

# Note

Zanqiu Shen

February 25, 2023

# Contents

<b>1</b>	<b>Prerequisites</b>	<b>4</b>
1.1	Hilbert Spaces and Linear Operators . . . . .	4
1.2	Quantum States . . . . .	5
1.3	Composite systems, partial trace, entanglement . . . . .	5
1.4	Measurements . . . . .	6
1.5	Entropies . . . . .	6
<b>2</b>	<b>Representations</b>	<b>7</b>
2.1	Unitary evolution of (closed) quantum systems . . . . .	7
2.1.1	Quantum mechanics . . . . .	7
2.1.2	Evolution of quantum systems . . . . .	7
2.2	Open systems and noisy evolution . . . . .	8
2.3	Choi–Jamiołkowski isomorphism . . . . .	9
2.3.1	Recap . . . . .	11
2.3.2	Examples of CP maps . . . . .	13
2.4	Kraus representation and the isometric picture . . . . .	14
2.5	Unitary picture and open system dynamics . . . . .	18
2.6	Linear representation . . . . .	18
2.7	Complementary Channels . . . . .	21
<b>3</b>	<b>Classes of Quantum Channels</b>	<b>22</b>
3.1	Qubit channels . . . . .	22
3.2	Generalized dephasing channels . . . . .	25
3.2.1	Detour: Holevo information ( $\mathcal{X}$ -quantity) . . . . .	26
3.2.2	Some comments on last lecture . . . . .	27
3.3	Entanglement-breaking channels . . . . .	28
3.4	PPT-channels . . . . .	30

---

3.5	Anti-degradable channels . . . . .	31
<b>4</b>	<b>Quantum sensing and imaging</b>	<b>36</b>
4.1	Joint measurement of time-frequency entanglement via sum frequency generation . . . . .	36
4.2	Quantum and non-local effects offer over 40 dB noise resilience advantage towards quantum lidar . . . . .	36

# Chapter 1

## Prerequisites

### 1.1 Hilbert Spaces and Linear Operators

Throughout this course,  $\mathcal{H}$  denotes a finite-dimensional Hilbert space (complex vector space with an associated inner product). Using Dirac's "bra-ket" notation we denote elements of the Hilbert space (called kets) as

$$|\psi\rangle \in \mathcal{H}. \quad (1.1)$$

The elements of the dual Hilbert space are called bras and are denoted

$$\langle\psi| \in \mathcal{H}^*, \quad (1.2)$$

where  $\langle\psi| = (|\psi\rangle)^\dagger$ . Here,  $X^\dagger := \bar{X}^T$  denotes the Hermitian adjoint (also called the conjugate transpose). We denote

$$B(\mathcal{H}_1, \mathcal{H}_2) := \{\text{linear maps from } \mathcal{H}_1 \text{ to } \mathcal{H}_2\} \quad (1.3)$$

and the set of all linear maps to and from the same space will be denoted  $B(\mathcal{H}) = B(\mathcal{H}, \mathcal{H})$ . An operator  $X \in B(\mathcal{H})$  is *normal* if  $XX^T = X^T X$ . Every normal operator has a *spectral decomposition*. That is, there exists a unitary  $U$  and a diagonal matrix  $D$  whose entries are the eigenvalues  $\lambda_1, \dots, \lambda_d \in \mathbb{C}$  of  $X$  such that

$$X = UDU^\dagger. \quad (1.4)$$

In other words,

$$X = \sum_{i=1}^d \lambda_i |\psi_i\rangle \langle\psi_i| \quad (1.5)$$

where  $X|\psi_i\rangle = \lambda_i|\psi_i\rangle$  and  $U = (|\psi_1\rangle, \dots, |\psi_d\rangle)$ . If  $X$  is Hermitian,  $X = X^\dagger$ , then  $\lambda_i \in \mathbb{R}$ . An operator  $X$  is positive semi-definite (PSD) if

$$\langle\varphi| X |\varphi\rangle \geq 0 \quad \forall |\varphi\rangle \in \mathcal{H}. \quad (1.6)$$

As a consequence,  $X \geq 0$  and  $\lambda_i \geq 0$ . It holds that  $\text{PSD} \implies \text{Hermitian} \implies \text{normal}$ . Unless otherwise stated, we will always assume we are working in an orthonormal basis.

## 1.2 Quantum States

A quantum state  $\rho$  in a Hilbert space  $\mathcal{H}$  is a PSD linear operator with

$$\rho \in B(\mathcal{H}), \quad \rho \geq 0, \quad \text{tr} \rho = 1. \quad (1.7)$$

This means that the state has eigenvalues  $\{\lambda_i\}_{i=1}^d$  satisfying  $\lambda_i \geq 0$  and  $\sum_{i=1}^d \lambda_i = 1$ . Thus,  $\{\lambda_i\}_{i=1}^d$  forms a probability distribution.

A *pure quantum state*  $\psi$  is a quantum state with rank 1. We can find  $|\psi\rangle \in \mathcal{H}$  such that  $\psi = |\psi\rangle \langle \psi|$ . In this case,  $\psi$  is called a *projector*. A *mixed state* is a quantum state with rank  $> 1$ . Mixed states are convex combinations of pure states. That is, for every quantum state  $\rho$  with  $r = \text{rank}(\rho)$  there are pure states  $|\psi_i\rangle_{i=1}^k$  ( $k \geq r$ ) and a probability distribution  $\{p_i\}_{i=1}^k$  such that

$$\rho = \sum_{i=1}^k p_i |\psi_i\rangle \langle \psi_i|. \quad (1.8)$$

The spectral decomposition of  $\rho$  is a special case of this property.

## 1.3 Composite systems, partial trace, entanglement

Let  $A$  and  $B$  be two quantum systems with Hilbert spaces  $\mathcal{H}_A$  and  $\mathcal{H}_B$ . The *joint system*  $AB$  is described by the Hilbert space  $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$ . We denote quantum states of the joint system as  $\rho_{AB} \in \mathcal{H}_{AB}$ . The marginal of the bipartite state, denoted  $\rho_A$ , is uniquely defined as the operator satisfying

$$\rho_A := \text{tr}_B \rho_{AB}, \quad (1.9)$$

which is defined via  $\text{tr}(\rho_{AB}(X_A \otimes \mathbb{I}_B)) = \text{tr} \rho_A X_A \quad \forall X_A \in B(\mathcal{H}_A)$ . For a Hilbert space with  $|B| := \dim \mathcal{H}_B$ , the explicit form of the partial trace is

$$\text{tr}_B \rho_{AB} = \sum_{i=1}^{|B|} (\mathbb{I}_A \otimes \langle i|_B) \rho_{AB} (\mathbb{I}_A \otimes |i\rangle_B), \quad (1.10)$$

for some basis  $\{|i\rangle_B\}_{i=1}^{|B|}$  of  $\mathcal{H}_B$ .

A *product state* on  $AB$  is a state of the form  $\rho_A \otimes \sigma_B$ . The state is called *separable* if it lies in the convex hull of product states:

$$\rho_{AB} = \sum_i p_i \rho_A^i \otimes \sigma_B^i \quad (1.11)$$

for some states  $\{\rho_A^i\}_i$  and  $\{\sigma_B^i\}_i$  and probability distribution  $\{p_i\}_i$ . A state is called *entangled*, if it is not separable. An entangled state of particular interest is the *maximally entangled state*. Let  $d = \dim \mathcal{H}$ ,  $\{|i\rangle\}_{i=1}^d$  be a basis for  $\mathcal{H}$ . A maximally entangled state is expressed as

$$|\phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle \otimes |i\rangle \in \mathcal{H} \otimes \mathcal{H} \quad (1.12)$$

## 1.4 Measurements

The most general measurement is given by a *positive operator-valued measure* (POVM)  $E = \{E_i\}_i$  where  $E_i \geq 0 \quad \forall i$  and  $\sum_i E_i = \mathbb{I}$ . Then, for a quantum system  $\mathcal{H}$  in state  $\rho$ , the probability of obtaining measurement outcome  $i$  is given by  $p_i = \text{tr}[\rho E_i]$ . So, we have

$$\sum_i p_i = \sum_i \text{tr}[\rho E_i] = \text{tr} \left[ \rho \sum_i E_i \right] = \text{tr}[\rho \mathbb{I}] = \text{tr} \rho = 1, \quad (1.13)$$

for all normalized quantum states. A *projective measurement*  $\Pi = \{\Pi_i\}$  is a POVM with the added property of orthogonality, which for projectors means

$$\Pi_i \Pi_j = \delta_{ij} \Pi_i. \quad (1.14)$$

Any basis  $\{|e_i\rangle\}_{i=1}^{\dim \mathcal{H}}$  gives rise to a projective measurement  $\Pi = \{|e_i\rangle \langle e_i|\}_{i=1}^{\dim \mathcal{H}}$ .

## 1.5 Entropies

The *Shannon entropy*  $H(p)$  of a probability distribution  $p = \{p_i, \dots, p_d\}$  is defined as  $H(p) = -\sum_{i=1}^d p_i \log p_i$ , where the logarithm is base 2 unless otherwise specified. Note that when the logarithm is base 2, the entropy has units of *bits*. The *von Neumann entropy*  $S(\rho)$  of a quantum state  $\rho$  is defined as

$$S(\rho) = -\text{tr} [\rho \log \rho] = H(\{\lambda_i, \dots, \lambda_d\}), \quad (1.15)$$

where  $\rho = \sum_i \lambda_i |\psi_i\rangle \langle \psi_i|$  is a spectral decomposition of  $\rho$  and where the logarithm of an operator is obtained by first diagonalizing the matrix representing the operator and then taking the logarithm of the diagonal elements. That is,

$$\log \rho = \sum_{i: \lambda_i > 0} \log(\lambda_i) |\psi_i\rangle \langle \psi_i|. \quad (1.16)$$

## Chapter 2

# Representations

### 2.1 Unitary evolution of (closed) quantum systems

#### 2.1.1 Quantum mechanics

We start by stating some broadly-accepted facts or axioms about quantum mechanics.

- we represent quantum systems using (in our case) finite dimensional Hilbert spaces, denoted  $\mathcal{H}$
- Observables: measurable quantities are Hermitian operators  $A \in B(\mathcal{H})$ ,  $A = A^\dagger$ ,  $A = \sum_i a_i |a_i\rangle \langle a_i|$  where  $\langle a_i | a_j \rangle = \delta_{ij}$  and  $a_i \in \mathbb{R}$ .
- eigenvalues  $a_i \in \mathbb{R}$  are the possible measurement outcomes of the observable  $A$ .
- quantum states on  $\mathcal{H}$ :  $\rho \in B(\mathcal{H})$ ,  $\rho \geq 0$ ,  $\text{tr} \rho = 1$ ,  $\equiv \sum_i \lambda_i = 1$ ,  $\rho = \sum_i \lambda_i |\psi_i\rangle \langle \psi_i|$ ,  $\rho |\psi_i\rangle = \lambda_i |\psi_i\rangle$
- pure quantum states have rank 1: i.e.  $\exists |\psi\rangle \in \mathcal{H}$  s.t.  $\rho = |\psi\rangle \langle \psi|$
- given a state  $\rho$  and an observable  $A$  on the Hilbert space,  $\mathcal{H}$ , the probability of a specific outcome is given by  $p_i = \text{tr}(\rho |a_i\rangle \langle a_i|) = \langle a_i | \rho | a_i \rangle$
- expected outcomes of measurement:  $\langle A \rangle_\rho = \sum_i p_i a_i = \text{tr}(\rho A)$

#### 2.1.2 Evolution of quantum systems

There are essentially three *pictures* of quantum evolution:

1. Evolving states (Schrodinger picture)
2. Evolving observables (Heisenberg picture)
3. Evolving both (interaction picture)

We primarily focus on the Schrodinger picture in this course. Now, what do we require of a formalism that describes quantum evolution?

