41076: Methods in Quantum Computing

‘Quantum Information’ Module

Min-Hsiu Hsieh
Centre for Quantum Software & Information, Faculty of Engineering and Information Technology, University of Technology Sydney

Abstract

Contents to be covered in this lecture are

1. Quantum Channels;
   - Kraus representation
   - Stinespring dilation
2. Distance Measures;
   - Trace distance
   - Fidelity
3. State Discrimination.
   - Helstrom bound

Notations

For a Hilbert space $\mathcal{H}$, let

- $\mathcal{L}(\mathcal{H})$ denote the collection of linear operators acting on $\mathcal{H}$,
- $\mathcal{L}(\mathcal{H})_+$ denote the set of positive semi-definite operators on $\mathcal{H}$,
- $\mathcal{D}(\mathcal{H})$ denote the set of density matrices (or states), i.e., positive semi-definite operators of unit trace.

Unless otherwise stated, we assume all Hilbert spaces to be finite-dimensional. We will denote the dimensionality of a Hilbert space $\mathcal{H}_A$ by d_A, or simply by d if the subscript is not specified. We denote the identity map by id, and denote the identity operator on $\mathcal{H}_B$ by I_B.

1 Quantum Channels

Recall that in the first lecture, we introduced the system evolution, which can be modelled as a unitary operation, in a close (noiseless) environment. Here, we will introduce a more general system evolution: a noisy quantum channel $\mathcal{N}^{A\to B}$, which is a completely-positive trace-preserving (CPTP) map, because it takes a quantum state $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ as an input and produces another quantum state $\sigma_B \in \mathcal{D}(\mathcal{H}_B)$ as the output.

1. Recall that a quantum state is a positive semi-definite matrix with unit trace. Since the channel maps a positive semi-definite matrix to another positive semi-definite matrix, it has to be a positive map. Furthermore, this has to hold true even if the input to the quantum channel is only part of a larger quantum system:
$$\sigma_{BR} = \mathrm{id}_R \otimes \mathcal{N}^{A\to B}(\rho_{AR}) \in \mathcal{D}(\mathcal{H}_{BR}). \tag{1}$$
Hence, the quantum channel has to be completely positive.
2. The trace-preserving condition follows since both the input and output quantum states have equal trace.

Exercise 1 *Show that transpose is a positive map, but not a completely positive map.*

Definition 2 *A quantum channel $\mathcal{N}$ is unital if $\mathcal{N}(I) = I$.*

Examples

- Dephasing Channel:
$$\mathcal{N}(\rho) = (1-p)\rho + pZ\rho Z.$$
- Depolarizing Channel:
$$\mathcal{N}(\rho) = (1-p)\rho + p\pi,$$
where π is the completely mixed state.
- Pauli Channel:
$$\mathcal{N}(\sigma) = \sum_{i,j=0}^{1} p(i,j) Z^i X^j \sigma X^j Z^i$$
where we denote $X^0 = Z^0 = I$.
- Measure-and-prepare channel: For a POVM $\{\Lambda_i\}$ and a collection of quantum states $\{\sigma_i\}$, we can define
$$\mathcal{N}(\rho) = \sum_i \sigma_i \operatorname{Tr}(\Lambda_i \rho). \tag{2}$$
This channel is also known as an *entanglement-breaking* channel.

Exercise 3 *The set of generalized Pauli matrices $\{U_m\}_{m\in[d^2]}$ is defined by $U_{l\cdot d+k} = \hat{Z}_d(l)\hat{X}_d(k)$ for $k, l = 0, 1, \cdots, d-1$ and*
$$\begin{aligned} \hat{X}_d(k) &= \sum_s |s\rangle\langle s+k| = \hat{X}_d(1)^k, \\ \hat{Z}_d(l) &= \sum_s e^{i2\pi sl/d}|s\rangle\langle s| = \hat{Z}_d(1)^l. \end{aligned} \tag{3}$$
The + sign denotes addition modulo d. Show that
$$\frac{1}{d^2}\sum_{m=1}^{d^2} U_m \rho U_m^\dagger = \pi, \tag{4}$$
where $\pi = \frac{I}{d}$.

