Characterizations of sufficient quantum channels

Anna Jenčová
Mathematical Institute, Slovak Academy of Sciences

Beyond IID in Information Theory, BIRS, July 2015

Some basic references

- D. Petz: Sufficient subalgebras and the relative entropy of states of a von Neumann algebra, Commun. Math. Phys, 105 (1986)
- D. Petz: Sufficiency of channels over von Neumann algebras, Quart. J. Math. Oxford, 39 (1988)
- M. Mosonyi, D. Petz: Structure of sufficient quantum coarse-grainings, Let. Math. Phys, 68 (2004)
- A. Jenčová, D. Petz: Sufficiency in quantum statistical inference, Commun. Math. Phys. 263 (2006)
- F. Hiai, M. Mosonyi, D. Petz, C. Beny: Quantum f-divergences and error correction, Rev. Math. Phys, 23 (2011)
- A. Jenčová: Reversibility conditions for quantum operations, Rev. Math. Phys, 24 (2012)

Classical sufficiency

- A statistical model: a family

$$\{P_\theta,\ \theta \in \Theta\}$$

  of probability distributions on a sample space (X, Ω)
- A statistic: measurable map $T : (X, \Omega) \to (Y, \Sigma)$
- T is sufficient if the conditional probability does not depend on θ:

$$P_\theta(X|T) = P(X|T), \qquad \forall \theta \in \Theta$$

  In this case, the transformed vector $Y = T(X)$ contains all information about the parameter

R.A. Fisher, Philos. T. Roy. Soc. A, 222 (1922).

Quantum sufficiency

- Let $\mathcal{S} \subset \mathcal{S}(\mathcal{H})$ be a set of quantum states (density operators on a Hilbert space $\mathcal{H}$)
- Let $T : B(\mathcal{H}) \to B(\mathcal{K})$ be a quantum channel

$$T : \mathcal{S} \mapsto T(\mathcal{S}) \subset \mathcal{S}(\mathcal{K})$$

- T is sufficient (or also reversible) with respect to $\mathcal{S}$ if there is some

$$R : B(\mathcal{K}) \to B(\mathcal{H}) \quad \text{recovery channel}$$

such that

$$R \circ T(\rho) = \rho \qquad \forall \rho \in \mathcal{S}$$

Sufficient subalgebras

We assume $\dim(\mathcal{H}) < \infty$, $\mathcal{S}$ contains a faithful state.

- Let $\mathcal{A} \subseteq B(\mathcal{H})$ be a *-subalgebra, $T_{\mathcal{A}} : B(\mathcal{H}) \to \mathcal{A}$ the trace preserving conditional expectation

$$T_{\mathcal{A}} : \rho \mapsto \rho|_{\mathcal{A}}$$

- If $T_{\mathcal{A}}$ is sufficient, then $\mathcal{A}$ is a sufficient subalgebra
- The recovery channel R satisfies

$$R(\rho) = R(\rho|_{\mathcal{A}}) = \rho, \quad \rho \in \mathcal{S}$$

Minimal sufficient subalgebra

Let $\mathcal{I}_{\mathcal{S}}$ be the set of all unital cp maps Φ on $B(\mathcal{H})$, such that

$$\Phi^*(\rho) = \rho, \quad \rho \in \mathcal{S}$$

- $\mathcal{I}_{\mathcal{S}}$ is a closed convex semigroup of unital cp maps.
- By the mean ergodic theorem, there is a (faithful) conditional expectation $E \in \mathcal{I}_{\mathcal{S}}$ such that

$$\Phi \in \mathcal{I}_{\mathcal{S}} \text{ if and only if } \Phi \circ E = E \circ \Phi = E.$$

- The range of E,

$$\mathcal{F}_{\mathcal{S}} := E(B(\mathcal{H})) = \{X \in B(\mathcal{H}), \Phi(X) = X, \forall \Phi \in \mathcal{I}_{\mathcal{S}}\}$$

- In particular, $\mathcal{F}_{\mathcal{S}}$ is a subalgebra in $B(\mathcal{H})$.