1. Evolution operation must be linear
2. Transformation  $T : B(\mathcal{H}) \rightarrow B(\mathcal{H})$  should preserve the structure of the Hilbert space. Mathematically, this means

$$\text{tr}(\psi\phi) = \text{tr}(T(\psi)T(\phi)) \quad \forall \psi, \phi \in B(\mathcal{H}) \quad (2.1)$$

**Theorem 1.** *Wigner's Theorem: The above requirements imply that  $T(X)$  must be either unitary or anti-unitary. That is,*

$$T(X) = UXU^\dagger \quad \text{or} \quad UX^TU^\dagger \quad (2.2)$$

for some unitary  $U$ .

## 2.2 Open systems and noisy evolution

Because interaction with the environment (some external, inaccessible system) is unavoidable, the closed system assumption is not realistic. Even if the environment is inaccessible, for all cases we are interested in we can first write a new system as the system we are interested in plus the environment we cannot access. That is, SE = system + environment and

$$X_{SE} \mapsto UX_{SE}U^\dagger, \quad \text{where } U \in \mathcal{U}(\mathcal{H}_S \otimes \mathcal{H}_E). \quad (2.3)$$

Note that  $\mathcal{U}$  denotes the unitary group. We can then trace out the environment to recover the evolved system of interest via

$$X_S = \text{Tr}_E(UX_{SE}U^\dagger) \quad (2.4)$$

This partial trace over the environment corresponds to a *noisy and irreversible* evolution of  $S$ . Recall that we are focusing on the Schrodinger picture of quantum mechanics. This means we evolve quantum states with maps  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$ . Maps that evolve quantum states must satisfy the following requirements.

1. Linearity
2. Map states to states
  - (a)  $T$  should preserve trace:  $\text{tr}(T(X)) = \text{tr}X$
  - (b)  $(X \geq 0 \implies T(X) \geq 0) \Leftrightarrow T \geq 0$  (short-hand notation)
  - (c) Complete positivity:  $T \otimes \mathbb{I}_n \geq 0, \quad \forall n \in \mathbb{N}$

These requirements lead us to our first definition.

**Definition 2.2.1.** *A quantum channel is a linear, completely positive (CP), trace-preserving (TP) map  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$ .*

Given a map  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$ , the *adjoint map* is  $T^\dagger : B(\mathcal{H}_2) \rightarrow B(\mathcal{H}_1)$  defined via

$$\langle T^\dagger(X), Y \rangle = \langle X, T(Y) \rangle \quad (2.5)$$

for all  $X \in B(\mathcal{H}_2)$  and  $Y \in B(\mathcal{H}_1)$ . Our map,  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$  is:



- CP iff  $T^\dagger$  is CP.
- TP iff  $T^\dagger$  is unital:  $T^\dagger(\mathbb{I}_2) = \mathbb{I}_1$ .

$$\langle T^\dagger(\mathbb{I}_2), Y \rangle = \langle \mathbb{I}_2, T(Y) \rangle = \text{tr}(T(Y)) = \text{tr} Y = \langle \mathbb{I}_1, Y \rangle \quad \forall \quad Y \in B(\mathcal{H}_1) \quad (2.6)$$

This chain of equalities implies that  $T^\dagger(\mathbb{I}_2) = \mathbb{I}_1$ . Note that unital quantum channels are both TP and unital.

### 2.3 Choi–Jamiołkowski isomorphism

We now turn to a very useful tool for studying quantum channels.

**Definition 2.3.1.** Let  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$  be a linear map. The Choi operator  $\tau \in B(\mathcal{H}_1 \otimes \mathcal{H}_2)$  is defined as

$$\tau := (\mathbb{I}_1 \otimes T)(\gamma) \quad (2.7)$$

where  $\gamma := |\gamma\rangle \langle \gamma|$  and  $|\gamma\rangle = \sum_{i=1}^{\dim \mathcal{H}_1} |i\rangle \otimes |i\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_1$ . Note that  $\{|i\rangle\}_{i=1}^{\dim \mathcal{H}_1}$  is an orthonormal basis for  $\mathcal{H}_1$ .

The explicit form of this operator is then

$$\tau = \sum_{i,j} |i\rangle \langle j| \otimes T(|i\rangle \langle j|) \quad (2.8)$$

**Example.** If  $\mathcal{H}_1 = \mathcal{H}_2 = \mathbb{C}^2$ , then we can express the Choi operator with the block matrix given by

$$\tau = \begin{pmatrix} T(|0\rangle \langle 0|) & T(|1\rangle \langle 0|) \\ T(|0\rangle \langle 1|) & T(|1\rangle \langle 1|) \end{pmatrix} \quad (2.9)$$

where the elements of this matrix are themselves operators  $T(|i\rangle \langle j|)$ .

**Proposition 2.3.1.** Let  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$ . The map  $T \mapsto \tau = (\mathbb{I}_1 \otimes T)(\gamma)$  is a bijection between  $\{T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)\}$  and  $B(\mathcal{H}_1 \otimes \mathcal{H}_2)$ , with the inverse mapping  $\tau \mapsto T(X) := \text{tr}_1(\tau(X^T \otimes \mathbb{I}))$ .

*Proof.* Let  $\tau = (\mathbb{I} \otimes T)(\gamma)$ , where as usual  $\gamma = |\gamma\rangle \langle \gamma|$ . Tracing over the first

system, we have

$$\mathrm{tr}_1(\tau(X^T \otimes \mathbb{I})) = \mathrm{tr}_1 \left( \left( \sum_{i,j} |i\rangle \langle j| \otimes T(|i\rangle \langle j|) \right) (X^T \otimes \mathbb{I}) \right) \quad (2.10)$$

$$= \sum_{i,j} \mathrm{tr}(|i\rangle \langle j| X^T) T(|i\rangle \langle j|) \quad (2.11)$$

$$= \sum_{i,j} \left( \sum_i \langle i| (|i\rangle \langle j| X^T) |i\rangle T(|i\rangle \langle j|) \right) \quad (2.12)$$

$$= \sum_{i,j} \langle j| X^T |i\rangle T(|i\rangle \langle j|) \quad (2.13)$$

$$= \sum_{i,j} x_{ij} T(|i\rangle \langle j|), \quad \langle j| X^T |i\rangle = \langle i| X |j\rangle := x_{ji} \quad (2.14)$$

$$= T\left(\sum_{i,j} x_{ij} |i\rangle \langle j|\right), \quad \text{linearity of } T \quad (2.15)$$

$$= T(X) \quad (2.16)$$

It remains to be shown that  $T \mapsto (\mathbb{I} \otimes T)(\gamma)$  is surjective. We note that there exists  $|\psi_i\rangle, |\phi_i\rangle$  such that  $\tau = \sum_i |\psi_i\rangle \langle \phi_i| \in B(\mathcal{H}_1 \otimes \mathcal{H}_2)$  where  $|\psi_i\rangle \neq |\phi_i\rangle$ .

**Claim:** For every vector  $|\psi\rangle \in B(\mathcal{H}_1 \otimes \mathcal{H}_2) \exists V \in B(\mathcal{H}_1, \mathcal{H}_2)$  such that

$$|\psi\rangle = (\mathbb{I} \otimes V) |\gamma\rangle. \quad (2.17)$$

To see this, let  $|\psi\rangle = \sum_{i,j} p_{ij} |i\rangle \otimes |e_j\rangle$  where  $\{|i\rangle\}$  is  $\gamma$ 's basis and  $\{|e_j\rangle\}$  is an arbitrary basis. Then we can construct  $V$  as

$$V = \sum_{i,j} p_{ij} |e_j\rangle \langle i|. \quad (2.18)$$

Recall  $\tau = \sum_i |\psi_i\rangle \langle \phi_i| \in B(\mathcal{H}_1 \otimes \mathcal{H}_2)$ . We next claim that there exists  $L_i, K_i$  such that

$$|\psi_i\rangle = (\mathbb{I} \otimes K_i) |\gamma\rangle, \quad (2.19)$$

$$|\phi_i\rangle = (\mathbb{I} \otimes L_i) |\gamma\rangle. \quad (2.20)$$

$$(2.21)$$

This implies

$$\tau = \sum_i |\psi_i\rangle \langle \phi_i| \quad (2.22)$$

$$= \sum_i (\mathbb{I} \otimes K_i) |\gamma\rangle \langle \gamma| (\mathbb{I} \otimes L_i)^\dagger \quad (2.23)$$

$$= (\mathbb{I} \otimes T)(\gamma), \quad (2.24)$$

where we have identified

$$T(X) = \sum_i K_i X L_i \quad (2.25)$$

as the linear map we sought. This completes the proof of the proposition.  $\square$

### 2.3.1 Recap

- Quantum systems are modeled by Hilbert spaces
- Quantum state:  $\rho \in B(\mathcal{H}), \rho \geq 0, \text{tr} \rho = 1$ . The state has an eigendecomposition given by

$$\rho = \sum_i \lambda_i |\psi_i\rangle \langle \psi_i|, \quad \text{where } \rho |\psi_i\rangle = \lambda_i |\psi_i\rangle, \lambda_i \geq 0, \langle \psi_i | \psi_j \rangle = \delta_{ij} \quad (2.26)$$

- Schrodinger picture: evolution of quantum states
- Closed systems: evolution given by unitary maps (Wigner’s theorem)
- Open systems: unitary evolution on system + environment. This induces noisy evolution on the system
- Quantum channel:  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$ 
  - linear
  - trace-preserving (TP):  $\text{tr}(X(T)) = \text{tr} X \quad \forall X \in B(\mathcal{H}_1)$
  - completely positive (CP):  $T \otimes \mathbb{I} \geq 0 \quad \forall n \in \mathbb{N}$
- Choi operator:  $\tau \in B(\mathcal{H}_1 \otimes \mathcal{H}_2), \tau := (\mathbb{I} \otimes T)(\gamma)$  where  $|\gamma\rangle = \sum_i |i\rangle \otimes |i\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_1$
- Choi–Jamiołkowski isomorphism:  $T \mapsto \tau = (\mathbb{I} \otimes T)(\gamma)$  is a bijection  $\{T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2) \text{ linear}\} \Leftrightarrow B(\mathcal{H}_1 \otimes \mathcal{H}_2)$  with inverse mapping given by

$$\tau \mapsto [T : X \mapsto \text{tr}_1(\tau(X^T \otimes \mathbb{I}))]. \quad (2.27)$$

- Steering inequality:  $\forall |\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \quad \exists \quad K \in B(\mathcal{H}_1, \mathcal{H}_2)$  such that

$$|\psi\rangle = (\mathbb{I} \otimes K) |\gamma\rangle \quad (2.28)$$

**Proposition 2.3.2.** *Let  $T$  be a linear map that acts as  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$ . Let  $\tau$  denote the associated Choi operator that is defined as  $\tau = (\mathbb{I} \otimes T)(\gamma)$ , with  $|\gamma\rangle = \sum_i |i\rangle \otimes |i\rangle$ . Then the following hold:*

1.  $T(X)^\dagger = T(X^\dagger)$  iff  $\tau = \tau^\dagger$ .
2.  $T$  is CP iff  $\tau \geq 0$ .
3.  $T$  is TP iff  $\text{tr}_2 \tau = \mathbb{I}_1$ .
4.  $T$  is unital iff  $\text{tr}_1 \tau = \mathbb{I}_2$ .

Recall an operator  $S$  is unital if  $S(\mathbb{I}_1) = \mathbb{I}_2$ .