1.1 Kraus Representation

Denote

$$|\Gamma\rangle_{RA} = \sum_{i=1}^{d_A} |i\rangle_R \otimes |i\rangle_A \in \mathcal{H}_R \otimes \mathcal{H}_A \tag{5}$$

with $|\mathcal{H}_A| = |\mathcal{H}_R| = d_A$. Recall Choi's theorem on completely positive maps: $\mathcal{N}^{A\to B}$ is completely positive if and only if its Choi matrix

$$C_{\mathcal{N}} := (\mathrm{id}_R \otimes \mathcal{N}^{A\to B})(|\Gamma\rangle\langle\Gamma|_{RA}) \in \mathcal{L}(\mathcal{H}_R \otimes \mathcal{H}_B)_+ \tag{6}$$

is positive. A consequence of Choi's theorem implies that $\mathcal{N}$ is completely positive if and only if it can be expressed as

$$\mathcal{N}(A) = \sum_i K_i A K_i^\dagger, \tag{7}$$

where $\{K_i\}$ are known as Kraus operators of $\mathcal{N}$. If $\mathcal{N}$ is also trace preserving, then $\sum_i K_i^\dagger K_i = I$. Specifically, assume that the Choi matrix has the following spectral decomposition

$$C_{\mathcal{N}} = \sum_{k=1}^{d_A d_B} |\nu_k\rangle\langle\nu_k|, \tag{8}$$

where we abuse notation slightly because $\{|\nu_k\rangle\}$ are not necessarily normalized. Note that

$$\begin{aligned}
\mathcal{N}(|i\rangle\langle j|) &= (\langle i| \otimes I_B) C_{\mathcal{N}} (|j\rangle \otimes I_B) && (9)\\
&= (\langle i| \otimes I_B) \left(\sum_{\ell=1}^{d_A d_B} |\nu_\ell\rangle\langle\nu_\ell| \right) (|j\rangle \otimes I_B) && (10)\\
&= \sum_{\ell=1}^{d_A d_B} (\langle i| \otimes I_B) |\psi_\ell\rangle\langle\psi_\ell| (|j\rangle \otimes I_B). && (11)
\end{aligned}$$

Now we can define the set of operators $\{K_\ell : \mathcal{H}_A \to \mathcal{H}_B\}$ by the following relations: $\forall |i\rangle$,

$$K_\ell |i\rangle_A = (\langle i| \otimes I_B)|\nu_\ell\rangle. \tag{12}$$

Then

$$\mathcal{N}(|i\rangle\langle j|) = \sum_{\ell=1}^{d_A d_B} K_\ell |i\rangle\langle j|_A K_\ell^\dagger. \tag{13}$$

Linearity of $\mathcal{N}$ yields

$$\mathcal{N}(\rho_A) = \sum_{\ell=1}^{d_A d_B} K_\ell \rho_A K_\ell^\dagger. \tag{14}$$

Finally,

$$\begin{aligned} I_R &= \mathrm{Tr}_B\big\{(\mathrm{id}_R \otimes \mathcal{N}^{A\to B})(|\Gamma\rangle\langle\Gamma|_{RA})\big\} && (15)\\ &= \mathrm{Tr}_B\left\{\sum_\ell (I_R\otimes K_\ell)(|\Gamma\rangle\langle\Gamma|_{RA})(I_R\otimes K_\ell^\dagger)\right\} && (16)\\ &= \mathrm{Tr}_B\left\{\sum_\ell (K_\ell^T\otimes I_A)(|\Gamma\rangle\langle\Gamma|_{RA})(K_\ell^*\otimes I_A^\dagger)\right\} && (17)\\ &= \sum_\ell K_\ell^T K_\ell^*, && (18)\end{aligned}$$

where $|\Gamma\rangle_{RA}$ in the first line is given in Eq. (5); the second line uses Eq. (13); and the third equality uses

$$(I_R\otimes A)|\Gamma\rangle_{RA} = (A^T\otimes I_A)|\Gamma\rangle_{RA}. \tag{19}$$

Therefore $\sum_i K_i^\dagger K_i = I$ can be obtained by taking conjugation on Eq. (18).