Kümmerer and Nagel, Ann. Sci. Math, 41 (1979), 151-159

Minimal sufficient subalgebra

- Since $E \in \mathcal{I}_{\mathcal{S}}$, we have

$$\rho = E^*(\rho) = E^*(\rho|_{\mathcal{F}_{\mathcal{S}}}), \quad \rho \in \mathcal{S},$$

that is, E^* is a recovery channel for the channel $T_{\mathcal{F}_{\mathcal{S}}}$:

$$\Longrightarrow \quad \mathcal{F}_{\mathcal{S}} \text{ is a sufficient subalgebra}$$

- A subalgebra $\mathcal{A} \subseteq B(\mathcal{H})$ is sufficient if and only if $\mathcal{F}_{\mathcal{S}} \subseteq \mathcal{A}$
- $\mathcal{F}_{\mathcal{S}}$ is minimal sufficient

A. Luczak, Int. J. Theor. Phys, 53 (2014)

Minimal sufficient subalgebra

Let $\omega \in \mathcal{S}$ be a faithful state.

- Since E is a conditional expectation and $E^*(\omega) = \omega$,

$$\omega^{it} \mathcal{F}_{\mathcal{S}} \omega^{-it} \subseteq \mathcal{F}_{\mathcal{S}}, \quad t \in \mathbb{R}$$

- The algebra $\mathcal{F}_{\mathcal{S}}$ is generated by the Radon-Nikodym cocycles

$$\rho^{it} \omega^{-it}, \quad t \in \mathbb{R}, \ \rho \in \mathcal{S}$$

- A subalgebra $\mathcal{A}$ is sufficient if and only if

$$\rho^{it} \omega^{-it} \in \mathcal{A}, \quad t \in \mathbb{R}, \ \rho \in \mathcal{S}$$

- By analytic continuation

$$\rho^{z} \omega^{-z} \in \mathcal{A}, \quad z \in \mathbb{C}, \ \rho \in \mathcal{S}$$

Factorization of states in $\mathcal{S}$

There is a decomposition $\mathcal{H} = \bigoplus_j \mathcal{H}_j^L \otimes \mathcal{H}_j^R$ such that

$$\mathcal{F}_{\mathcal{S}} = \bigoplus_j B(\mathcal{H}_j^L) \otimes I_{\mathcal{H}_j^R},$$

$$E^*(\sigma) = \bigoplus_j \mathrm{Tr}_{\mathcal{H}_j^R}[P_j \sigma P_j] \otimes \omega_j^R, \quad \omega_j^R \in \mathcal{S}(\mathcal{H}_j^R)$$

$P_j = \mathcal{H} \to \mathcal{H}_j^L \otimes \mathcal{H}_j^R$ is the projection. Since $\rho = E^*(\rho)$ for $\rho \in \mathcal{S}$,

$$\rho = \bigoplus p_j(\rho) \rho_j^L \otimes \omega_j^R, \qquad \rho \in \mathcal{S},$$

where $p_j(\rho) = \mathrm{Tr}\,[\rho P_j]$, $\rho_j^L \in \mathcal{S}(\mathcal{H}_j^L)$.

M. Koashi and N. Imoto, Phys. Rev. A, 66 (2002)
P. Hayden, R. Jozsa, D. Petz, A. Winter, Commun. Math. Phys. 246 (2004)

Sufficient channels

Let $T : B(\mathcal{H}) \to B(\mathcal{K})$ be a channel, suppose there exists a recovery channel $R : B(\mathcal{K}) \to B(\mathcal{H})$. Then $R \circ T(\rho) = \rho$ for $\rho \in \mathcal{S}$, so that

$$T^* \circ R^* \in \mathcal{I}_{\mathcal{S}}$$

T is sufficient with respect to $\mathcal{S}$ if and only if there is some unital cp map β such that

$$T^* \circ \beta = E \qquad (\beta = R^* \circ E)$$

Sufficient channels

Let $T(\mathcal{S}) = \{T(\rho),\ \rho \in \mathcal{S}\}$. Assume $T(\omega)$ is faithful. The following are equivalent.