*Proof.* 1. ( $\Rightarrow$ ) First we prove if  $T(X)^\dagger = T(X^\dagger)$ , then  $\tau = \tau^\dagger$ .

$$\tau^\dagger = \left( \sum_{i,j} |i\rangle \langle j| \otimes T(|i\rangle \langle j|) \right)^\dagger \quad (2.29)$$

$$= \sum_{i,j} |j\rangle \langle i| \otimes T(|i\rangle \langle j|)^\dagger \quad (2.30)$$

$$= \sum_{i,j} |j\rangle \langle i| \otimes T(|i\rangle \langle j|^\dagger) \quad (2.31)$$

$$= \sum_{i,j} |j\rangle \langle i| \otimes T(|j\rangle \langle i|) \quad (2.32)$$

$$= \tau \quad (2.33)$$

( $\Leftarrow$ ) The other way, if  $\tau = \tau^\dagger$ ,  $T(X)^\dagger = T(X^\dagger)$ . We know that  $\tau = \sum_{i,j} |i\rangle \langle j| \otimes T(|i\rangle \langle j|)$  so  $\tau = \tau^\dagger$  allows us to write

$$\left( \sum_{i,j} |i\rangle \langle j| \otimes T(|i\rangle \langle j|) \right) = \left( \sum_{i,j} |i\rangle \langle j| \otimes T(|i\rangle \langle j|) \right)^\dagger \quad (2.34)$$

$$= \left( \sum_{i,j} |j\rangle \langle i| \otimes T(|i\rangle \langle j|)^\dagger \right) \quad (2.35)$$

This is a matrix equality, so each element must be the same. Sandwiching  $\langle j| \otimes \mathbb{I}_2 \cdot |i\rangle \otimes \mathbb{I}_2$  around both sides of the expression above yields

$$T(|i\rangle \langle j|)^\dagger = T(|j\rangle \langle i|) \quad \forall i, j, \quad (2.36)$$

which implies

$$T(X)^\dagger = T(X^\dagger) \quad \forall X \in B(\mathcal{H}_1), \quad (2.37)$$

because all bounded operators can be expanded in the form  $X = \sum_{i,j} x_{ij} |i\rangle \langle j|$  and because  $T$  is linear.

2. ( $\Rightarrow$ ) First we prove that if  $T$  is CP, then  $\tau \geq 0$ .  $\tau = (\mathbb{I} \otimes T)(\gamma), \gamma \geq 0 \Rightarrow \tau \geq 0$ .

( $\Leftarrow$ ) Going the other way, we want to prove that if  $\tau \geq 0$ , then  $T$  is CP. To do so, we need to show

$$(\mathbb{I}_n \otimes T)(\rho) \geq 0 \quad \forall \rho \in B(\mathbb{C}^n \otimes \mathcal{H}_2), \rho \geq 0. \quad (2.38)$$

3. ( $\Rightarrow$ ) If  $T$  is TP, then  $\text{tr}_2 \tau = \mathbb{I}_1$ .

$$\text{tr}_2 \tau = \text{tr}_2 \left( \sum_{i,j} |i\rangle \langle j| \otimes T(|i\rangle \langle j|) \right) \quad (2.39)$$

$$= \sum_{i,j} |i\rangle \langle j| \text{tr}(T(|i\rangle \langle j|)) \quad (2.40)$$

$$= \sum_{i,j} |i\rangle \langle j| T(\text{tr}(|i\rangle \langle j|)) \quad (2.41)$$

$$= \sum_{i,j} |i\rangle \langle j| \delta_{ij} \quad (2.42)$$

$$= \sum_i |i\rangle \langle i|_1 \quad (2.43)$$

$$= \mathbb{I}_1 \quad (2.44)$$

( $\Leftarrow$ ) If  $\text{tr}_2 \tau = \mathbb{I}_2$ , then  $\text{tr} T(X) = \text{tr} X$ .

$$\text{tr} T(X) = \text{tr} [\text{tr}_1(\tau(X^T \otimes \mathbb{I}))] \quad (2.45)$$

$$= \text{tr}(\tau(X^T \otimes \mathbb{I})) \quad \text{tr}(\text{tr}_i(\cdot)) = \text{tr}(\cdot) \quad (2.46)$$

$$= \text{tr}(\text{tr}_2(\tau) X^T) \quad (2.47)$$

$$= \text{tr} X^T \quad (2.48)$$

$$= \text{tr} X \quad (2.49)$$

4. ( $\Rightarrow$ )  $T$  is unital if  $\text{tr}_1 \tau = \mathbb{I}_2$ .

$$\text{tr}_1 \tau = \sum_{i,j} \text{tr}(|i\rangle \langle j|_1) T(|i\rangle \langle j|_1) \quad (2.50)$$

$$= \sum_i T(|i\rangle \langle i|_1) \quad (2.51)$$

$$= T(\mathbb{I}_1) \quad (2.52)$$

$$= \mathbb{I}_2 \quad (2.53)$$

( $\Leftarrow$ ) If  $\text{tr}_1 \tau = \mathbb{I}_2$ , then  $T$  is unital.

$$T(\mathbb{I}_1) = \text{tr}_1(\tau(\mathbb{I}_1^T \otimes \mathbb{I}_2)) \quad (2.54)$$

$$= \text{tr}_1 \tau \quad (2.55)$$

$$= \mathbb{I}_2 \quad (2.56)$$

□

### 2.3.2 Examples of CP maps

1. unitary maps are CP:  $(\mathbb{I} \otimes U) |\gamma\rangle \langle \gamma| (\mathbb{I} \otimes U)^\dagger \geq 0$
2. isometries are CP:  $V : \mathcal{H}_1 \rightarrow \mathcal{H}_2 : V^\dagger V = \mathbb{I}_1 \Leftrightarrow \langle \varphi | V^\dagger V | \psi \rangle = \langle \varphi | \psi \rangle \quad \forall \varphi, \psi$ , and

where  $\dim \mathcal{H}_1 \leq \dim \mathcal{H}_2$ .

3. trace:  $(\mathbb{I}_1 \otimes \text{tr})(\gamma) = \sum_{i,j} |i\rangle \langle j| \text{tr}(|i\rangle \langle j|) = \mathbb{I}_1 \geq 0$ . Note that this also implies that the partial trace,  $\text{tr}_2 : B(\mathcal{H}_1 \otimes \mathcal{H}_2) \rightarrow B(\mathcal{H}_1)$  is CPTP. We will later show that all channels can be expressed as unitary evolution on system + environment followed by a partial trace over the environment.
4.  $X \mapsto \sum_i K_i X K_i^\dagger$  are CP (more on this later).

We have seen examples of CP maps. What about a map that is not CP? The transposition map,  $V : X \mapsto X^T$  with respect to a fixed basis, is positive but not *completely positive*.

Consider the following operator:

$$\mathbb{F} = (\mathbb{I} \otimes V)(\gamma) \quad (2.57)$$

$$= \sum_{i,j} |i\rangle \langle j| \otimes V(|i\rangle \langle j|) \quad (2.58)$$

$$= \sum_{i,j} |i\rangle \langle j| \otimes |j\rangle \langle i|. \quad (2.59)$$

We call this the swap operator because  $|\psi_i\rangle, |\psi_2\rangle \in \mathcal{H}_1 : \mathbb{F}(|\psi_1\rangle \otimes |\psi_2\rangle) = |\psi_1\rangle \otimes |\psi_1\rangle$ .

## 2.4 Kraus representation and the isometric picture

We saw before that  $X \mapsto \sum_i K_i X K_i^\dagger$  are CP. The converse is also true.

**Proposition 2.4.1.** 1. A map  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$  is CP iff  $\exists \{K_i\}_i$  with  $K_i \in B(\mathcal{H}_1, \mathcal{H}_2)$  such that  $T(X) = \sum_i K_i X K_i^\dagger$ . We call the  $K_i$ 's the Kraus operators of  $T$ .

2. The Kraus rank,  $r(T)$ , the minimal number of Kraus operators needed to represent  $T$ , is equal to the rank of the Choi operator,  $\tau = (\mathbb{I} \otimes T)(\gamma)$ . It is always true that

$$r(T) \leq \dim \mathcal{H}_1 \cdot \dim \mathcal{H}_2 \quad (2.60)$$

3. There exists a Kraus representation with  $r = \text{rank}(\tau)$  operators such that  $\langle K_i, K_j \rangle = \text{tr}(K_i^\dagger K_j) = c_i \delta_{i,j}$  for some constant  $c_i$  that results from using an unnormalized  $\gamma$  state.

4.  $T$  is TP iff  $\sum_i K_i^\dagger K_i = \mathbb{I}_1$ ,  $T$  is unital iff  $\sum_i K_i K_i^\dagger = \mathbb{I}_2$

5. Any two Kraus representations  $\{K_i\}_i$  and  $\{L_j\}_j$  of a channel  $T$  are related by a unitary  $U$  via

$$K_i = \sum_{j} U_{ij} L_j. \quad (2.61)$$

This means that  $T(X) = \sum_i K_i X K_i^\dagger = \sum_j L_j X L_j^\dagger$ .

*Proof.* 1. A map  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$  is CP iff  $\exists \{K_i\}_i$  with  $K_i \in B(\mathcal{H}_1, \mathcal{H}_2)$  such that  $T(X) = \sum_i K_i X K_i^\dagger$ . We call the  $K_i$ 's the Kraus operators of  $T$ .

$(\Leftarrow)$  is obvious. **Why?**

$(\Rightarrow)$  Going the other way, we know  $T$  is CP  $\Leftrightarrow \tau \geq 0$ , by Prop 4.

**Claim:**  $X \geq 0 \Leftrightarrow \exists \{|\psi_i\rangle\}_{i=1}^r$  with  $r \geq \text{rank } X$  such that  $X = \sum_i |\psi_i\rangle \langle \psi_i|$  with  $\langle \psi_i | \psi_j \rangle \neq \delta_{ij}$  in general.

*Proof.*  $(\Leftarrow)$   $X = \sum_i |\psi_i\rangle \langle \psi_i|$  for some  $\{|\psi_i\rangle\}_i$ .

We know,  $X \geq 0 \Leftrightarrow \langle \varphi | X | \varphi \rangle \geq 0 \quad \forall |\varphi\rangle$ . This allows us to write

$$\langle \varphi | \left( \sum_i |\psi_i\rangle \langle \psi_i| \right) | \varphi \rangle = \sum_i |\langle \varphi | \psi_i \rangle|^2 \geq 0 \quad (2.62)$$

$(\Rightarrow)$   $X \geq 0 : X = \sum_i \lambda_i |X_i\rangle \langle X_i|$  where  $X |X_i\rangle = \lambda_i |X_i\rangle$  and  $\langle X_i | X_j \rangle = \delta_{ij}$ . Let  $|\psi_i\rangle := \sqrt{\lambda_i} |X_i\rangle \Rightarrow X = \sum_i |\psi_i\rangle \langle \psi_i|$ .  $\square$

Returning to the proof of the first item of the proposition, we have that  $\tau \geq 0 \Rightarrow \exists \{|\psi_i\rangle\}$  such that  $\tau = \sum_i |\psi_i\rangle \langle \psi_i|$ . Further, for all  $i$  there exists  $K_i$  such that  $|\psi_i\rangle = (\mathbb{I}_1 \otimes K_i) |\gamma\rangle$ . Then we can write

$$\tau = \sum_i |\psi_i\rangle \langle \psi_i| \quad (2.63)$$

$$= \sum_i (\mathbb{I}_1 \otimes K_i) |\gamma\rangle \langle \gamma| (\mathbb{I}_1 \otimes K_i)^\dagger \quad (2.64)$$

by the C-J isomorphism we conclude that  $T(X) = \sum_i K_i X K_i^\dagger$ .

2. Clear from proof of 1.)  $r = \text{rank}(\tau) \Rightarrow$  at least  $r$  pure states in the decomposition of  $\tau$ . This implies that there are at least  $r$  Kraus operators.
3. There exists a Kraus representation with  $r = \text{rank}(\tau)$  operators such that  $\langle K_i, K_j \rangle = \text{tr}(K_i^\dagger K_j) = c_i \delta_{i,j}$  for some constant  $c_i$  that results from using an unnormalized  $\gamma$  state.