Take Home

A quantum channel can be described by a corresponding Kraus operators $\{K_i\}$.

1.2 Stinespring Dilation

For a quantum channel $\mathcal{N}^{A\to B}$ with the following Kraus representation

$$\mathcal{N}^{A\to B}(\sigma_A) = \sum_i K_i\sigma_A K_i^\dagger, \tag{20}$$

it can be modeled by an isometry $U_\mathcal{N}: A\to BE$ with a larger target space BE, followed by tracing out the "environment" system E. Specifically,

$$U_\mathcal{N}^{A\to BE} := \sum_i K_i\otimes|i\rangle_E. \tag{21}$$

Note that $U_\mathcal{N}$ is known as the Stinespring dilation [7] of $\mathcal{N}$. We will often write $U_\mathcal{N}(\rho)$ for $U_\mathcal{N}\,\rho\,U_\mathcal{N}^\dagger$. The Stinespring dilation is commonly used when we choose to work in the purified setting, as illustrated in Figure 1. Let $|\psi^\rho\rangle_{AR}$ be the purification of ρ_A. The output of $U_\mathcal{N}$ will become

$$|\Psi\rangle_{RBE} = I_R\otimes U_\mathcal{N}|\psi^\rho\rangle_{AR}. \tag{22}$$

It follows that

$$\mathcal{N}(\rho_A) = \mathrm{Tr}_{RE}|\Psi\rangle\langle\Psi|_{RBE}. \tag{23}$$

Exercise 4 *Verify that $U_\mathcal{N}^\dagger U_\mathcal{N} = I_A$, where $U_\mathcal{N}$ is given in Eq. (21).*

Exercise 5 *Verify that*

$$\mathrm{Tr}_E\, U_\mathcal{N}(\sigma_A) = \sum_i K_i\sigma_A K_i^\dagger.$$

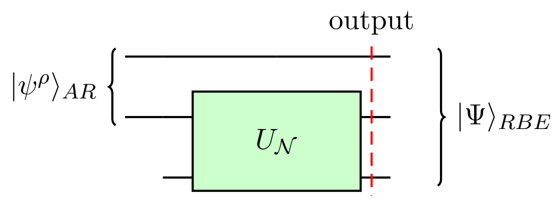

Figure 1: Purified picture of a quantum channel.

Further reading

A *conditional quantum encoder* $\mathcal{E}^{MA\to B}$, or *conditional quantum channel* , is a collection $\{\mathcal{E}_m^{A\to B}\}_m$ of CPTP maps. Its inputs are a classical system M and a quantum system A and its output is a quantum system B. A classical-quantum state ρ^{MA}, where

$$\rho^{MA} \equiv \sum_m p(m)|m\rangle\langle m|^M \otimes \rho_m^A,$$

can act as an input to the conditional quantum encoder $\mathcal{E}^{MA\to B}$. The action of the conditional quantum encoder $\mathcal{E}^{MA\to B}$ on the classical-quantum state ρ^{MA} is as follows:

$$\begin{aligned}&\mathcal{E}^{MA\to B}\left(\rho^{MA}\right)\\ &= \operatorname{Tr}_M\left\{\sum_m p(m)|m\rangle\langle m|^M \otimes \mathcal{E}_m^{A\to B}\left(\rho_m^A\right)\right\}.\end{aligned}$$

It is actually possible to write *any* quantum channel as a conditional quantum encoder when its input is a classical-quantum state. In this article, a conditional quantum encoder functions as the sender Alice's encoder of classical and quantum information.

