal{H}_A \otimes \mathcal{H}_R$ such that $\rho_A = \text{Tr}_R[|\psi\rangle\langle\psi|_{AR}]$.

- canonical purification $|\Psi\rangle_{AR} = \sqrt{\rho_A} \otimes \mathbb{1}_R |\Omega\rangle_{AR}$
- a purification always exists iff $\dim \mathcal{H}_R \geq r$ (otherwise Schmidt rank is smaller than ρ_A 's rank)
- minimal purifications have $\dim \mathcal{H}_R = r$
- $\rho_A, \rho_R = \text{Tr}_A[\Psi_{AR}]$ have same eigenvals s_k^2 by Schmidt decomposition (but distinct eigenfuncs)
- *steering*: any purification can produce every ensemble decomposition by suitable measurement

Unitary relations of ensembles & Kraus operators

- For *ensemble dec* $\{p_k, |\varphi_k\rangle\}_{k=1}^n, \{q_j, |\psi_j\rangle\}_{j=1}^m$ of the same density operator ρ , there exists an $l \times l$ unitary matrix U ($l = \max(n, m)$) st

$$\sqrt{q_j} |\psi_j\rangle = \sum_{k=1}^l \sqrt{p_k} \langle b_j | U | b_k \rangle |\varphi_k\rangle$$

- For *Kraus operators* $\{K_i\}_{i=1}^n, \{K_j\}_{j=1}^m$ of the same superoperator \mathcal{E} , there exists an $l \times l$ unitary matrix U ($l = \max(n, m)$) st

$$K'_j = \sum_i U_{ij} K_i$$

Isometric relations of dilations & purifications

- For any two purifications $|\Psi\rangle_{AR}, |\Psi'\rangle_{AR'}$, there exists a partial isometry $V_{R'|R}$ st

$$|\Psi'\rangle_{AR'} = (\mathbb{1}_A \otimes V_{R'|R}) |\Psi\rangle_{AR}$$

- For any two dilations $V_{BR|A}, V'_{BR|A}$, there exists a partial isometry $W_{R'|R}$ st

$$V'_{BR|A} = W_{R'|R} V_{BR|A}$$

If $\dim \mathcal{H}_{R'} > (=) \dim \mathcal{H}_R$, the partial isometries can be taken to be an isometry (unitary).

Steering purifications and Stinespring dilations

- Given a state ρ_A , suppose $|\Psi\rangle_{AB}$ is a purification and $\{P_X(x), \rho_A(x)\}$ an ensemble decomposition. Then there exists a POVM $\Gamma_B(x)$ st

$$\text{Tr}_B[\Gamma(x)\Psi_{Ab}] = P_X(x)\rho_A(x)$$

- In particular, let $V_{B|A}$ be the partial isometry such that $|\Psi\rangle_{AB}$ such that $|\Psi\rangle_{AB} = \sqrt{\rho_A} \otimes V_{B|A} |\Omega\rangle_{AA'}$ and $\{\Lambda_B(x)\}$ be the pretty-good measurement associated with the ensemble. Then $\Gamma_B(x) = V_{V|A} \Lambda_A(x)^T V_{B|A}^*$.

- Given a channel $\mathcal{E}_{B|A}$, suppose $V_{BR|A}$ is a Stinespring dilation and $\{\mathcal{E}_{B|A}(x)\}_x$ is an ensemble decomp. Then there exists a POVM $\Gamma_R(x)$ st

$$(\mathcal{E}_x)_{B|A} : S_A \mapsto \text{Tr}_R[\Gamma_R(x) V_{BR|A} S_A (V_{BR|A})^*]$$

Schmidt decompositions

Pretty-good measurement

Measurement as coherent process

Information disturbance

- Measurements are disturb qsystems, but without measurement one cannot learn anything.
- No disturbance implies no information gain: for any qinstrument $\mathcal{Q}_{XA|A}$ st $\text{Tr}_X \circ \mathcal{Q}_{XA|A} = \mathcal{I}_A$, there exists a probability distribution P_X st $\mathcal{Q}_{XA|A} = P_X \otimes \mathcal{I}_A$ (X, A are independent).
- Converse is not true.
- Rank-1 projective measurements are maximally disturbing: let $\mathcal{Q}_{XB|A}$ a qinstrument st

$$\mathcal{M}_{X|A} = \text{Tr}_B \mathcal{Q}_{XB|A} : \rho_A \mapsto \sum_x |x\rangle \langle x|_X \langle x | \rho | x \rangle.$$