Let  $\tau = \lambda_i |X_i\rangle \langle X_i|$  be the spectral decomposition of  $\tau$  with  $|\varphi_i\rangle = \sqrt{\lambda_i} |X_i\rangle$ . We have

$$\tau = \sum_i |\varphi_i\rangle \langle \varphi_i| \quad (2.65)$$

$$= \sum_i (\mathbb{I} \otimes L_i) |\gamma\rangle \langle \gamma| (\mathbb{I} \otimes L_i)^\dagger \quad (2.66)$$

$$\Rightarrow T = \sum_{i=1}^{r(\tau)} L_i \cdot L_i^\dagger \quad (2.67)$$

We also need to show  $\langle L_i, L_j \rangle = c\delta_{ij}$ . We know

$$|\varphi_i\rangle = (\mathbb{I}_1 \otimes L_i) |\gamma\rangle \quad (2.68)$$

so, we can write

$$c\delta_{ij} = \langle \varphi_i | \varphi_j \rangle \quad (2.69)$$

$$= \langle \gamma | \left( \mathbb{I}_1 \otimes L_i^\dagger \right) (\mathbb{I} \otimes L_j) |\gamma\rangle \quad (2.70)$$

$$= \sum_{k,l} \langle k | l \rangle \langle k | L_i^\dagger L_j | l \rangle \quad (2.71)$$

$$= \sum_k \langle k | L_i^\dagger L_j | k \rangle \quad (2.72)$$

$$= \text{tr} \left( L_i^\dagger L_j \right) \quad (2.73)$$

$$= \langle L_i, L_j \rangle \quad (2.74)$$

4.  $T$  is TP iff  $\sum_i K_i^\dagger K_i = \mathbb{I}_1$ ,  $T$  is unital iff  $\sum_i K_i K_i^\dagger = \mathbb{I}_2$ .

$$\text{tr}(T(X)) = \sum_i \text{tr} \left( K_i X K_i^\dagger \right) \quad (2.75)$$

$$= \sum_i \text{tr} \left( K_i^\dagger K_i X \right) \quad \text{cyclicity of trace} \quad (2.76)$$

$$= \text{tr} \left( \sum_i K_i^\dagger K_i X \right) \quad \text{linearity of trace} \quad (2.77)$$

$$= \text{tr} X \quad \forall X \quad (2.78)$$

$$\Leftrightarrow \sum_i K_i^\dagger K_i = \mathbb{I}_1 \quad (2.79)$$

The other way is even easier.

$$T(\mathbb{I}_1) = \sum_i K_i \mathbb{I} K_i^\dagger \quad (2.80)$$

$$= \sum_i K_i K_i^\dagger \quad (2.81)$$

$$= \mathbb{I}_2. \quad (2.82)$$

5. Any two Kraus representations  $\{K_i\}_i$  and  $\{L_j\}_j$  of a channel  $T$  are related by a unitary  $U$  via

$$K_i = \sum_{j} U_{ij} L_j. \quad (2.83)$$

This means that  $T(X) = \sum_i K_i X K_i^\dagger = \sum_j L_j X L_j^\dagger$ .

**Claim:**  $\sum_i |\psi_i\rangle \langle \psi_i| = \sum_j |\varphi_j\rangle \langle \varphi_j|$  iff there exists a unitary,  $U$ , with  $|\psi_i\rangle = \sum_j U_{ij} |\varphi_j\rangle$ .



*Proof.*  $|\Psi\rangle = \sum_i |\psi_i\rangle \otimes |i\rangle$ , where  $\{|i\rangle\}$  is a reference systems' orthonormal basis. Also,  $|\Phi\rangle = \sum_j |\varphi_j\rangle \otimes |j\rangle$ . Then, there always exists an isometry  $V$  such that  $(\mathbb{I} \otimes V)|\Psi\rangle = |\Phi\rangle$ .  $\square$

The above result is useful for our proof because the isometry  $V$  above can always be extended to a unitary.

$$|\varphi_i\rangle = (\mathbb{I} \otimes \langle i|) |\Phi\rangle \quad (2.84)$$

$$= (\mathbb{I} \otimes \langle i|) (\mathbb{I} \otimes V) |\Psi\rangle \quad (2.85)$$

$$= (\mathbb{I} \otimes \langle i|) (\mathbb{I} \otimes V) \sum_j |\psi_j\rangle \otimes |j\rangle \quad (2.86)$$

$$= \sum_j |\psi_j\rangle \langle i|V|j\rangle \quad (2.87)$$

$$= \sum_j V_{ij} |\psi_j\rangle \quad (2.88)$$

$\square$

We now want to relate the Kraus representation to the isometric picture. Recall that an isometry is a map

$$V : \mathcal{H}_1 \rightarrow \mathcal{H}_2 : \langle \psi | \varphi \rangle = \langle \psi | V^\dagger V | \varphi \rangle \quad \forall |\psi\rangle, |\varphi\rangle \in \mathcal{H}_1 \quad (2.89)$$

where  $\dim \mathcal{H}_2 \geq \mathcal{H}_1$ . Note that if the dimensions are equal,  $V$  is unitary. We often consider a  $\mathcal{H}_2 = \mathcal{H}_B \otimes \mathcal{H}_E$ .

**Proposition 2.4.2.** 1.  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$  is CP iff  $\exists V : \mathcal{H}_1 \rightarrow \mathcal{H}_2 \otimes \mathbb{C}^r$  where  $r \geq r(T)$  and  $T(X) = \text{tr}_E V X V^\dagger$  with environment equal to  $\mathbb{C}^r$ .

2.  $T$  is TP iff  $V : \mathcal{H}_1 \rightarrow \mathcal{H}_2 \otimes \mathbb{C}^r$  is an isometry.

*Proof.* 1.  $(\Leftarrow)$  is done.

$(\Rightarrow)$   $T$  is CP:  $\exists \{K_i\}_{i=1}^n$  such that  $T(X) = \sum_i K_i X K_i^\dagger, r \geq r(T)$ . Choose an orthonormal basis  $\{|i\rangle\}_{i=1}^r$  in  $\mathbb{C}^r : V = \sum_{i=1}^r K_i \otimes |i\rangle$ . We then have

$$\text{tr}_E V X V^\dagger = \sum_{i,j} \text{tr}_1 \left( (K_i \otimes |i\rangle) X (K_j \otimes |j\rangle)^\dagger \right) \quad (2.90)$$

2.  $T$  is TP iff  $V^\dagger V = \mathbb{I}$ .

$(\Rightarrow)$

$$\text{tr} X = \text{tr} T(X) \quad (2.91)$$

$$= \text{tr} \left( \text{tr}_E V X V^\dagger \right) \quad (2.92)$$

$$= \text{tr} (V X V^\dagger) \quad (2.93)$$

$$= \text{tr} X \quad \forall X \Leftrightarrow V^\dagger V = \mathbb{I} \quad (2.94)$$

$\square$

- The isometry  $V$  in proposition above is called the Stinespring isometry or the Stinespring dilation of the channel  $T$ .
- Given Stinespring isometry  $V$ , a Kraus representation  $\{K_i\}_i$  is obtained via  $K_i = (\mathbb{I} \otimes \langle i|)V$ . This is evident if we recall

$$\mathrm{tr}_E Y = \sum_i (\mathbb{I} \otimes \langle i|) Y (\mathbb{I} \otimes |i\rangle) \quad (2.95)$$

## 2.5 Unitary picture and open system dynamics

For quantum channel  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$ :

$$\exists \text{ Stinespring isometry } V : \mathcal{H}_1 \rightarrow \mathcal{H}_2 \otimes \mathbb{C}^r \text{ such that} \quad (2.96)$$

$$T(X) = \mathrm{tr}_E V X V^\dagger \quad (2.97)$$

where  $r = \dim \mathcal{H}_1 \dim \mathcal{H}_2$ . Complete  $V$  to a unitary acting on  $\mathcal{H}_1 = \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}$  such that  $V = U(\mathbb{I}_{d_1} \otimes |\varphi\rangle)$  where  $|\varphi\rangle$  is some fixed vector in  $\mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}$ . What we then have is

$$T(X) = \mathrm{tr}_E V X V^\dagger \quad (2.98)$$

$$= \mathrm{tr}_{E'} U(X \otimes \varphi) U^\dagger \quad (2.99)$$

where the environment  $E'$  is  $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ . This all allows us to consider noisy quantum evolution as unitary evolution on a larger closed system followed by a tracing out of the environment.

## 2.6 Linear representation

Let  $T$  be a linear map  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$ . A key result from linear algebra is that **a linear map on a finite-dimensional Hilbert space can always be represented with a matrix with respect to a fixed basis.**

- If we are in a bounded Hilbert space  $B(\mathcal{H})$ , we have an associated inner product (called the Hilbert-Schmidt inner product) which is given as

$$\langle X, Y \rangle = \mathrm{tr}(X^\dagger Y). \quad (2.100)$$

- We can think of operators  $X \in B(\mathcal{H})$  as vectors, and maps  $T : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$  as matrices.
- Let  $\{|i\rangle\}_{i=1}^{\dim \mathcal{H}}$  be an orthonormal basis for  $\mathcal{H}$ . Then  $\{|i\rangle\langle j|\}_{i,j=1}^{\dim \mathcal{H}}$  is a basis for  $B(\mathcal{H})$ . Note that  $\dim \mathcal{H} = d \implies \dim B(\mathcal{H}) = d^2$ .
- Define a linear mapping

$$\mathrm{vec} : B(\mathcal{H}) \rightarrow \mathcal{H} \otimes \mathcal{H}. \quad (2.101)$$

So,

$$|i\rangle\langle j| \mapsto |i\rangle \otimes |j\rangle + \text{linear extension} \quad (2.102)$$

- $\{|i\rangle \otimes |j\rangle\}_{i,j=1}^d$  is a basis for  $\mathcal{H} \otimes \mathcal{H} \implies \text{vec}$  is an isomorphism,  $B(\mathcal{H}) \cong \mathcal{H} \otimes \mathcal{H}$

**Properties of  $\text{vec}$ :**

- $\text{vec}(|\psi\rangle \langle \varphi|) = |\psi\rangle \otimes |\varphi^*\rangle$  where  $*$  denotes the complex conjugate in the basis  $\{|i\rangle\}_i$
- $\langle X, Y \rangle_{B(\mathcal{H})} = \langle \text{vec}(X), \text{vec}(Y) \rangle_{\mathcal{H} \otimes \mathcal{H}}$
- $\text{vec}(AXB) = (A \otimes B^T) \text{vec}(X)$

Let  $\mathcal{N} : B(\mathcal{H}) \rightarrow B(\mathcal{H})$  be a linear map. Then via the  $\text{vec}$  map, this will correspond to some operator in  $N \in B(\mathcal{H} \otimes \mathcal{H})$ . In particular, there exist  $A_i, B_i$  such that  $N = \sum_i A_i \otimes B_i$ . Then, for  $X \in B(\mathcal{H})$  we would have

$$\mathcal{N}(X) = \sum_i A_i X B_i^T, \quad (2.103)$$

by using the identity  $\text{vec}(AXB^T) = (A \otimes B) \text{vec}(X)$ . When considering quantum channels, we have  $\mathcal{N}(X) = \sum_i K_i X K_i^\dagger$  which via  $\text{vec}$  will be  $N = \sum_i K_i \otimes K_i^*$ . This is called the *transfer matrix* of  $\mathcal{N}$ . The unitality condition  $\sum_i K_i K_i^\dagger = \mathbb{I}_2$  under  $\text{vec}$  becomes

$$N |\gamma\rangle = \left( \sum_i K_i^\dagger \otimes K_i^T \right) |\gamma\rangle = |\gamma\rangle = \text{vec}(\mathbb{I}) \quad (2.104)$$

The trace-preserving condition  $\sum_i K_i^\dagger K_i = \mathbb{I}_2$  under  $\text{vec}$  becomes

$$N^\dagger |\gamma\rangle = \left( \sum_i K_i^\dagger \otimes K_i^T \right) |\gamma\rangle = |\gamma\rangle. \quad (2.105)$$

Note that if  $T = \sum_i A_i \otimes B_i^T$ , then  $T^\dagger = \sum_i B_i^T \otimes A_i$ . The linear representation is useful, because it translates channel composition into matrix multiplication.