A *quantum instrument* $\mathcal{D}^{A\to BM}$ is a CPTP map whose input is a quantum system A and whose outputs are a quantum system B and a classical system M. A collection $\{\mathcal{D}_m^{A\to B}\}_m$ of completely-positive trace-reducing maps specifies the instrument $\mathcal{D}^{A\to BM}$. The action of the instrument $\mathcal{D}^{A\to BM}$ on an arbitrary input state ρ is as follows:

$$\mathcal{D}^{A\to BM}\left(\rho^A\right) = \sum_m \mathcal{D}_m^{A\to B}\left(\rho^A\right) \otimes |m\rangle\langle m|^M. \tag{24}$$

Tracing out the classical register M gives the induced quantum operation $\mathcal{D}^{A\to B}$ where

$$\mathcal{D}^{A\to B}\left(\rho^A\right) \equiv \sum_m \mathcal{D}_m^{A\to B}\left(\rho^A\right).$$

This sum map is trace preserving:

$$\operatorname{Tr}\left\{\sum_m \mathcal{D}_m^{A\to B}\left(\rho^A\right)\right\} = 1.$$

We can think of the following quantity

$$p(m) \equiv \operatorname{Tr}\left\{\mathcal{D}_m^{A\to B}\left(\rho^A\right)\right\},$$

as a probability $p(m)$ of receiving the classical message m. In this article, a quantum instrument functions as Bob's decoder of classical and quantum information.

2 Distance Measures

2.1 Matrix Norm

We will introduce a few useful matrix norms in this section. First of all, every norm $\|\cdot\|$ must satisfy the following conditions.

- $\|A\| \geq 0$ with equality if and only if $A = 0$.
- $\|\alpha A\| = |\alpha|\|A\|$ for any $\alpha \in \mathbb{C}$.
- Triangle inequality: $\|A + B\| \leq \|A\| + \|B\|$.

Definition 6 (Schatten norm) *For $p \in [1, \infty)$, the Shatten p-norm of a matrix $A \in \mathbb{C}^{m\times n}$ is defined as*

$$\|A\|_p := \mathrm{Tr}(|A|^p)^{\frac{1}{p}} \tag{25}$$

where $|A| := \sqrt{A^\dagger A}$. We extend $p \to \infty$ as follows

$$\|A\|_\infty := \max\{\|A\boldsymbol{x}\| : \forall \boldsymbol{x} \in \mathbb{C}^n,\ \|\boldsymbol{x}\| = 1\}. \tag{26}$$

Properties of Schatten p-norms are summarized below

1. The Schatten norms are unitarily invariant: for any unitary operators U and V
$$\|UAV\|_p = \|A\|_p \tag{27}$$
for any $p \in [1, \infty]$.
2. The Schatten norms satisfy Hölder's inequality: for $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{n\times \ell}$, it holds that
$$\|AB\|_1 \leq \|A\|_p\|B\|_q, \tag{28}$$
where $p, q \geq 1$ and $\frac{1}{p} + \frac{1}{q} = 1$.
3. Sub-multiplicativity: for $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{n\times \ell}$, it holds that
$$\|AB\|_p \leq \|A\|_p\|B\|_p. \tag{29}$$
4. Monotonicity: for $1 \leq p \leq q \leq \infty$, it holds that
$$\|A\|_1 \geq \|A\|_p \geq \|A\|_q \geq \|A\|_\infty. \tag{30}$$

Exercise 7 *Denote by $\sigma_i(A)$ the i-th (non-zero) singular value of A. Show that*

$$\|A\|_p = \left(\sum_i (\sigma_i(A))^p\right)^{\frac{1}{p}}. \tag{31}$$

There are important special cases of Schatten p-norm. Specifically, the Schatten 1-norm is commonly known as the *trace norm*, and will lead to the definition of trace distance in Sec. 2.2. The Schatten 2-norm is also known as the *Frobenius norm* whose explicit form is given below.

Definition 8 (Frobenuis norm) *The Frobenius norm (or the Hilbert-Schmidt norm) of a matrix $A \in \mathbb{C}^{m\times n}$ is defined as*

$$\|A\|_2 \equiv \|A\|_F = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}|A_{i,j}|^2}. \tag{32}$$

Finally, the Schatten ∞-norm is also called the *operator norm* or the *spectral norm* whose definition is given in Eq. (26).

2.2 Trace Distance and Fidelity

We will introduce two commonly used distance measures in quantum information science; namely the trace distance and fidelity.