Then there exists $\varphi_B(x)$ st $\mathcal{Q}_{XB|A} = \mathcal{E}_{XB|X} \circ \mathcal{M}_{X|A}$ with $\mathcal{E}_{XB|X} : |x\rangle \langle x|_X \mapsto |x\rangle \langle x|_X \otimes \varphi_B(x)$.

3 Quantum Hypothesis testing

Hypothesis testing

- Idea: find POVM to distinguish quantum states, i.e. maximize $P_{\text{guess}}(X|B)_\tau$ given CQ state τ
- For two states, $\tau = p|0\rangle\langle 0| \otimes \rho + (1-p)|1\rangle\langle 1| \otimes \sigma$, solved exactly (Bayesian and NP agree):

$$P_{\text{guess}}(X|B)_\tau = \max_{0 \leq \Lambda \leq \mathbb{1}} P_{\text{guess}}(X|B)_{\Lambda, \tau}$$

$$= \max_{\Lambda} \text{Tr}[\Lambda M], \quad \text{st } 0 \leq \Lambda \leq \mathbb{1}$$

$$P_{\text{guess}}(X|B)_\tau = \frac{1}{2} + \frac{1}{2} \|p\rho - (1-p)\sigma\|_1$$

- For more states, $\rho_{XB} = \sum_x P_X(x) |x\rangle\langle x|_X \otimes \rho_B(x)$, no general solution known.

$$P_{\text{guess}}(X|B)_\rho = \sup_{\Lambda_{XB}} \text{Tr}[\Lambda_{XB} \rho_{XB}]$$

$$= \sup_{\Lambda_{XB}} \sum_x P_X(x) \text{Tr}[\Lambda_B(x) \rho_B(x)]$$

$$\text{st } \text{Tr}_X[\Lambda_{XB}] \leq \mathbb{1}_B, \Lambda_{XB} \geq 0$$

- monotonicity: $P_{\text{guess}}(X|C)_\sigma \leq P_{\text{guess}}(X|B)_\rho$, for $\sigma_{XC} = \mathcal{E}_{C|B}[\rho_{XB}]$

Bayesian hypothesis testing

$$P_{\text{guess}} = \max_{\Lambda} \{(1-p) + \text{Tr}[\Lambda(p\rho - (1-p)\sigma)]\}$$

$$f(M) = \max\{\text{Tr}[\Lambda M] : 0 \leq \Lambda \leq \mathbb{1}\}$$

$$f(M) \geq \text{Tr}\{\{M \geq 0\}M\} = \text{Tr}\{\{M\}_+\}$$

$$\hat{f}(M) = \min\{\text{Tr}[\theta] : 0 \leq \theta, \theta \geq M\}$$

$$\hat{f}(M) \leq \text{Tr}\{\{M\}_+\}$$

$$f(M) = \text{Tr}\{\{M\}_+\} = \frac{1}{2}(\text{Tr}[M] + \|M\|_1)$$

$$P_{\text{guess}} = \frac{1}{2} + \frac{1}{2} \|p\rho + (1-p)\sigma\|$$

Neyman-Pearson hypothesis testing

$$H_0 = \text{given state is } \rho, \text{ error type I} = 1 - \alpha$$

$$H_1 = \text{given state is } \sigma, \text{ error type II} = \beta$$

$$\beta_\alpha(\rho, \sigma) = \min\{\text{Tr}[\Lambda\sigma] : 0 \leq \Lambda \leq \mathbb{1}, \text{Tr}[\Lambda\rho] \geq \alpha\}$$

$$\Lambda^* = \{m\rho - \sigma > 0\} + c\{m\rho - \sigma = 0\}$$

$$\hat{\beta}_\alpha(\rho, \sigma) = \min_{m, \theta} \{m\alpha - \text{Tr}[\theta] : m\rho - \theta \leq \sigma, 0 \leq \theta, m\}$$

$$\theta^* = \{m\rho - \sigma\}_+$$

- Neyman-Pearson lemma: likelihood ratio test $\Lambda(a) = \{\rho - a\sigma\}_+$ is optimal in $\beta_\alpha(\rho, \sigma)$
- Complementary slackness: constraints of dual or primal are strictly satisfied, iff optimality.
- Slater condition: if primal (dual) feasible + dual (primal) strictly feasible, duality gap is zero.