**Proposition 2.6.1.** *Let  $\mathcal{M} : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$ ,  $\mathcal{N} : B(\mathcal{H}_2) \rightarrow B(\mathcal{H}_3)$  be linear maps with transfer matrices  $M, N$ , respectively. Then,  $N \cdot M$  is the transfer matrix of  $\mathcal{N} \circ \mathcal{M} : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_3)$ .*

*Proof.*

$$\mathcal{M} = \sum_i A_i X B_i^T \quad A_i, B_i \in B(\mathcal{H}_1, \mathcal{H}_2) \quad (2.106)$$

$$\mathcal{N} = \sum_i C_i X D_i^T \quad C_i, D_i \in B(\mathcal{H}_2, \mathcal{H}_3) \quad (2.107)$$

The transfer matrices are

$$M = \sum_i A_i \otimes B_i, \quad (2.108)$$

$$N = \sum_i C_i \otimes D_i. \quad (2.109)$$

We then have

$$\mathcal{N} \circ \mathcal{M} = \sum_{i,j} C_i A_j X B_j^T D_i^T \quad (2.110)$$

$$N \cdot M = \sum_{i,j} C_i A_j \otimes D_i B_j \quad (2.111)$$

□

**Proposition 2.6.2.** *Let  $\mathcal{N} : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)$  be a linear map with transfer matrix  $N$  and  $\tilde{\tau} = (\mathcal{N} \otimes \mathbb{I}_2)(\gamma)$ . Then,  $\tilde{\tau} = N^\Gamma$  where  $\Gamma$  is an involution ( $\Gamma^2 = \mathbb{I}$ ) defined by*

$$\langle i, j | X^\Gamma | k, l \rangle = \langle i, k | X | j, l \rangle \quad |i, j\rangle := |i\rangle \otimes |j\rangle \quad (2.112)$$

*Proof.* Without loss of generality,  $\mathcal{N} = XY^\Gamma$ , where  $X, Y \in B(\mathcal{H}_1, \mathcal{H}_2)$ . Let  $\{|i\rangle\}, \{|\alpha\rangle\}$  denote a basis on  $\mathcal{H}_1, \mathcal{H}_2$ , respectively. Then we have

$$X = \sum_{i,\alpha} x_{\alpha,i} |\alpha\rangle \langle i|, \quad (2.113)$$

$$Y = \sum_{j,\beta} y_{\beta,j} |\beta\rangle \langle j|, \quad (2.114)$$

which allows us to write

$$N = X \otimes Y \sum_{i,j,\alpha,\beta} x_{\alpha,i} y_{\beta,j} |\alpha\rangle \langle i| \otimes |\beta\rangle \langle j|, \quad (2.115)$$

then

$$\tilde{\tau} = (\mathcal{N} \otimes \mathbb{I})(\gamma), \quad (2.116)$$

$$= \sum_{k,l} X |k\rangle \langle l| Y^T \otimes |k\rangle \langle l|, \quad (2.117)$$

$$= \sum_{k,l,i,j,\alpha,\beta} x_{\alpha,i} y_{\beta,j} |\alpha\rangle \langle i|k\rangle \langle l|j\rangle \langle \beta| \otimes |k\rangle \langle l|, \quad (2.118)$$

$$= \sum_{i,j,\alpha,\beta} x_{\alpha,i} y_{\beta,j} |\alpha\rangle \langle \beta| \otimes |i\rangle \langle j|, \quad (2.119)$$

so we conclude

$$\langle \alpha, \beta | N | i, j \rangle = \langle \alpha, i | \tilde{\tau} | \beta, j \rangle \quad (2.120)$$

□

Note that  $\tilde{\tau} \in B(\mathcal{H}_2 \otimes \mathcal{H}_1, \mathcal{H}_1 \otimes \mathcal{H}_2)$  while  $N \in B(\mathcal{H}_1 \otimes \mathcal{H}_1, \mathcal{H}_2 \otimes \mathcal{H}_2)$ .

## 2.7 Complementary Channels

Let  $T : B(\mathcal{H}_A) \rightarrow B(\mathcal{H}_B)$  be a quantum channel. To simplify notation, we write  $T : A \rightarrow B$ . From proposition 6, we know that there exists a Stinespring isometry  $V : \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$  such that

$$T(X_A) = \text{tr}_E V X_A V^\dagger \quad (2.121)$$

A (non-unique) *complementary channel* is

$$T^c(X_A) = \text{tr}_B V X_A V^\dagger. \quad (2.122)$$

For a given channel  $T$  with Stinespring isometry  $V$ , the isometry  $\tilde{V} = (\mathbb{I} \otimes U)V$  with  $U$  unitary leads to the same channel. This relies on the cyclicity of partial trace. That is,

$$\text{tr}_E [(\mathbb{I}_B \otimes Y_E) X_{BE} (\mathbb{I}_B \otimes Z_E)] = \text{tr}_E [X_{BE} (\mathbb{I}_B \otimes Z_E Y_E)] \quad (2.123)$$

Using this we can write

$$\text{tr}_E \tilde{V} X_A \tilde{V}^\dagger = \text{tr}_E [(\mathbb{I} \otimes U) V X_A V^\dagger (\mathbb{I} \otimes U^\dagger)] = \text{tr}_E V X_A V^\dagger = T(X_A) \quad (2.124)$$

So, if we take an arbitrary unitary  $U$ , we can write  $\tilde{V} = (\mathbb{I} \otimes U)V$  and then

$$\text{tr}_B \tilde{V} X_A \tilde{V}^\dagger = \text{tr}_B [(\mathbb{I} \otimes U) V X_A V^\dagger (\mathbb{I} \otimes U^\dagger)] \quad (2.125)$$

$$= U \text{tr}_B (V X_A V^\dagger) U^\dagger \quad (2.126)$$

$$= U T^c(X_A) U^\dagger \quad (2.127)$$

Example:  $V = \sum_i K_i \otimes |i\rangle$  where  $\{|i\rangle\}$  is *some* orthonormal basis.

## Chapter 3

# Classes of Quantum Channels

### 3.1 Qubit channels

Note: please see Nielsen and Chuang for figures depicting these channels' actions on the Bloch sphere. I may make nice ones at some point but for now, I am too lazy.

1. **Bit flip channel.** First, we look at the classical bit flip channel, the properties of which were established by Claude Shannon in his seminal 1948 paper. The quantum version is simply given by the Pauli  $X$  operator,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (3.1)$$

which acts as

$$X |0\rangle = |1\rangle, \quad (3.2)$$

$$X |1\rangle = |0\rangle. \quad (3.3)$$

It's eigenbasis is  $|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ . So,  $X|+\rangle = |+\rangle$  and  $X|-\rangle = -|-\rangle$ . The channel acts as

$$\mathcal{F}_p^X : \rho \mapsto (1-p)\rho + pX\rho X \quad (3.4)$$

So, the Kraus operators are  $\sqrt{1-p}\mathbb{I}, \sqrt{p}X$

2. **Phase-flip/Z-dephasing channel**

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (3.5)$$

$$Z |0\rangle = |0\rangle \quad (3.6)$$

$$Z |1\rangle = -|1\rangle \quad (3.7)$$

$$Z |+\rangle = |-\rangle \quad (3.8)$$

$$Z |-\rangle = |+\rangle \quad (3.9)$$

The channel is given as

$$\mathcal{F}_p^Z : \rho \mapsto (1-p)\rho + pZ\rho Z \quad (3.10)$$

### 3. Bit-phase flip/Y-dephasing channel

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (3.11)$$

$$|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle) \quad (3.12)$$

$$Y|i\rangle = |i\rangle \quad (3.13)$$

$$Y|-i\rangle = -|-i\rangle \quad (3.14)$$

$$Y|0\rangle = i|1\rangle \quad (3.15)$$

$$Y|1\rangle = -i|0\rangle \quad (3.16)$$

The channel is then

$$\mathcal{F}_p^Y : \rho \mapsto (1-p)\rho + pY\rho Y \quad (3.17)$$

$$= (1-p)\rho + pXZ\rho ZX \quad (3.18)$$

4. **Depolarizing channel.** Corresponds to an error model in which each Pauli error occurs with equal probability. The channel is

$$\mathcal{D}_p : \rho \mapsto (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z) \quad (3.19)$$

with equal probability  $p/3$ . The Kraus operators are then  $\sqrt{1-p}\mathbb{I}$ ,  $\sqrt{p/3}X$ ,  $\sqrt{p/3}Y$ ,  $\sqrt{p/3}Z$ . Thus, the Kraus rank is 4 for this channel when  $p \in (0, 1)$ . An alternative representation is given by

$$\rho \mapsto (1-q)\rho + q\text{tr}(\rho)\frac{\mathbb{I}}{2} \quad (3.20)$$

This represents replacing the input state with the maximally mixed state with “probability”  $q$  ( $q$  can be greater than 1).

What about the relation  $p \leftrightarrow q$ ? To deduce this, we can use the identity

$$\frac{1}{2}\mathbb{I}_2 = \frac{1}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z) \quad \forall \rho \in B(\mathbb{C}^2) \quad (3.21)$$

We can then derive the relationship between  $p$  and  $q$ . We have

$$\frac{1}{2}\mathbb{I}_2 = \frac{1}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z) \quad \forall \rho \in B(\mathbb{C}^2) \quad (3.22)$$

$$(1-p)\rho + p\frac{\mathbb{I}}{2} = (1-q)\rho + \frac{q}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z) \quad (3.23)$$

$$\implies \boxed{q = \frac{4}{3}p} \quad (3.24)$$

5. **Generalized Pauli channel.** Let  $\vec{p} = (p_0, p_1, p_2, p_3)$  be a probability distribution. The generalized Pauli channel is

$$\mathcal{N}_{\vec{p}}(\rho) = p_0\rho + p_1X\rho X + p_2Y\rho Y + p_3Z\rho Z \quad (3.25)$$

where we recover the depolarizing channel by setting  $p_0 = 1 - p$  and  $p_i = p/3$ . Note that for any  $\vec{p}$ , this channel is unital.

Pauli channels are interesting from an information theoretic standpoint. Classically, they are very easily understood. Quantum mechanically, they very much are not understood (except in the case of flip or dephasing channels).

In what sense are these flip channels de-phasing? Let us look at the example of the phase flip channel

$$\mathcal{F}_p^Z : \rho \mapsto (1-p)\rho + pZ\rho Z. \quad (3.26)$$

We can understand the justification of the term de-phasing by looking at the action on the density matrix

$$\begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix} \mapsto \begin{pmatrix} \rho_{11} & (1-2p)\rho_{12} \\ (1-2p)\rho_{21} & \rho_{22} \end{pmatrix} \quad (3.27)$$

where  $\rho \geq 0, \text{tr}(\rho) = 1 \implies \rho_{11} + \rho_{22} = 1$ . We can make the following observations

1. If  $\rho = x|0\rangle\langle 0| + (1-x)|1\rangle\langle 1|$ , then

$$\mathcal{F}_p^Z(\rho) = \rho \quad \forall p \in [0, 1] \quad (3.28)$$

2.  $p = \frac{1}{2}$ : the channel is diagonal in the z-basis for all input states

We can also think about sending classical information through this channel. Let us encode 0 as  $|0\rangle\langle 0|$  and 1 as  $|1\rangle\langle 1|$ . That is, we are encoding one bit in one qubit. We can do this reliably with this channel because

$$\mathcal{F}_p^Z(|0\rangle\langle 0|) = |0\rangle\langle 0|, \quad (3.29)$$

$$\mathcal{F}_p^Z(|1\rangle\langle 1|) = |1\rangle\langle 1|. \quad (3.30)$$

This means that we can send one bit through the channel. The key idea is: this channel preserves classical information because it preserves the orthogonality of the basis states. The same would hold for the  $X$  channel but you would have to encode info in the  $|\pm\rangle$  basis.