Definition 9 (Trace Distance) *The trace distance between two operators A and B is given by*

$$\|A - B\|_1 := \operatorname{Tr}|A - B|.$$

Exercise 10

$$\|\sigma - \rho\|_1 = \max_{-I\leq\Lambda\leq I}\operatorname{Tr}[\Lambda(\sigma-\rho)]. \tag{33}$$

Denote $T(\rho,\sigma) \equiv \|\rho - \sigma\|_1$. The trace distance of two density operators is an extension of total variation distance of probability measures:

$$T(P,Q) = \frac{1}{2}\sum_x |p(x) - q(x)|, \tag{34}$$

where P and Q are probability distributions with pdf $p(x)$ and $q(x)$, respectively.

Properties of the trace distance include

- $T(\rho,\sigma) = 0$ if and only if $\rho = \sigma$.
- Invariant under unitary operation: $T(U\rho U^\dagger, U\sigma U^\dagger) = T(\rho,\sigma)$
- Contraction: $T(\mathcal{N}(\rho),\mathcal{N}(\sigma)) \leq T(\rho,\sigma)$, where $\mathcal{N}$ is any trace-preserving and completely positive map.
- Convexity: $T(\sum_i p_i\rho_i,\sigma) \leq \sum_i p_i T(\rho_i,\sigma)$.

Definition 11 (Fidelity) *For $\rho,\sigma \in \mathcal{D}(\mathcal{H})$, their fidelity is*

$$F(\rho,\sigma) := \operatorname{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}.$$

Note that fidelity is not a metric on $\mathcal{D}(\mathcal{H})$. Fidelity is a quantum generization of classical Bhattacharyya distance:

$$F(P,Q) = \sum_x \sqrt{p(x)q(x)} \tag{35}$$

where P and Q are probability distributions with pdf $p(x)$ and $q(x)$, respectively.

Exercise 12 *Shot that, for $\rho, \sigma \in \mathcal{D}(\mathcal{H})$,*

$$F(\rho,\sigma) = \min_{\Lambda_i} \left(\sum_i \sqrt{\mathrm{Tr}[\rho\Lambda_i]\,\mathrm{Tr}[\sigma\Lambda_i]} \right) \tag{36}$$

where $\Lambda = \{\Lambda_i\}$ is a POVM [4].

Exercise 13 *Show that*

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

where the maximum is taken over all purifications ψ_ρ, ψ_σ of ρ and σ, respectively. ***Hint:*** *Uhlmann's theorem* [9].

Properties of the fidelity include

- Symmetry: $F(\rho,\sigma) = T(\sigma,\rho)$.
- $0 \leq F(\rho,\sigma) \leq 1$.
- $F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho,\sigma)$.
- $F(|\psi_\rho\rangle, |\psi_\sigma\rangle) = |\langle\psi_\rho|\psi_\sigma\rangle|$.
- $F(\mathcal{N}(\rho), \mathcal{N}(\sigma)) \geq F(\rho,\sigma)$, where $\mathcal{N}$ is any trace-preserving and completely positive map.

Lemma 14

$$1 - F(\rho,\sigma) \leq \|\rho - \sigma\|_1 \leq \sqrt{1 - F^2(\rho,\sigma)}. \tag{37}$$

The distance $d_s(\rho,\sigma) := \sqrt{1 - F^2(\rho,\sigma)}$ on density operators was introduced in [5] under the name *sine distance*. The sine distance was extended to a metric on subnormalized states in a different way under the name *purified distance* in [8].

Exercise 15 (Advanced) *We can extend the definition of sine distance to that on the set of positive semidefinite operators* [3]. *Define*

$$d_{op}(\rho,\sigma) := \min_{\psi_\rho,\psi_\sigma} \frac{1}{2} \| |\psi_\rho\rangle\langle\psi_\rho| - |\psi_\sigma\rangle\langle\psi_\sigma| \|_1 \tag{38}$$

where ψ_ρ, ψ_σ are purifications of $\rho, \sigma \in \mathcal{L}(\mathcal{H})_+$. We will call d_{op} the distance of optimal purifications.