Distinguishability

$$\delta(\rho, \sigma) := 2P_{\text{guess}}(X|B)_\tau - 1$$

$$= \max_{\Lambda} \{\text{Tr}[\Lambda(\rho - \sigma)] : 0 \leq \Lambda \leq \mathbb{1}\}$$

$$= \min_{\theta} \{\text{Tr}[\theta] : \rho - \sigma \leq \theta, \theta \geq 0\}$$

$$= \frac{1}{2} \|\rho - \sigma\|_1$$

$$\delta(\mathcal{E}_{B|A}, \mathcal{F}_{B|A}) = \sup_{\rho, \Lambda} \text{Tr}[\Lambda_{BR}(\mathcal{E}_{B|A}[\rho_{AR}] - \mathcal{F}_{B|A}[\rho_{AR}])]$$

$$\text{st } \text{Tr}[\rho_{AR}] = 1, \rho_{AR} \geq 0, 0 \leq \Lambda_{BR} \leq \mathbb{1}$$

- faithfulness: $\delta(\rho, \sigma) = 0 \iff \rho = \sigma$
- triangle ineq: $\delta(\rho, \sigma) \leq \delta(\rho, \tau) + \delta(\tau, \sigma)$
- monotonicity: $\delta(\mathcal{E}_{B|A}[\rho], \mathcal{E}_{B|A}[\sigma]) \leq \delta(\rho, \sigma)$
- joint convexity:

$$\delta\left(\sum P_x \rho_x, \sum P_x \sigma_x\right) \leq \sum P_x \delta(\rho_x, \sigma_x)$$

Fidelity

$$F(\rho, \sigma) = \sup_R \max_{|\psi_\rho\rangle, |\psi_\sigma\rangle} |\langle \psi_\rho, \psi_\sigma \rangle_{AR}|$$

$$= \|\sqrt{\rho}\sqrt{\sigma}\|_1 = \text{Tr}\left[\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right]$$

- $\delta(\psi_\rho, \psi_\sigma)^2 = 1 - |\langle \psi_\rho, \psi_\sigma \rangle|^2$
- $F(\mathcal{E}_{B|A}[\rho_A], \mathcal{E}_{B|A}[\sigma_A]) \geq F(\rho_A, \sigma_A)$ and equality for isometries $\mathcal{E}_{B|A}[\rho_A] = V_{B|A}\rho_A V_{B|A}^*$
- $F(\rho \otimes \rho', \sigma \otimes \sigma') = F(\rho, \sigma)F(\rho', \sigma')$
- $F_{\text{pg}}(\rho, \sigma) = \text{Tr}[\sqrt{\rho}\sqrt{\sigma}]$
- $F(\rho, \sigma)^2 \leq F_{\text{pg}}(\rho, \sigma)$
- $\delta(\rho, \sigma) + F(\rho, \sigma) \geq 1$
- $\delta^2(\rho, \sigma) + F^2(\rho, \sigma) \leq 1$

Optimal measurement in classical case

- commuting $\varphi_B(x) = \sum_y P_{Y|X=x}(y) |y\rangle\langle y|_Y$
- optimal measurement is deterministic: maximize conditional distribution $x \mapsto P_{X|Y=y}(x)$
- optimal POVM els $\Lambda_B(x) = \sum_y Q(x, y) |y\rangle\langle y|_Y$
- $P_{\text{guess}} = \sum_x P_X(x) \sum_y Q(x, y) P_{Y|X=x}(y) = \sum_y P_Y(y) \sum_x Q(x, y) P_{X|Y=y}(x)$