6. **Amplitude damping channel.** Physical model: 2-level system (e.g. an atom with a ground state  $|0\rangle$  and excited state  $|1\rangle$ ). If the system is in an excited state  $|1\rangle$ , it decays with a certain probability,  $\gamma$ , emitting a photon to the environment. How can we capture this decay process mathematically? Consider the isometry

$$|0\rangle_A \mapsto |0\rangle_B |0\rangle_E, \quad (3.31)$$

$$|1\rangle \mapsto \sqrt{1-\gamma}|1\rangle_B |0\rangle_E + \sqrt{\gamma}|0\rangle_B |1\rangle_E. \quad (3.32)$$

Compactly we can write

The Kraus operators for this channel are

$$K_0 = \langle 0|_E V = |0\rangle\langle 0|_B + \sqrt{1-\gamma}|1\rangle\langle 1|_B = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad (3.33)$$

$$K_1 = \langle 1|_E V = \sqrt{\gamma}|0\rangle\langle 0|_B = \begin{pmatrix} 0 & \gamma \\ 0 & 0 \end{pmatrix}. \quad (3.34)$$

In the Kraus representation, then, we can write the amplitude damping channel

$$\mathcal{A}_\gamma : \rho \mapsto K_0 \rho K_0^\dagger + K_1 \rho K_1^\dagger. \quad (3.35)$$



We note that the amplitude damping channel is not unital. Therefore, it is not a Pauli (or even a mixed-unitary) channel. Interestingly, it is completely understood how to send *quantum information* through the amplitude damping channel; however, it is not known how much classical information can be sent through this channel.

**7. Erasure channel.** Classical model:

Quantum version:  $\mathcal{E}_p : B(\mathcal{H}) \rightarrow B(\mathcal{H} \otimes \mathbb{C})$ . The channel acts as

$$\rho \mapsto (1-p)\rho + p \text{tr}(\rho) |e\rangle \langle e|. \quad (3.36)$$

This channel has Kraus operators given by  $K_0\sqrt{1-p}\mathbb{I}, K_1\sqrt{p}|0\rangle\langle 0|, K_2\sqrt{p}|e\rangle\langle 1|$ . Note that  $|e\rangle$  must be orthogonal to all  $\rho \in B(\mathcal{H})$ . That is,  $\langle e|e\rangle, \rho = 0 \quad \forall \rho \in B(\mathcal{H})$ . Bob can always tell whether erasure happened by performing a measurement! This is a very well-understood quantum channel.

### 3.2 Generalized dephasing channels

A generalized dephasing channel leaves a *fixed* orthonormal basis invariant and it dephases off-diagonal elements with respect to that fixed basis. That is, we lose quantum coherences under the action of a generalized dephasing channel.

Construction:  $\mathcal{H} = \mathbb{C}^d$  with orthonormal basis  $\{|i\rangle\}_{i=1}^d$ . Choose an environment  $\mathcal{H}_E$  with  $\dim \mathcal{H}_E := |E| \geq 2$ , and let  $\{\varphi_i\}_{i=1}^{|E|}$  be *some* set of pure states on  $E$ . This set is normalized but not orthogonal. Then, define the isometry

$$V : |i\rangle_A \mapsto |i\rangle_B \otimes |\varphi_i\rangle_E. \quad (3.37)$$

The Stinespring extension is

$$\mathcal{N}(\rho_A) = \text{tr}_E V \rho_A V^\dagger, \quad (3.38)$$

$$= \sum_{i,j} |i\rangle \rho \langle i| |j\rangle \langle j|_B \text{tr}(|\varphi_i\rangle \langle \varphi_j|), \quad (3.39)$$

$$= \sum_{i,j} \langle \varphi_i | \varphi_j \rangle \langle i | \rho | j \rangle |i\rangle \langle i|_B. \quad (3.40)$$

Let us confirm this channel acts as expect.

$$[\mathcal{N}(\rho)]_{kk} = \langle \varphi_k | \varphi_k \rangle \langle k | \rho | k \rangle = \rho_{kk}, \quad (3.41)$$

$$[\mathcal{N}(\rho)]_{jk} = \langle \varphi_j | \varphi_k \rangle \langle j | \rho | k \rangle, \quad (3.42)$$

but  $0 < \langle \varphi_j | \varphi_k \rangle \leq 1$ . Thus, we see that the diagonals are preserved but the off-diagonals are dephased.

Higher-dimensional example: Let  $d \geq 2$ , and define two unitaries

$$X |i\rangle = |i+1 \bmod d\rangle \quad (\text{shift operator}) \quad (3.43)$$

$$Z |j\rangle = \omega^j |j\rangle, \text{ where } \omega = \exp\left(\frac{2\pi i}{d}\right) \quad (\text{clock operator}) \quad (3.44)$$

This generalizes the Pauli operators:  $X^d = Z^d = \mathbb{I}$ . These are the generators of the Heisenberg-Weyl group:

$$\{\omega^j Z^k X^l : j, k, l \in [d]\}. \quad (3.45)$$

So, for  $\rho \in B(\mathbb{C}^d)$  we maps like

$$\rho \mapsto (1-p)\rho + pX\rho X^\dagger, \quad (3.46)$$

$$\rho \mapsto (1-p)\rho + \frac{p}{3}Z\rho Z^\dagger + \frac{2p}{3}Z^2\rho(Z^\dagger)^2. \quad (3.47)$$

The generalized de-phasing channels have full classical capacity

$$C(\mathcal{N}) = \log d \quad (\text{in general, } C(\mathcal{N}) \leq \log d) \quad (3.48)$$

Sketch of a proof: we know that for a generalized dephasing channel, there exists an orthonormal basis  $\{|i\rangle\}_i$  such that

$$\mathcal{N}(|i\rangle\langle i|) = |i\rangle\langle i| \quad (3.49)$$

of classical signals/messages  $x_i, \dots, x_d$ . We can use the encoding

$$x_i \mapsto |i\rangle\langle i| \quad (3.50)$$

where  $\langle i|j\rangle = \delta_{ij}$ . Thus,  $d$  messages can be sent perfectly. So  $\log d$  bits of classical info can be sent through  $\mathcal{N}$ . Bob can measure the output to retrieve the classical message.

### 3.2.1 Detour: Holevo information ( $\mathcal{X}$ -quantity)

Recall: the von Neumann entropy is defined as

$$S(\rho) = -\text{tr} \rho \log \rho. \quad (3.51)$$

When one has the spectral decomposition of  $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$ , the von Neumann entropy is just the Shannon entropy for the eigenvalue distribution

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i. \quad (3.52)$$

If we then have an ensemble of quantum states  $E = \{p_x, \rho_x\}$ , we have

$$\mathcal{X}(E, \mathcal{N}) = S\left(\sum_x p_x \mathcal{N}(\rho_x)\right) - \sum_x p_x S(\mathcal{N}(\rho_x)) \quad (3.53)$$

The Holevo information is then defined as

$$\boxed{\text{Holevo Information, } \mathcal{X}(\mathcal{N}) = \max_E \mathcal{X}(E, \mathcal{N})} \quad (3.54)$$

A fundamental result due to Holevo, Schumacher, and Westmoreland is

$$\boxed{C(\mathcal{N}) \geq \mathcal{X}(\mathcal{N})} \quad (3.55)$$

If  $\mathcal{N}$  is a generalized dephasing channel, there exists an orthonormal basis  $\{|i\rangle\}$  such that  $\mathcal{N}(|i\rangle\langle i|) = |i\rangle\langle i|$  for all  $i$ . Let our ensemble be

$$\rho_i = |i\rangle\langle i| \quad (3.56)$$

$$p_i = \frac{1}{d}, \quad (3.57)$$

which implies

$$\bar{\rho} = \sum_i p_i \rho_i = \frac{1}{d} \mathbb{I} \quad (3.58)$$

Then,  $E_n = \{\frac{1}{d}, \rho_i\}$ , so the Holevo quantity is

$$\mathcal{X}(E_n, \mathcal{N}) = S\left(\sum_i p_i \mathcal{N}(\rho_i)\right) - \sum_i p_i S(\mathcal{N}(\rho_i)) \quad (3.59)$$

$$= S\left(\sum_i p_i \rho_i\right) - \sum_i p_i S(\rho_i) \quad (3.60)$$

$$= \log d - 0 \quad (3.61)$$

$$= \log d \quad (3.62)$$

Thus, we have the following chain of inequalities

$$\log d \leq \mathcal{X}(\mathcal{N}) \leq C(\mathcal{N}) \leq \log d \implies \boxed{C(\mathcal{N}) = \log d} \quad (3.63)$$

as desired.

### 3.2.2 Some comments on last lecture

- The rank of the Kraus operators is not unitarily invariant. We can see this by examining the 50-50 dephasing channel.

$$\rho \mapsto \frac{1}{2}\rho + \frac{1}{2}Z\rho Z \implies K_0 = \frac{1}{\sqrt{2}}\mathbb{I}, \quad K_1 = \frac{1}{\sqrt{2}}Z \quad (3.64)$$

We can apply a Hadamard transform to the operators to obtain new Kraus operators

$$L_i = \sum_j H_{ij} K_j, \quad (3.65)$$

$$\implies L_0 = |0\rangle\langle 0|, L_1 = |1\rangle\langle 1|, \quad (3.66)$$

which are rank-1 operators now when the previous Kraus operators were full rank.

- Every unital qubit channel is unitarily equivalent to a Pauli channel. That is, if  $\mathcal{N} : B(\mathbb{C}^2) \rightarrow B(\mathbb{C}^2)$  is a unital channel, then there are unitaries  $U, V$  such that

$$M(\rho) = U\mathcal{N}(V\rho V^\dagger)U^\dagger \quad (3.67)$$

is Pauli.

- mixed unitary channels

$$\rho \mapsto \sum_i p_i U_i \rho U_i^\dagger, \quad U_i \text{ unitary} \quad (3.68)$$

$$\mathbb{I} \mapsto \sum_i p_i U_i U_i^\dagger = \mathbb{I} \quad \text{unital!} \quad (3.69)$$

Every unital qubit channel is mixed unitary. Watrous' book provides a nice example of a unital channel that is *not* mixed unitary:

$$X \in B(\mathbb{C}^3), \quad \rho \mapsto \frac{1}{2} \text{tr}(X) \mathbb{I} - \frac{1}{2} X^T \quad (3.70)$$

### 3.3 Entanglement-breaking channels

Reminder: A bipartite  $\rho_{AB}$  is called separable if it lies in the convex hull of product states. That is,

$$\rho_{AB} \in \text{conv}\{\omega_A \otimes \sigma_B : \omega_{A(B)} \text{ state on } \mathcal{H}_{A(B)}\} \quad (3.71)$$

Explicitly,

$$\rho_{AB} = \sum_i p_i \omega_A^i \otimes \sigma_B^i \quad (3.72)$$

**Definition 3.3.1.** A channel  $\mathcal{N} : A \rightarrow B$  is entanglement-breaking if

$$(\mathbb{I}_R \otimes \mathcal{N})(\rho_{RA}) \quad (3.73)$$

is separable for any  $\rho_{RA}$ .

**Proposition 3.3.1.** The following are all equivalent

- $\mathcal{N} : A \rightarrow B$  is entanglement breaking
- $\tau_{AB}^{\mathcal{N}} = (\mathbb{I}_A \otimes \mathcal{N})(\gamma_{AA'})$  is separable
- $\mathcal{N}$  has a Kraus representation with rank-1 Kraus operators
- $\mathcal{N}$  is a measure-and-prepare channel: there exists POVM  $E = \{E_i\}_i$  and states  $\{\sigma_i\}_i$  such that

$$\mathcal{N}(\rho) = \sum_i \text{tr}(\rho E_i) \sigma_i \quad (3.74)$$

where we recall that a POVM must satisfy  $E_i \geq 0, \sum_i E_i = \mathbb{I}$ .

*Proof.* (a  $\implies$  b):  $(\mathbb{I}_R \otimes \mathcal{N})(\rho_{RA})$  is separable for all  $\rho_{RA}$ . In particular, for  $\gamma_{RA}$ ,  $(|\gamma\rangle_{RA}) = \sum_i |i\rangle_R |i\rangle_A$ .