- T is sufficient with respect to $\mathcal{S}$
- $T^*|_{\mathcal{F}_{T(\mathcal{S})}}$ is a homomorphism and for $A \in \mathcal{F}_{T(\mathcal{S})}$,

$$T^*(T(\omega)^{it} A T(\omega)^{-it}) = \omega^{it} T^*(A) \omega^{-it}, \quad t \in \mathbb{R}$$

- $T^*(T(\rho)^{it} T(\omega)^{-it}) = \rho^{it} \omega^{-it}$, $t \in \mathbb{R}$, $\rho \in \mathcal{S}$
- $T^*(T(\rho)^{z} T(\omega)^{-z}) = \rho^{z} \omega^{-z}$, $z \in \mathbb{C}$, $\rho \in \mathcal{S}$
- $T^*(T(\rho)^{p} T(\omega)^{-p}) = \rho^{p} \omega^{-p}$ for some $p \in (0, 1)$

Sufficient channels - factorization

T is sufficient with respect to $\mathcal{S}$ if and only if there is a decomposition

$$\mathcal{K} = \bigoplus_j \mathcal{K}_j^L \otimes \mathcal{K}_j^R$$

such that

$$T = \bigoplus_j U_j \otimes T_j$$

for some unitary channels $U_j : B(\mathcal{H}_j^L) \to B(\mathcal{K}_j^L)$ and some channels $T_j : B(\mathcal{H}_j^R) \to B(\mathcal{K}_j^R)$

The dual map

Let $T : B(\mathcal{H}) \to B(\mathcal{K})$ be a channel, $\omega \in \mathcal{S}(\mathcal{H})$ a faithful state.

- The dual map of T with respect to ω is the channel $T_\omega : B(\mathcal{K}) \to B(\mathcal{H})$, defined by

$$T_\omega(B) = \omega^{1/2} T^*(T(\omega)^{-1/2} B T(\omega)^{-1/2}) \omega^{1/2}$$

- Alternatively, T_ω^* is the adjoint of T^*:

$$\langle A, T^*(B) \rangle_\omega = \langle T_\omega^*(A), B \rangle_{T(\omega)}, \quad A \in B(\mathcal{H}), B \in B(\mathcal{K})$$

  with respect to the inner product

$$\langle A, B \rangle_\omega = \mathrm{Tr}\, A^\dagger \omega^{1/2} B \omega^{1/2}$$

D. Petz, Quart. J. Math. Oxford, 35 (1984)

The dual map as a recovery channel

$T^* \circ T^*_\omega$ is a unital cp map on $B(\mathcal{H})$, preserving a faithful state,

$$T_\omega \circ T(\omega) = \omega.$$

Again by mean ergodic theorem, there exists a conditional expectation F on $B(\mathcal{H})$, $F^*(\omega) = \omega$, with range

$$F(B(\mathcal{H})) = \{A, T^* \circ T^*_\omega(A) = A\}$$

and this satisfies

$$T^* \circ T^*_\omega \circ F = F.$$

The dual map as a recovery channel

Let ω be a faithful state, E be a conditional expectation, $E^*(\omega) = \omega$. The following are equivalent.

- There exists some unital cp map β such that $T^* \circ \beta = E$.
- $F \circ E = E \circ F = E \quad (E \subseteq F)$
- $T^* \circ T_\omega^* \circ E = E$
- $T_\omega = T_\rho$ for all faithful states ρ such that $E^*(\rho) = \rho$.
- T is sufficient for $\mathcal{S}_E = \{E^*(\rho), \rho \in \mathcal{S}(\mathcal{H})\}$.