Pretty good measurements

$$P_{\text{guess}}^{\text{PGM}}(X|B)_\rho = \text{Tr}[(\mathbb{1} \otimes \rho_B^{-\frac{1}{2}}) \rho_{XB} (\mathbb{1} \otimes \rho_B^{-\frac{1}{2}}) \rho_{XB}]$$

$$= Q(\rho_{XB}, \mathbb{1}_X \otimes \rho_B)$$

- $Q(\rho, \sigma) := \text{Tr}[\rho\sigma^{-1/2}\rho\sigma^{-1/2}]$
- Q fulfills joint convexity, monotonicity and isometric invariance
- in classical case $\Lambda_B(x) = \sum_y P_{X|Y=y}(x) |y\rangle\langle y|_Y$ and the PGM is to the optimal measurement
- *pretty good*: for CQ state ρ_{XB} (X classical)

$$P_{\text{guess}}(X|B)_\rho^2 \leq P_{\text{guess}}^{\text{PGM}}(X|B)_\rho \leq P_{\text{guess}}(X|B)_\rho$$

4 Communication Converses

classical info, classical channel, unassisted

$$\begin{aligned} W_{M'|M}(m'|m) &= \sum_{x,y} D_{M'|Y}(m'|y) N_{Y|X}(y|x) E_{X|M}(x|m) \\ P_{\text{agree}} &\leq \frac{\min(|X|, |Y|)}{|M|} \end{aligned}$$

classical info, quantum channel, unassisted

$$\begin{aligned} W_{M'|M}(m'|m) &= \text{Tr}[\Lambda_B(m') \mathcal{N}_{B|A}[\rho_A(m)]] \\ P_{\text{agree}} &\leq \frac{\min(|A|, |B|)}{|M|} \end{aligned}$$

quantum info, classical ch, unassisted

tool: PPT ineq: $\text{Tr}[\Phi_{AB} \sigma_{AB}] \leq \frac{1}{|A|}$ with PPT σ_{AB}

$$\begin{aligned} \mathcal{N}_{Q'|Q}[\rho_Q] &= \mathcal{D}_{Q'|Y} \circ N_{Y|X} \circ \mathcal{E}_{X|Q}[\rho_Q] \\ &= \sum_{x,y} N_{Y|X}(y|x) \rho_{Q'}(y) \text{Tr}_Q[\Lambda_Q(x) \rho_Q] \\ \mathcal{N}_Q[\Phi_{QQ'}] &= \sum_{x,y} N_{Y|X}(y|x) \rho_Q(y) \otimes \text{Tr}_Q[\Lambda_Q(x) \Phi_{QQ'}] \\ P_{\text{agree}} &\leq \frac{1}{|Q|} \end{aligned}$$

quantum info, quantum ch, unassisted

pinching $S_{AB} \leq |A| \mathbb{1}_A \otimes S_B$ for $S_{AB} \geq 0$

$$\begin{aligned} \mathcal{N}_{Q'|Q}[\rho_Q] &= \mathcal{D}_{Q'|B} \circ \mathcal{N}_{B|A} \circ \mathcal{E}_{A|Q}[\rho_Q] \\ \mathcal{N}_Q[\Phi_{QQ'}] &= \mathcal{D}_{Q|B} \circ \mathcal{N}_{B|A} \circ \mathcal{E}_{A|Q}[\Phi_{QQ'}] \\ P_{\text{agree}} &\leq \frac{1}{|Q|^2} \min(|A|^2, |B|^2) \end{aligned}$$

classical info, classical channel, assisted

pinching $\mathcal{E}_{X|M=m,T}[\rho_{TT'}] \leq \mathbb{1}_X \otimes \rho_{T'}$

$$\begin{aligned} W_{M'=m'|M=m}[\rho_{TT'}] &= \mathcal{D}_{M'=m'|Y=y,T'} \circ N_{Y|X} \circ \mathcal{E}_{X|M=m,T}[\rho_{TT'}] \\ P_{\text{agree}} &\leq \frac{\min(|X|, |Y|)}{|M|} \end{aligned}$$

cl info, q ch, assisted (superdense coding)