(b  $\implies$  c):  $\tau_{AB}^{\mathcal{N}}$  is separable: there exist pure states  $\psi_i = |\psi_i\rangle\langle\psi_i|_A$  and  $\varphi_i = |\varphi_i\rangle\langle\varphi_i|_B$  such that  $\frac{1}{d}\tau_{AB}^{\mathcal{N}} = \sum_i p_i \psi_i \otimes \varphi_i$ , where  $d = |A|$ . Then, set  $K_i = \sqrt{p_i d} |\varphi_i\rangle_B \langle\psi_i|_A$ . We can then check the action of these operators

$$\frac{1}{d} \sum_i (\mathbb{I} \otimes K_i) (\gamma_{AA'}) (\mathbb{I}_A \otimes K_i)^\dagger = \frac{1}{d} \sum_{i,j,k} |j\rangle\langle k|_A \otimes K_i |j\rangle\langle k|_{A'} K_i^\dagger \quad (3.75)$$

$$= \sum_{i,j,k} d p_i |j\rangle\langle k|_A \otimes \langle\bar{\psi}_i| |j\rangle\langle k| |\bar{\psi}_i\rangle |\varphi_i\rangle\langle\varphi_i|_B \quad (3.76)$$

$$= \sum_{i,j,k} p_i |j\rangle\langle k|_A \otimes \langle\bar{\psi}_i| |j\rangle\langle k| |\bar{\psi}_i\rangle |\varphi_i\rangle\langle\varphi_i|_B \quad (3.77)$$

$$= \sum_i p_i \left( \sum_{j,k} \langle k| \bar{\psi}_i | j \rangle |j\rangle\langle k| \right) \otimes |\varphi_i\rangle\langle\varphi_i|_B \quad (3.78)$$

$$= \sum_i p_i (\psi_i) \otimes \varphi_i \quad (3.79)$$

$$= \frac{1}{d} \tau_{AB}^{\mathcal{N}} \quad (3.80)$$

$$\sum_i K_i^\dagger K_i = \mathbb{I} \quad (3.81)$$

$$= d \sum_i p_i |\bar{\psi}_i\rangle\langle\bar{\psi}_i| |\varphi_i\rangle\langle\varphi_i| \quad (3.82)$$

$$= d \sum_i p_i \bar{\psi}_i \quad (3.83)$$

$$= d \left( \sum_i p_i \bar{\psi}_i \right) \quad (3.84)$$

$$= d \frac{1}{d} \bar{\mathbb{I}}_A \quad (3.85)$$

$$= \mathbb{I}_A \quad (3.86)$$

(c  $\implies$  d):  $\text{rank}(K_i)=1$ :  $K_i = |\mathcal{X}_i\rangle_B \langle\omega_i|_A$  for some vectors  $|\mathcal{X}_i\rangle_B, |\omega_i\rangle_A, \langle\mathcal{X}_i|\mathcal{X}_i\rangle = 1$ .

$$\mathcal{N}(\rho) = \sum_i K_i \rho K_i^\dagger \quad (3.87)$$

$$= \sum_i \langle\omega_i|\rho|\omega_i\rangle |\mathcal{X}_i\rangle\langle\mathcal{X}_i|_B \quad (3.88)$$

POVM:  $\omega = \{\omega_i\}$ , states:  $\mathcal{X}_i$

$$\mathbb{I} = \sum_i K_i^\dagger K_i \quad (3.89)$$

$$= \sum_i |\omega_i\rangle\langle\omega_i| \langle\mathcal{X}_i|\mathcal{X}_i\rangle \quad (3.90)$$

$$= \sum_i |\omega_i\rangle\langle\omega_i| \quad (3.91)$$

(d  $\implies$  a): Let  $\rho_{RA}$  be arbitrary:

$$(\mathbb{I}_R \otimes \mathcal{N})(\rho_{RA}) = \sum_i \text{tr}_B [(\mathbb{I}_A \otimes E_i)\rho_{RA}] \otimes \sigma_i \quad (3.92)$$

$$= \sum_i \text{tr}_B [(\mathbb{I}_R \otimes \sqrt{E_i})\rho_{RA}(\mathbb{I}_R \otimes \sqrt{E_i})] \otimes \sigma_i \quad (3.93)$$

$$= \sum_i p_i \omega_i \otimes \sigma_i \quad (3.94)$$

where  $p_i = \text{tr}(E_i \rho_{RA})$ ,  $\omega_i = \frac{1}{p_i} \text{tr}_B [(\mathbb{I}_R \otimes \sqrt{E_i})\rho_{RA}(\mathbb{I}_R \otimes \sqrt{E_i})] \geq 0$ .  $\square$

We note that there are *some* channel capacities of entanglement-breaking channels that are understood.

- Quantum information transmission is equivalent to generating entanglement. Because entanglement-breaking channels cannot do that, their quantum capacity is zero.
- $C(\mathcal{N}) \geq \mathcal{N}$ ,  $C(\mathcal{N}) = \sup_{n \in \mathbb{N}} \frac{1}{n} \mathcal{X}(\mathcal{N}^{\otimes n})$ . Entanglement-breaking channels destroy entanglement between different inputs. This implies that

$$C(\mathcal{N}) = \mathcal{X}(\mathcal{N}) \quad (3.95)$$

BUT:  $\mathcal{X}(\mathcal{N})$  is NP-hard to compute, so this relationship doesn't actually get us much.

### 3.4 PPT-channels

Checking separability is NP-hard. So, is there some easier criterion? The standard relaxed criterion is following.

**Definition 3.4.1.** *Peres-Horodecki criterion: if  $\rho_{AB}$  is separable if  $\rho_{AB}$  has a positive partial transpose with respect to either party.*

Let us see why this is a reasonable criterion for separability. If  $\rho_{AB}$  is separable,

$$\rho_{AB} = \sum_i p_i \omega_A^i \otimes \sigma_B^i \quad (3.96)$$

$$\implies \rho_{AB}^{T_B} = \sum_i p_i \omega_A^i \otimes (\sigma_B^i)^T \geq 0 \quad (3.97)$$

- if  $\rho_{AB}$  is NPT  $\implies \rho_{AB} \notin \text{SEP}$ .
- if  $|A| \cdot |B| \leq 6$ , then  $\rho_{AB} \in \text{SEP} \Leftrightarrow \rho_{AB} \in \text{PPT}$ .

**Definition 3.4.2.** *A channel  $\mathcal{N} : A \rightarrow B$  is called PPT if  $(\mathbb{I}_R \otimes \mathcal{N})(\rho_{RA})$  is PPT for all  $\rho_{RA}$ .*

**Proposition 3.4.1.** *The following are all equivalent*

- $\mathcal{N} : A \rightarrow B$  is PPT
- $\tau_{AB}^{\mathcal{N}}$  is PPT
- $\vartheta \circ \mathcal{N}$  is CP (Recall that when  $\vartheta : X \mapsto X^T : (\mathbb{I}_R \otimes \vartheta)(\gamma) = \mathbb{F} \not\geq 0$ )

*Proof.* (a  $\Rightarrow$  b): True by definition. We know

$$(\mathbb{I}_A \otimes \mathcal{N})(\rho_{AA'}) \quad (3.98)$$

is PPT, in particular for  $\rho = \gamma_{AA'}$ .

(b  $\Rightarrow$  c):

$$(\mathbb{I}_A \otimes \vartheta \circ \mathcal{N})(\gamma) = (\mathbb{I} \otimes \vartheta)(\mathbb{I} \otimes \mathcal{N})(\gamma_{AA'}) \quad (3.99)$$

$$= (\mathbb{I}_A \otimes \vartheta)(\tau_{AB}^{\mathcal{N}}) \quad (3.100)$$

$$= (\tau_{AB}^{\mathcal{N}})^{T_B} \geq 0 \quad (3.101)$$

(c  $\Rightarrow$  a)  $\vartheta \circ \mathcal{N}$  is CP:

$$(\mathbb{I}_R \otimes \vartheta \circ \mathcal{N})(\rho_{RA}) \geq 0 \quad \forall \rho_{RA} \geq 0 \quad (3.102)$$

This implies  $\mathcal{N}$  is PPT.  $\square$

**Remarks:** In general,  $\vartheta \circ \mathcal{N}$  is *not* CP. However, for every CP map  $\mathcal{N}$ , the map  $\vartheta \circ \mathcal{N} \circ \vartheta$  is CP (see exercises).

What about the capacities of PPT channels?

- Horodeckis: PPT states are undistillable. Entanglement distillation: given iid copies of a state  $\rho_{AB}$ , the goal is to convert these copies into a smaller number of maximally entangled states. If there is an entanglement distillation protocol (LOCC) such that

1. error of the protocol tends to 0 as  $n \Rightarrow \infty$
2. rate  $c := \frac{1}{n} \log m_n \rightarrow c > 0$  as  $n$  goes to infinity

then  $\rho_{AB}$  is *distillable*. We conclude that the quantum capacity for PPT channels is zero. This result even holds if two-way classical communication is allowed!

We note that the set of protocols allowing only one-way communication is a strict subset of the set of protocols allowing two-way communication. Even still, the Horodecki's showed that the quantum capacity of all PPT channels is zero in both cases. Also note that the classical capacity is generally unknown.

### 3.5 Anti-degradable channels

Let  $\mathcal{N}$  be a quantum channel from  $A$  to  $B$  with an isometry  $V : \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$  such that  $\mathcal{N}(\rho) = \text{tr}_E V \rho V^\dagger$ . Recall that the complementary channel is  $\mathcal{N}^c(\rho) = \text{tr}_B V \rho V^\dagger$ .

**Definition 3.5.1.**  $\mathcal{N}$  as above is called *antidegradable* if there exists a channel  $\mathcal{A} : E \rightarrow B$  such that

$$\mathcal{N} = \mathcal{A} \circ \mathcal{N}^c \quad (3.103)$$

Intuition: Eve (environment) can locally obtain Bob's output via the channel  $\mathcal{A}$ . Antidegradable channels cannot transmit quantum information and thus have zero quantum capacity,  $Q(\mathcal{N}) = 0$ .

A "proof" of this is as follows. Assume that this channel has non-zero quantum capacity. This means that Alice can faithfully send qubits to Bob at a positive rate. But there is a protocol based on the channel  $\mathcal{A}$  that lets Eve implement the same protocol that Alice and Bob use. This violates no-cloning and is thus prohibited.

**Examples of anti-degradable channels:**

1. erasure channel  $\mathcal{E}_p : \rho \mapsto (1-p)\rho + p\text{tr}(\rho) |e\rangle\langle e|$  for  $p \geq \frac{1}{2}$ .

Let  $\mathcal{H}_1 = \mathbb{C}^2$  be the input space. Let the  $\mathcal{H}_2 = \mathbb{C}$  be an erasure flag. Let  $\mathcal{E}_p : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_1 \oplus \mathcal{H}_2)$ . That is, an input state maps as

$$\rho \mapsto (1-p)\tilde{\rho} + p\text{tr}(\rho) |e\rangle\langle e| \quad (3.104)$$

So, how do we embed our input state in the larger space? We use a pretty trivial embedding that is represented as:

$$\hat{\rho} = \begin{pmatrix} \rho_{00} & \rho_{01} & 0 \\ \rho_{10} & \rho_{11} & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (3.105)$$

and the erasure flag is simply

$$|e\rangle\langle e| = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \quad (3.106)$$

Note that the complementary channel of the erasure channel has the same form but with the probabilities flipped:

$$\mathcal{E}_p^c : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_1 \oplus \mathcal{H}_2), \rho \mapsto p\tilde{\rho} + (1-p)\text{tr}(\rho) |e\rangle\langle e|. \quad (3.107)$$

Now consider  $p \geq \frac{1}{2}$  and define  $q = \frac{2p-1}{p}$ . the idea is that we erase  $\tilde{\rho}$  with probability  $q$  and do nothing with  $|e\rangle\langle e|$ .

$$\mathcal{E}_q(p\rho) = p(1-q)\tilde{\rho} + pq\text{tr}(\rho) |e\rangle\langle e| \quad (3.108)$$

$$= (1-p)\tilde{\rho} + (2p-1) |e\rangle\langle e| \quad (3.109)$$

$$= (1-p) |e\rangle\langle e| \quad (3.110)$$

**almost certainly messed up p's and q's here.**

We need to extend the action of  $\mathcal{E}_q$  to  $B(\mathcal{H}_1 \otimes \mathcal{H}_2)$ . The solution is to define  $\mathcal{A}$  in



the Kraus representation. The Kraus operators are

$$K_0 = \sqrt{1-q} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (3.111)$$

$$K_1 = \sqrt{q} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad (3.112)$$

$$K_2 = \sqrt{q} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad (3.113)$$

$$K_3 = \sqrt{q} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (3.114)$$

where the first three operators correspond to erasure on  $B(\mathcal{H}_1 \oplus 0)$  and the last to doing nothing on  $B(0 \oplus \mathcal{H}_2)$ . This definition ensures that  $\mathcal{E}_p = \mathcal{A} \circ \mathcal{E}_p^c$  for  $p \geq \frac{1}{2}$ . We have  $B(\mathcal{H}_1 \oplus 0), B(0 \oplus \mathcal{H}_2) : \mathcal{A}_p = \mathcal{E}_p \oplus \mathbb{I}$ .