Moreover, $\beta \circ E = T_\omega^* \circ E$.

Corollary

If T is sufficient with respect to $\mathcal{S}$, then T_ω is a recovery channel.

A Radon-Nikodym derivative

Let $\rho, \omega \in \mathcal{S}(\mathcal{H})$, ω faithful. We define a Radon-Nikodym derivative

$$d(\rho, \omega) = \omega^{-1/2} \rho \omega^{-1/2}$$

Alternatively: $\langle d(\rho, \omega), A \rangle_\omega = \mathrm{Tr}\, \rho A, \qquad A \in B(\mathcal{H})$.

Properties:

- $d(\rho, \omega) \geq 0$
- $\log \| d(\rho, \omega) \| = D_{max}(\rho, \omega)$ (max relative entropy)
- note that the sandwiched Rényi relative entropy is

$$\tilde{D}_\alpha(\rho, \omega) = \frac{\alpha}{\alpha - 1} \log \| d(\rho, \omega) \|_{\alpha, \omega}$$

where

$$\|A\|_{\alpha,\omega}^{\alpha} = \mathrm{Tr}\, |\omega^{\frac{1}{2\alpha}} A \omega^{\frac{1}{2\alpha}}|^{\alpha}$$

Sufficiency characterization

Let T be a channel, it is easy to see that

$$T_\omega^*(d(\rho,\omega)) = d(T(\rho), T(\omega))$$

and

$$T_\omega \circ T(\rho) = \rho \iff T^*(d(T(\rho), T(\omega))) = d(\rho,\omega)$$

T is sufficient

- iff the last equality holds for all $\rho \in \mathcal{S}$
- iff $d(\rho,\omega)$ is in the fixed points domain of $T^* \circ T_\omega^*$.

Operator convex functions

- $f : [0,\infty) \to \mathbb{R}$,

$$f(\lambda A + (1-\lambda)B) \leq \lambda f(A) + (1-\lambda) f(B)$$

  for all $0 \leq A, B \in B(\mathcal{H})$, $\dim(\mathcal{H}) < \infty$, $\lambda \in (0,1)$.
- Integral representation of operator convex functions:

$$f(x) = f(0) + ax + bx^2 + \int_{(0,\infty)} (\frac{x}{1+t} - \frac{x}{x+t}) d\mu_f(t)$$

  $a \in \mathbb{R}$, $b \geq 0$, μ_f is a measure on $(0,\infty)$ such that $\int (1+t)^{-2} d\mu_f(t) < \infty$

Generalized divergences

- Let $\tilde{\mathcal{H}} \equiv B(\mathcal{H})$ with inner product

$$\langle A, B \rangle = \mathrm{Tr}\, A^\dagger B$$

- Relative modular operator: $\rho, \omega \in \mathcal{S}(\mathcal{H})$, ω faithful

$$\Delta_{\rho,\omega}(A) = \rho A \omega^{-1}, \qquad A \in \tilde{\mathcal{H}}$$

  a positive operator on $\tilde{\mathcal{H}}$

- Generalized divergence: for f operator convex,

$$D_f(\rho, \omega) = \langle \omega^{1/2}, f(\Delta_{\rho,\omega})\omega^{1/2} \rangle$$

D. Petz, Rep. Math. Phys., 21 (1986)

Generalized divergences - examples

- relative entropy: $f(x) = x \log(x)$

$$D(\rho, \omega) = \mathrm{Tr}\, \rho(\log \rho - \log \omega)$$

- α-divergence: $f_\alpha(x) = 1 - x^\alpha$, $\alpha \in (0, 1)$

$$D_\alpha(\rho, \omega) = 1 - \mathrm{Tr}\, \rho^\alpha \omega^{1-\alpha}$$

- $\varphi_t(x) = -\frac{x}{x+t}$, $t \in (0, 1)$

$$D_t(\rho, \omega) = -\mathrm{Tr}\, \omega^{1/2}(L_\rho + tR_\omega)^{-1}(\rho\omega^{1/2})$$