$$\begin{aligned} W_{M'|M}(m'|m) &= \mathcal{D}_{M'=m'|BT'} \circ \mathcal{N}_{B|A} \circ \mathcal{E}_{A|M=m,T}[\rho_{TT'}] \\ &= \text{Tr}[\Lambda_B(m') \mathcal{N}_{B|A} \mathcal{E}_{A|M=m,T}[\rho_{TT'}]] \\ P_{\text{agree}} &\leq \min\left(\frac{|A|^2}{|M|}, \frac{|B|^2}{|M|}, \frac{|A||T|}{|M|}, \frac{|B||T|}{|M|}, \frac{|A||T'|}{|M|}, \frac{|B||T'|}{|M|}\right) \\ &= \frac{|A|}{|M|} \min(|A|, |T|) \quad \text{for } |A| = |B|, |T| = |T'| \end{aligned}$$

q info, cl ch, assisted (teleportation)

PPT ineq: $\text{Tr}[\Phi_{AB} \sigma_{AB}] \leq \frac{1}{|A|}$ with PPT σ_{AB}

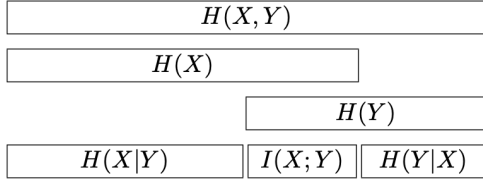
$$\begin{aligned} \mathcal{N}_{Q'|Q}[\rho_Q] &= \mathcal{D}_{Q'|YT'} \circ N_{Y|X} \circ \mathcal{E}_{X|QT}[\rho_Q \otimes \rho_{TT'}] \\ \mathcal{N}_Q[\Phi_{QQ'}] &= \mathcal{D}_{Q|YT'} \circ N_{Y|X} \circ \mathcal{E}_{X|QT}[\Phi_{QQ'} \otimes \rho_{TT'}] \\ P_{\text{agree}} &\leq \min\left(\frac{|X|}{|Q|^2}, \frac{|Y|}{|Q|^2}, \frac{|T|}{|Q|}, \frac{|T'|}{|Q|}\right) \end{aligned}$$

quantum info, quantum ch, assisted

pinching: $\mathcal{E}_{A|Q}[\Phi_{QQ'} \otimes \rho_{TT'}] \leq \frac{|A|}{|Q|} \mathbb{1}_A \otimes \mathbb{1}_{Q'} \otimes \rho_{T'}$

$$\begin{aligned} \mathcal{N}_{Q'|Q}[\rho_Q] &= \mathcal{D}_{Q'|BT'} \circ \mathcal{N}_{B|A} \circ \mathcal{E}_{A|Q}[\rho_Q \otimes \rho_{TT'}] \\ \mathcal{N}_Q[\Phi_{QQ'}] &= \mathcal{D}_{Q|BT'} \circ \mathcal{N}_{B|A} \circ \mathcal{E}_{A|Q}[\Phi_{QQ'} \otimes \rho_{TT'}] \\ P_{\text{agree}} &\leq \frac{1}{|Q|^2} \min(|A|^2, |B|^2) \end{aligned}$$

5 Entropy & Mutual Information



Relative Entropy

$$D(\rho, \sigma) := \begin{cases} \text{Tr}[\rho(\log \rho - \log \sigma)] & \text{supp}(\sigma) \subset \text{supp}(\rho) \\ \infty & \text{else} \end{cases}$$

- $D(\rho, \sigma) \geq 0$ and $D(\rho, \sigma) = 0 \iff \rho = \sigma$
- $D(\rho \otimes \theta, \sigma \otimes \tau) = D(\rho, \sigma) + D(\theta, \tau)$
- $D(\rho_{AB}, \pi \otimes \rho_B) = D(\rho_{AB}, \rho'_{AB}) + D(\rho'_{AB}, \pi \otimes \rho_B)$
with pinched $\rho'_{AB} = \mathcal{P}_A[\rho_{AB}]$ (chain rule)
- $\forall \alpha \in (0, 1) : \lim_{n \rightarrow \infty} -\frac{1}{n} \beta_\alpha(\rho^{\otimes n}, \sigma^{\otimes n}) = D(\rho, \sigma)$
- $D(\mathcal{E}_{B|A}[\rho_A], \mathcal{E}_{B|A}[\sigma_A]) \leq D(\rho_A, \sigma_A)$
- $D(\rho_A, \sigma_A) \geq -\alpha \log \beta_\alpha - h_2(\alpha)$