For  $\rho \in B(\mathcal{H}_1)$ ,  $\sigma = (1-\lambda)\tilde{\rho} + \lambda|e\rangle\langle e|$ . This has the block matrix:

$$\begin{pmatrix} (1-\lambda)\rho & 0 \\ 0 & \lambda \end{pmatrix} \quad (3.115)$$

So

$$(\mathcal{E}_p \oplus \mathbb{I})(\sigma) = \begin{pmatrix} \mathcal{E}_p((1-\lambda)\rho) & 0 \\ 0 & \mathbb{I}(\lambda) \end{pmatrix} \quad (3.116)$$

Then for  $\omega \in B(\mathcal{H}_1 \oplus \mathcal{H}_2)$  we have

$$\omega = \begin{pmatrix} \omega_{\mathcal{H}_1} & * \\ * & \omega_{\mathcal{H}_2} \end{pmatrix} \quad (3.117)$$

which has off-diagonal elements. We can get rid of these by measuring with respect to  $\mathcal{H}_1 \oplus \mathcal{H}_2 = \mathcal{H}$ . Let  $P_2 = |e\rangle\langle e|$ ,  $P_1 = \mathbb{I} - |e\rangle\langle e|$ . Then  $P_1\omega P_1 + P_2\omega P_2$  is diagonal. Finally,  $\mathcal{A}_M = P_1 \cdot P_1 + P_2 \cdot P_2$  which implies  $\mathcal{A} - \mathcal{A}_p \circ \mathcal{A}_M$  where  $\mathcal{A}_p = \mathcal{E}_p \oplus \mathbb{I}$ .

2. amplitude damping channel  $\mathcal{A}_\gamma$  for  $\gamma \geq \frac{1}{2}$ .
3. depolarizing channel  $\mathcal{D}_p$  for  $p \geq \frac{1}{4}$

**Definition 3.5.2.** Let  $\mathcal{N} : A \rightarrow B$  be a quantum channel and let  $G$  be a group with unitary representations  $U_g$  on  $\mathcal{H}_A$  and  $V_g$  on  $\mathcal{H}_B$ . Then  $\mathcal{N}$  is called covariant with respect to  $(G, U_g, V_g)$  if

$$V_g \mathcal{N}(\cdot) V_g^\dagger = \mathcal{N}(U_g \cdot U_g^\dagger) \quad (3.118)$$

for all  $g \in G$ .

**Representation theory basics:**

- $(\varphi, V)$  is a representation of  $G$ :  $\varphi : G \rightarrow GL(V)$ ,  $\varphi(gh) = \varphi(g)\varphi(h)$ . Subspace  $W \leq V$  is called  $G$ -invariant, if  $\varphi(g)w \in W \quad \forall w \in W, \forall g \in G$ .
- $\{0\}, V$  are always  $G$ -invariant
- $(\varphi, V)$  is called irreducible if  $\{0\}, V$  are the only  $G$ -inv subspaces.
- Schur's lemma:  $(\varphi, V), (\psi, W)$  representations of  $G$ .  $G$ -linear map  $f : V \rightarrow W$   $f \circ \varphi(g) = \psi(g) \circ f$ . If  $\varphi, \psi$  are irreducible representations, then either  $V \not\cong W$  and  $f = 0$  or  $V \cong W$  and  $f = \lambda \mathbb{I}_{V \rightarrow W}$  for some  $\lambda \in \mathbb{C}$ .

### Some examples:

- Pauli channels:  $\rho \mapsto p_0\rho + p_1X\rho X + p_2Y\rho Y + p_3Z\rho Z$   
Covariance group: Pauli group,  $P = \{\pm 1, \pm i\} \cup \{\mathbb{I}, X, Y, Z\}$   
For  $\theta_1, \theta_2 \in P$ :  $\vartheta_1\theta_2 \cdot \theta_2^\dagger\vartheta_1^\dagger = \vartheta_2\theta_1 \cdot \theta_1^\dagger\vartheta_2^\dagger$
- depolarizing channel:  $\rho \mapsto (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$ . The covariance group is  $\mathcal{U}(2)$ . This is easy to see in the "q-representation":  $\rho \mapsto (1-q)\rho + q\text{tr}\rho \frac{1}{2}\mathbb{I}$

$$\mathcal{D}_q(U\rho U^\dagger) = (1-q)U\rho U^\dagger + q\text{tr}(U\rho U^\dagger)\frac{1}{2}\mathbb{I} = U\mathcal{D}_p(\rho)U^\dagger \quad (3.119)$$

In  $d \geq 2$  dimensions:  $\rho \mapsto (1-q)\rho + q\text{tr}\rho \frac{1}{d}\mathbb{I}$ . The covariance group is  $\mathcal{U}(d)$ .

- Amplitude damping channel  $A_\gamma = \{K_0, K_1\}$  as normal. Covariance group:  $\{\mathbb{I}, Z\} \cong \mathbb{Z}_2$ .
- Erasure channel  $\mathcal{E}_p(\rho) = (1-p)\rho + p\text{tr}\rho |e\rangle\langle e|$ . The covariance group is again  $\mathcal{U}(2)$ . Similarly, in  $d \geq 2$  dimensions, the  $d$ -dimensional erasure channel with covariance group  $\mathcal{U}(d)$ .

**Proposition 3.5.1.** *A channel  $\mathcal{N} : A \rightarrow B$  is  $(G, U_g, V_g)$ -covariant iff  $\tau^{\mathcal{N}_{AB}} = (\bar{U}_g \otimes V_g)\tau_{AB}^{\mathcal{N}}(\bar{U}_g \otimes V_g)^\dagger$  for all  $g \in G$ .*

*Proof.*  $(\Rightarrow)$ :  $V_g\mathcal{N}(\cdot)V_g^\dagger = \mathcal{N}(U_g \cdot U_g^\dagger)$  for all  $g \in G$ . This is equivalent to  $\mathcal{N}(\cdot) = V_g^\dagger\mathcal{N}(U_g \cdot U_g^\dagger)V_g$  for all  $g \in G$ .

$$\tau_{AB}^{\mathcal{N}} = (\mathbb{I} \otimes \mathcal{N})(\gamma) \quad (3.120)$$

$$= (\mathbb{I}_1 \otimes V_g^\dagger)(\mathbb{I} \otimes \mathcal{N}) \left( (\mathbb{I}_1 \otimes U_g)\gamma(\mathbb{I} \otimes U_g^\dagger) \right) (\mathbb{I}_1 \otimes V_g) \quad (3.121)$$

$$= (\mathbb{I} \otimes V_g)(\mathbb{I} \otimes \mathcal{N}) \left( (U_g^T \otimes \mathbb{I}_2)\gamma(U_g^T \otimes \mathbb{I}_2)^\dagger \right) (\mathbb{I} \otimes V_g) \quad (3.122)$$

$$= (U_g^T \otimes V_g^\dagger)(\mathbb{I} \otimes \mathcal{N})(\gamma)(\bar{U}_g \otimes V_g) \quad (3.123)$$

$$\Rightarrow \tau_{AB}^{\mathcal{N}} = (U_g^T \otimes V_g^\dagger)\tau_{AB}^{\mathcal{N}}(\bar{U}_g \otimes V_g) \quad \text{for all } g \in G \quad (3.124)$$

$(\Leftarrow)$ :  $\tau_{AB}^{\mathcal{N}} = (\bar{U}_g \otimes V_g)\tau_{AB}^{\mathcal{N}}(\bar{U}_g \otimes V_g)^\dagger$  for all  $g \in G$ . This implies  $(U_g^T \otimes \mathbb{I})\tau_{AB}^{\mathcal{N}}(U_g^T \otimes \mathbb{I})^\dagger = (\mathbb{I} \otimes V_g)\tau_{AB}^{\mathcal{N}}(\mathbb{I} \otimes V_g)^\dagger$ .

Recall the choi isomorphism:  $\mathcal{N}(X) = \text{tr}_1 \tau_{AB}^{\mathcal{N}}(X^T \otimes \mathbb{I})$ .

$$\mathcal{N}(U_g X U_g^\dagger) = \text{tr}_1 \left[ \tau_{AB}^{\mathcal{N}}((U_g X U_g^\dagger)^T \otimes \mathbb{I}) \right] \quad (3.125)$$

$$= \text{tr}_1 \left[ (U_g^T \otimes \mathbb{I}) \tau_{AB}(U_g^T \otimes \mathbb{I})^\dagger (X^T \otimes \mathbb{I}) \right] \quad (3.126)$$

$$= \text{tr}_1 \left[ (\mathbb{I} \otimes V_g) \tau_{AB}(\mathbb{I} \otimes V_g)^\dagger (X^T \otimes \mathbb{I}) \right] \quad (3.127)$$

$$= V_g \text{tr}_1 [\tau^{\mathcal{N}_{AB}}(X^T \otimes \mathbb{I})] V_g^\dagger \quad (3.128)$$

$$= V_g \mathcal{N}(X) V_g^\dagger \quad (3.129)$$

□

**Problem:** with the above proposition is that it is basis-dependent (via the Choi operator).

**Solution:** is that there is also a basis independent version based on the Jamolkowski operator  $J_{AB}^{\mathcal{N}} = (\mathbb{I} \otimes \mathcal{N})(\mathbb{F}_{AA'})$  where  $\mathbb{F}_{AB} = |\gamma\rangle\langle\gamma|^{TA}$ . In terms of the Jamolkowski operator,  $(G, U_g, V_g)$ -covariance of  $\mathbb{N}$  is equivalent to  $(U_g \otimes V_g) J_{AB}^{\mathcal{N}} (U_g \otimes V_g)^\dagger = J_{AB}^{\mathcal{N}}$  for all  $g \in G$ .

We note that a  $d$ -dimensional depolarizing channel;  $\rho \mapsto (1-q)\rho + q \text{tr} \rho \frac{1}{d} \mathbb{I}_d$  has  $\mathcal{U}(d)$  as its covariance group.

**Proposition 3.5.2.** *Let  $\mathcal{N} : A \rightarrow B$  be a channel with input and output spaces of equal dimension  $d$ . If  $U \mathcal{N}(\cdot) U^\dagger = \mathcal{N}(U \cdot U^\dagger)$  for all  $U \in \text{mathcal{U}}(d)$ , then*

$$\mathcal{N} = (1-q) \cdot + q \text{tr}(\cdot) \frac{1}{d} \mathbb{I}_d \quad (3.130)$$

with  $q = (1-f)/(1-d)$  where  $f = \langle \gamma | \tau^{\mathcal{N}} | \gamma \rangle$ .

## Chapter 4

# Quantum sensing and imaging

### 4.1 Joint measurement of time-frequency entanglement via sum frequency generation

Lemma 4.1.1.

$$a = b \tag{4.1}$$

### 4.2 Quantum and non-local effects offer over 40 dB noise resilience advantage towards quantum lidar