- quadratic divergence: $\varphi_0(x) = x^2$

$$D_0(\rho, \omega) = \mathrm{Tr}\, \rho^2 \omega^{-1}$$

Monotonicity

Theorem

Let $T : B(\mathcal{H}) \to B(\mathcal{K})$ be a channel, f operator convex. Then

$$D_f(\rho, \omega) \geq D_f(T(\rho), T(\omega))$$

- define $V : \tilde{\mathcal{K}} \to \tilde{\mathcal{H}}$ by

$$V : AT(\omega)^{1/2} \mapsto T^*(A)\omega^{1/2}, \qquad A \in B(\mathcal{K})$$

- By Kadison-Schwarz inequality $T^*(A)^\dagger T^*(A) \leq T^*(A^\dagger A)$, V is a contraction and

$$V^* \Delta_{\rho,\omega} V \leq \Delta_{T(\rho),T(\omega)}$$

Monotonicity

- By operator Jensen inequality, for an operator monotone function g such that $g(0) \geq 0$:

$$g(\Delta_{T(\rho),T(\omega)}) \geq g(V^*\Delta_{\rho,\omega}V) \geq V^*g(\Delta_{\rho,\omega})V$$

- D_α is monotone, $\alpha \in (0,1)$ (put $g(x) = 1 - f_\alpha(x) = x^\alpha$)
- D_t is monotone, $t \in (0,\infty)$ (put $g(x) = -\varphi_t(x) = \frac{x}{x+1}$)
- D_0 is monotone by the generalized Kadison-Schwarz inequality

$$T(\rho)T(\omega)^{-1}T(\rho) \leq T(\rho\omega^{-1}\rho)$$

- By the integral representation,

$$D_f(\rho,\omega) = D_0(\rho,\omega) + \int_{(0,\infty)} (\frac{1}{1+t} + D_t(\rho,\omega))d\mu_f(t)$$

Equality in the monotonicity

Assume that

$$D(T(\rho), T(\omega)) = D(\rho, \omega)$$

Then $D_t(T(\rho), T(\omega)) = D_t(\rho, \omega)$ for all $t \in \mathrm{supp}(\mu_f)$, so that

$$V^*(\Delta_{\rho,\omega} + t)^{-1}\omega^{1/2} = (\Delta_{T(\rho),T(\omega)} + t)^{-1} T(\omega)^{1/2}, \ \ t \in \mathrm{supp}(\mu_f)$$

If $|\mathrm{supp}(\mu_f)| \geq \dim(\mathcal{H})^2 + \dim(\mathcal{K})^2$, we get

$$h(\Delta_{\rho,\omega})\omega^{1/2} = Vh(\Delta_{T(\rho),T(\omega)})T(\omega)^{1/2}$$

for (bounded continuous) functions $h : [0, \infty) \to \mathbb{C}$.

Equality in the monotonicity

Put $h(x) = x^{is}$, $s \in \mathbb{R} \implies$

$$T^*(T(\rho)^{is} T(\omega)^{-is}) = \rho^{is} \omega^{-is}, \quad s \in \mathbb{R}$$

Theorem

Let f be an operator convex function such that $|\mathrm{supp}(\mu_f)| \geq \dim(\mathcal{H})^2 + \dim(\mathcal{K})^2$. Then T is sufficient with respect to $\mathcal{S}$ if and only if

$$D_f(T(\rho), T(\omega)) = D_f(\rho, \omega), \qquad \rho \in \mathcal{S}$$

Examples and counterexamples

- Equality implies sufficiency:

$$D,\ \ D_\alpha, \alpha \in (0,1)$$

- Equality does not imply sufficiency

$$D_0,\ \ D_t, t \in (0,\infty) \quad (f(x) = x^2,\ \ f(x) = \frac{1}{x+t})$$

Strong subadditivity of entropy

Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, then

$$S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{BC}),$$

where

$$S(\rho) = -\mathrm{Tr}\,\rho \log(\rho).$$

Equivalently,

$$D(\rho_{AB}, \rho_A \otimes \rho_B) \leq D(\rho_{ABC}, \rho_A \otimes \rho_{BC})$$