Entropy

$$H(A)_\rho = -\text{Tr}[\rho_A \log \rho_A] \\ = -D(\rho_A, \mathbb{1}_A) = \log |A| - D(\rho_A, \pi_A)$$

- $H(A)_\rho \geq 0$ for all ρ (duality)
- $H(A)_\rho = 0$ iff ρ pure
- $H(A)_{U\rho U^*} = H(A)_\rho$ for unitary U
- $H(A)_\rho \leq \log |\text{supp} \rho|$
- $H(A)_{\sum_k p_k \rho_k} \geq \sum_k p_k H(A)_{\rho_k}$ (convavity)
- $H(A)_\sigma \geq H(A)_\rho$ with $\sigma = \sum_k \Pi_k \rho \Pi_k$, where $\{\Pi_k\}$ is a complete set of projectors
- binary $h_2(p) := -p \log p - (1-p) \log(1-p)$

Joint Entropy

$$H(AB)_\rho := -D(\rho_{AB}, \mathbb{1}_{AB})$$

- $H(A)_\rho = H(B)_\rho$ for ρ_{AB} pure (duality)
- $H(AB)_\rho \leq H(A)_\rho + H(B)_\rho$ (subadditivity)
- $H(AB)_\rho = H(A)_\rho + H(B)_\rho$ iff $\rho_{AB} = \rho_A \otimes \rho_B$
- $H(AB)_\rho \geq |H(A)_\rho - H(B)_\rho|$ (triangle ineq)

Conditional Entropy

$$H(A|B)_\rho := -D(\rho_{AB}, \mathbb{1}_A \otimes \rho_B) \\ = \log |A| - D(\rho_{AB}, \pi_A \otimes \rho_B)$$

- $H(A|B)_\rho = -H(A|C)_\rho$ for ρ_{ABC} pure (duality)
- $-\log |A| \leq H(A|B)_\rho \leq \log |A|$
- $H(X|B)_\rho \geq 0$ for ρ_{XB} a CQ state (X classical)
- $H(A|B)_\Phi = -\log |A|$
- $H(A|BC)_\rho = H(AB|C)_\rho - H(B|C)_\rho$
- For $\mathcal{E}_{A'|A}$ unital, $\mathcal{F}_{B'|B}$, ρ_{AB} , let $\rho_{A'B'} = \mathcal{E}_{A'|A} \otimes \mathcal{F}_{B'|B}[\rho_{AB}]$. Then $H(A'|B')_{\rho'} \geq H(A|B)_\rho$
- $H(AB|C)_\rho \leq H(A|C)_\rho + H(B|C)_\rho$ (strong sub)

Mutual Information

$$I(A : B)_\rho := D(\rho_{AB}, \rho_A \otimes \rho_B) \\ = H(A)_\rho + H(B)_\rho - H(AB)_\rho \\ = H(A)_\rho - H(A|B)_\rho$$

- $I(A : B)_\rho + I(A : C)_\rho = 2H(A)_\rho$ if ρ_{ABC} pure
- $0 \leq I(A : B)_\rho \leq 2 \min(\log |A|, \log |B|)$
- $I(X : B)_\rho \leq \log |X|$ for CQ ρ_{XB}
- $I(A : B)_\rho = I(B : A)_\rho$
- $I(A : B)_\Phi = 2 \log |A|$
- For $\mathcal{E}_{A'|A}$, $\mathcal{F}_{B'|B}$ and ρ_{AB} , let $\rho_{A'B'} = \mathcal{E}_{A'|A} \otimes \mathcal{F}_{B'|B}[\rho_{AB}]$. Then $I(A' : B')_{\rho'} \leq I(A : B)_\rho$

Conditional Mutual Information

$$I(A : C|B)_\rho := H(A|B)_\rho - H(A|BC)_\rho \\ := H(B|A)_\rho - H(B|AC)_\rho$$

- $I(A : B|C)_\rho = I(A : B)$ for ρ_{ABC} pure
- $I(A : B|C)_\rho \geq 0$ (strong subadditivity)
- $I(A : B|C) = I(A : BC) - I(A : C)$

Properties of the operator log

- Let $A \in L(X)$, $B \in L(Y)$ pos. def. Then
 $\log(A \otimes B) = \log A \otimes \pi_B + \pi_A \otimes \log B$
- Let $\{A_a\}_{a \in \Sigma}$ pos. def. with mutually disjoint support. Then
 $\log \left(\sum_a A_a \right) = \sum_a \log A_a$
- If there exists a ONB such that a given operator is block diagonal, then its log is also block diagonal in this basis with the block being the log of the original block.