Show the following:

- *d_{op} is a metric on $\mathcal{L}(\mathcal{H})_+$.*
- *d_{op} coincides with d_s for density operators.*
- $$\frac{d_{op}(\rho,\sigma)^2}{\mathrm{Tr}\,\rho + \mathrm{Tr}\,\sigma} \leq \|\rho - \sigma\|_1 \leq d_{op}(\rho,\sigma).$$

3 State Discrimination

The (one-copy) *quantum state discrimination problem* involves the task of correctly identifying a quantum state that is randomly sampled from an ensemble $\mathcal{E} = \{\rho_i, p_i\}_{i=1}^n$, where $\rho_i \in \mathcal{D}(\mathcal{H})$ and p_i is the probability of obtaining ρ_i. The "which state" classical information is extracted from the sampled state using a positive operator-valued measure (POVM), which is a collection of positive semidefinite operators $\Pi = \{\Pi_i\}_{i=1}^n$ acting on $\mathcal{D}(\mathcal{H})$ such that $\sum_{i=1}^n \Pi_i = \mathbb{I}_d$. The total identification success probability of the POVM Π is

$$\Pi(\mathcal{E}) := \sum_{i=1}^n p_i \operatorname{Tr}[\Pi_i \rho_i]. \tag{39}$$

Define the optimal success probability

$$P_{succ}(\mathcal{E}) = \max_{\Pi} \Pi(\mathcal{E}), \tag{40}$$

and the *minimum error probability* is given by

$$P_{err}(\mathcal{E}) = 1 - P_{succ}(\mathcal{E}). \tag{41}$$

Here the minimization is taken over all n-outcome POVMs, and a minimum can indeed be obtained since the set of POVMs is compact.

For the case of $n = 2$, we have the following famous result.

Theorem 16 (Holevo-Helstrom) *The minimum error probability to discriminate a given ensemble $\mathcal{E} = \{\rho_i, p_i\}_{i=1}^2$ is*

$$P_{err}(\mathcal{E}) = \frac{1}{2} - \frac{1}{2}\|p_1\rho_1 - p_2\rho_2\|_1. \tag{42}$$

This result gives the trace distance an *operational* meaning.

Proof. The success probability of a POVM $\Pi = \{\Pi_1, \Pi_2\}$ on the ensemble $\mathcal{E}$ is

$$\begin{aligned}
\Pi(\mathcal{E}) &= p_1 \operatorname{Tr}\Pi_1\rho_1 + p_2 \operatorname{Tr}\Pi_2\rho_2 && (43)\\
&= \left(\frac{1}{2}\operatorname{Tr}\Pi_1 p_1\rho_1 + \frac{1}{2}\operatorname{Tr}\Pi_1 p_1\rho_1\right) + \left(\frac{1}{2}\operatorname{Tr}\Pi_2 p_2\rho_2 + \frac{1}{2}\operatorname{Tr}\Pi_2 p_2\rho_2\right) && (44)\\
&= \left(\frac{1}{2}\operatorname{Tr}\Pi_1 p_1\rho_1 + \frac{1}{2}\operatorname{Tr}(I - \Pi_2) p_1\rho_1\right) + \left(\frac{1}{2}\operatorname{Tr}\Pi_1 p_2\rho_2 + \frac{1}{2}\operatorname{Tr}(I - \Pi_1) p_2\rho_2\right) && (45)\\
&= \frac{1}{2} + \frac{1}{2}\operatorname{Tr}\Pi_1(p_1\rho_1 - p_2\rho_2) - \frac{1}{2}\operatorname{Tr}\Pi_2(p_1\rho_1 - p_2\rho_2) && (46)\\
&= \frac{1}{2} + \frac{1}{2}\operatorname{Tr}(\Pi_1 - \Pi_2)(p_1\rho_1 - p_2\rho_2) && (47)\\
&\le \frac{1}{2} + \frac{1}{2}\|p_1\rho_1 - p_2\rho_2\|_1, && (48)
\end{aligned}$$

where the inequality uses Eq. (33). In the following, we can explicitly construct Π such that it will saturate the bound in Eq. (48). Let $A = p_1\rho_1 - p_2\rho_2$, and assume its spectral decomposition to be

$$A = \sum_i \lambda_i |\nu_i\rangle\langle\nu_i|.$$

Define two projectors

$$P_+ = \sum_{i:\lambda_i \geq 0} |\nu_i\rangle\langle\nu_i| \tag{49}$$

$$P_- = \sum_{i:\lambda_i < 0} |\nu_i\rangle\langle\nu_i|, \tag{50}$$

and notice that

$$\|A\|_1 = \sum_i |\lambda_i| = \operatorname{Tr} P_+ A - \operatorname{Tr} P_- A. \tag{51}$$

Using $P_+ \equiv \Pi_1$ and $P_1 \equiv \Pi_2$ completes the proof. ■

The minimum error probability for a general ensemble has a closed form [6] that relates to the min entropy defined on the ensemble.