Equality in SSA and Markov property

Suppose

$$S(\rho_{ABC}) + S(\rho_B) = S(\rho_{AB}) + S(\rho_{BC})$$

Then

- Tr_C is sufficient with respect to $\{\rho_{ABC}, \rho_A \otimes \rho_{BC}\}$
- $\rho_{ABC} = T_{\rho_A \otimes \rho_{BC}}(\rho_{AB})$
- There is a decomposition $\mathcal{H}_B = \bigoplus_n \mathcal{H}^L_{Bn} \otimes \mathcal{H}^R_{Bn}$ such that

$$\rho_{ABC} = \bigoplus_n \lambda_n \rho^L_{ABn} \otimes \rho^R_{BCn}$$

where $\rho^L_{ABn} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}^L_{Bn})$, $\rho^R_{BCn} \in \mathcal{S}(\mathcal{H}^R_{Bn} \otimes \mathcal{H}_C)$.

P. Hayden, R. Jozsa, D. Petz, A. Winter, Commun. Math. Phys. 246 (2004)

Quantum hypothesis testing

Let $\rho, \omega \in \mathcal{S}(\mathcal{H})$. Consider the problem of testing the hypothesis $H_0 = \rho$ against the alternative $H_1 = \omega$.

- tests: $0 \leq M \leq I$, where

$$\mathrm{Tr}\, M\sigma = \text{probability of rejecting } H_0 \text{ if the state is } \sigma$$

- error probabilities

$$\alpha(M) = \mathrm{Tr}\, M\rho, \qquad \beta(M) = \mathrm{Tr}\,(I - M)\omega$$

- Minimum Bayes error probability: $\lambda \in (0,1)$,

$$\Pi_\lambda = \min_{0 \leq M \leq I} \lambda\alpha(M) + (1-\lambda)\beta(M) = \frac{1}{2}(1 - \|\lambda\rho - (1-\lambda)\omega\|_1)$$

Monotonicity

Let T be a channel, $H_0' = T(\rho)$, $H_1' = T(\omega)$.

- error probabilities: $0 \leq N \leq I$,

$$\alpha'(N) = \mathrm{Tr}\, T^*(N)\rho, \qquad \beta'(N) = \mathrm{Tr}\,(1 - T^*(N))\omega$$

- the minimum Bayes error probability cannot be smaller:

$$\Pi'_\lambda = \min_{0 \leq N \leq I} \lambda\alpha(T^*(N)) + (1-\lambda)\beta(T^*(N)) \geq \Pi_\lambda$$

- equivalently,

$$\|T(\rho) - tT(\omega)\|_1 \leq \|\rho - t\omega\|_1, \qquad t \in \mathbb{R}$$

Equality and sufficiency

In the classical case (ρ and ω commute), T is sufficient with respect to $\{\rho, \omega\}$ if and only

$$\|T(\rho) - tT(\omega)\|_1 = \|\rho - t\omega\|_1, \qquad t \in \mathbb{R}$$

Some further cases when this equivalence holds:

- $T(\rho)$ and $T(\omega)$ commute
- $\dim(\mathcal{H}) = \dim(\mathcal{K}) = 2$
- T^* commutes with the modular groups:

$$\omega^{it} T^*(A) \omega^{-it} = T^*(T(\omega)^{it} A T(\omega)^{-it}), \quad A \in B(\mathcal{K}), t \in \mathbb{R}$$