Important eigensystems

$$\begin{pmatrix} a & c \\ d & b \end{pmatrix} \quad \left(\frac{a-b \pm D}{2d}, \frac{1}{2}(a+b \pm D) \right), \\ D = \sqrt{(a-b)^2 + 4cd}$$

$$\begin{pmatrix} a & c^2 \\ d^2 & a \end{pmatrix} \quad \begin{pmatrix} c/d \\ \pm 1 \end{pmatrix}, a \pm cd$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 \\ \pm 1 \end{pmatrix}, \pm 1$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \begin{pmatrix} \pm i \\ i \end{pmatrix}, \mp i$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 \\ \pm 1 \end{pmatrix}, 1 \pm 1$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{pmatrix} 1 \pm \sqrt{2} \\ 1 \end{pmatrix}, \pm \sqrt{2}$$

6 Noisy Channel Coding

(k, ϵ) **code** is a pair of encoder and decoder such that $\delta(\mathcal{D} \circ \mathcal{N} \circ \mathcal{E}, \mathbb{1}) \leq \epsilon$ for an alphabet of size $k = |\mathcal{M}|$.

Capacity and rate of a channel

- $M^*(\mathcal{N}_{B|X}, \epsilon, n) =$ largest k st there exists (k, ϵ) code for $\mathcal{N}_{B|X}^{\otimes n}$
- optimal rate $R(\mathcal{N}_{B|X}, \epsilon, n) = \frac{\log M^*(\mathcal{N}_{B|X}, \epsilon, n)}{n}$
- ϵ -capacity $C(\mathcal{N}_{B|X}, \epsilon) = \lim_{n \rightarrow \infty} R(\mathcal{N}_{B|X}, \epsilon, n)$
- capacity $C(\mathcal{N}_{B|X}) = \lim_{\epsilon \rightarrow 0} C(\mathcal{N}_{B|X}, \epsilon)$

Capacities of some channels

- $C(\text{BSC}(q)) = 1 - h_2(q)$
- $C(\text{BEC}(q)) = 1 - q$

Capacity of noisy channel For any CQ channel $\mathcal{N}_{B|X}$ & assoc state $\omega_{XB} = \sum_x P(X) |x\rangle \langle x|_X \otimes \varphi_B(x)$

$$C(\mathcal{N}_{B|X}) = \max_{P_X} I(X : B)_\omega, \quad (\text{weak converse})$$

$$C(\mathcal{N}_{B|X}, \epsilon) = \max_{P_X} I(X : B)_\omega. \quad (\text{strong converse})$$

- strong conv: max capacity is independent of ϵ
- weak conv: rates larger than C cannot transmit with vanishing ϵ

Noisy channel coding converse For any CQ channel $\mathcal{N}_{B|X}$, every (k, ϵ) code satisfies

$$\min_{P_X} \max_{\sigma_B} \beta_{1-\epsilon}(\omega_{XB}, \omega_X \otimes \sigma_B) \leq \frac{1}{k},$$

where $\omega_{XB} = \sum_x P_X(x) |x\rangle \langle x|_X \otimes \varphi_B(x)$ for $\varphi_B(x) = \mathcal{N}_{B|X=x}$.

Noisy channel coding achievability For any CQ channel $\mathcal{N}_{B|X}$ and error $\epsilon > 0$, there exists a (k, ϵ) code with

$$\frac{1}{k} \leq \min_{\eta \in [0, \epsilon]} \min_{P_X} \frac{1 - \epsilon}{\eta(1 - \epsilon + \eta)} \beta_{1-\epsilon+\eta}(\omega_{XB}, \omega_X \otimes \omega_B).$$