Exercise 17 (Advanced) *Show that* $1 - P_{err}(\mathcal{E}) = 2^{-H_{\min}(X|B)_\rho}$*, where* $\rho^{\mathcal{E}}_{XB} = \sum_{x=1}^n p_x |x\rangle\langle x|^X \otimes \rho_x^B$*,*

$$H_{\min}(A|B)_\rho = -\inf_{\sigma_B} D_{\max}(\rho_{AB}||I_A \otimes \sigma_B) \tag{52}$$

and $D_{\max}(\tau\|\tau') = \inf\{\lambda \in \mathbb{R} : \tau \leq 2^\lambda \tau'\}$*.*

Further reading

A variant of the above state discrimination is as follows. An extra outcome Π_0 is appended to the set of POVMs, and an additional constraint must be satisfied that $\operatorname{Tr}[\Pi_i \rho_j] = 0$ whenever $i \neq j$. Under this condition, no error will ever be made when guessing the state; however, the outcome "0" represents an inconclusive outcome and no guess is made on the state's identity. The *minimum inconclusive probability* is thus given by the following

$$\begin{aligned} P_{inc}(\mathcal{E}) = \min_{\Pi} \quad & \sum_{i=1}^n \operatorname{Tr}[\Pi_0 \rho_i] \\ s.t. \quad & \operatorname{Tr}[\Pi_i \rho_j] = 0 \quad i \neq j > 0. \end{aligned} \tag{53}$$

This time, the minimization is taken over all $(n+1)$-outcome POVMs. Not all ensembles will allow for a feasible solution, and unambiguous discrimination is possible if and only if the states are linearly independent [2].

State discrimination is also used to demonstrate the phenomenon of *nonlocality without entanglement* [1].

References

[1] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin, and William K. Wootters, *Quantum nonlocality without entanglement*, Phys. Rev. A **59** (1999Feb), no. 2, 1070–1091.

[2] Anthony Chefles, *Unambiguous Discrimination between Sets of Linearly Independent Quantum states*, Phys. Lett. A **239** (1998), 339.

[3] Nilanjana Datta, Milan Mosonyi, Min-Hsiu Hsieh, and Fernando G.S.L. Brandao, *A smooth entropy approach to quantum hypothesis testing and the classical capacity of quantum channels*, IEEE Transactions on Information Theory **59** (2013Dec), no. 12, 8014–8026.

[4] Christopher A. Fuchs and Carlton M. Caves, *Ensemble-dependent bounds for accessible information in quantum mechanics*, Phys. Rev. Lett. **73** (1994Dec), 3047–3050.

[5] Alexei Gilchrist, Nathan K. Langford, and Michael A. Nielsen, *Distance measures to compare real and ideal quantum processes*, Phys. Rev. A **71** (2005Jun), 062310.

[6] R. Konig, R. Renner, and C. Schaffner, *The operational meaning of min- and max-entropy*, IEEE Transactions on Information Theory **55** (2009), no. 9, 4337–4347.

[7] W. Forrest Stinespring, *Positive functions on* $\mathbb{C}^*$*-algebras*, Proceedings of the American Mathematical Society **6** (1955), 211–216.

[8] M. Tomamichel, R. Colbeck, and R. Renner, *Duality between smooth min- and max-entropies*, IEEE Transactions on Information Theory **56** (2010), no. 9, 4674–4681.

[9] A. Uhlmann, *The "transition probability" in the state space of a* $*$*-algebra*, Reports on Mathematical Physics **9** (1976), no. 2, 273 –279.