Equality and sufficiency

Theorem

T is sufficient with respect to $\mathcal{S}$ if and only if

$$\|T(\sigma) - tT(\omega)\|_1 = \|\sigma - t\omega\|_1, \qquad t \in \mathbb{R}$$

holds for all $\sigma \in \tilde{\mathcal{S}} = \{\omega^{is}\rho\omega^{-is},\ s \in \mathbb{R}, \rho \in \mathcal{S}\}$.

i.i.d. sequences and quantum Chernoff distance

Take n copies, $H_0^n = \rho^{\otimes n}$, $H_1^n = \omega^{\otimes n}$,

$$\Pi_{\lambda,n} = \frac{1}{2}(1 - \|\lambda\rho^{\otimes n} - (1-\lambda)\omega^{\otimes n}\|_1)$$

Quantum Chernoff distance:

$$-\lim_n \frac{1}{n}\log(\Pi_{\lambda,n}) = -\log\left(\inf_{0\le s\le 1} \operatorname{Tr}\rho^s\omega^{1-s}\right) =: C(\rho,\omega)$$

Monotonicity: if T is a channel,

$$C(\rho,\omega) \ge C(T(\rho), T(\omega))$$

K.M.R. Audenaert, M. Nussbaum, A. Szkola, F. Verstraete, Comm. Math. Phys. 279 (2008)

Conditions for sufficiency

Theorem

The following are equivalent.

- $\|T(\sigma)^{\otimes n} - tT(\omega)^{\otimes n}\|_1 = \|\rho^{\otimes n} - t\omega^{\otimes n}\|_1$, $t \in \mathbb{R}$, $\rho \in \mathcal{S}$, $n \in \mathbb{N}$
- $C(\rho, \omega) = C(T(\rho), T(\omega))$, $\rho \in co(\mathcal{S})$ *(or* $\rho \in \mathcal{S}$ *if all elements in* $\mathcal{S}$ *are faithful)*
- T *is sufficient with respect to* $\mathcal{S}$*.*

Multiple hypothesis testing

An ensemble $\{\lambda_i, \rho_i\}_{i=1}^n$, $0 \leq \lambda_i$, $\sum_i \lambda_i = 1$, $\rho_i \in \mathcal{S}(\mathcal{H})$

Assume $\rho = \rho_i$ with prior probability λ_i, $i = 1, \ldots, n$.

- test: $M_1, \ldots, M_n$, $M_i \geq 0$, $\sum_i M_i = I$

  $\mathrm{Tr}\, M_i \rho$ is the probability that we choose ρ_i

- Optimal success probability:

$$P(\{\lambda_i, \rho_i\}) = \max_{M_i \geq 0, \sum M_i = I} \sum_i \lambda_i \mathrm{Tr}\, \rho M_i$$

Approximate sufficiency and multiple hypothesis testing

Let $\mathcal{S} = \{\rho_1, \dots, \rho_n\}$, $T : B(\mathcal{H}) \to B(\mathcal{K})$ a channel, $\epsilon \geq 0$. The following are equivalent.

- For any ensemble $\{\frac{1}{d^2}, \sigma^j\}_{j=1}^{d^2}$, where $d = \dim(\mathcal{K})$ and

$$\sigma^j = \sum_{i=1}^{n} |i\rangle\langle i| \otimes \sigma_i^j, \ \sigma_i^j \in B(\mathcal{K})^+, \ j = 1, \dots, d^2,$$

  we have

$$P(\{\frac{1}{d^2}, \sum_i \rho_i \otimes \sigma_i^j\}_j) \leq P(\{\frac{1}{d^2}, \sum_i T(\rho_i) \otimes \sigma_i^j\}_j) + \frac{\epsilon}{2} P(\{\frac{1}{d^2}, \sigma^j\}_j)$$

- T is ϵ-sufficient with respect to $\mathcal{S}$: there is some channel R_ϵ such that

$$\max_i \|\rho_i - R_\epsilon \circ T(\rho_i)\|_1 \leq \epsilon$$

A. Jenčová, arxiv:1404.3900