

UPPSALA UNIVERSITY

QUANTUM INFORMATION

---

# Lecture Notes

---

*Author:*  
Louis HENKEL

April 19, 2023



# Contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
1.1	Quantum Theory . . . . .	5
1.2	Qubits . . . . .	5
<b>2</b>	<b>Quantum Mechanics</b>	<b>7</b>
2.1	Density operator . . . . .	7
2.1.1	Properties . . . . .	8
2.2	Mixing theorem . . . . .	9
2.3	Composite Systems . . . . .	9
2.3.1	Bipartite case . . . . .	10
2.4	Reduced density operator, partial trace . . . . .	12
2.5	Completely positive maps (quantum channels) . . . . .	12
2.5.1	Stinespring dilation . . . . .	15
2.6	Application of the CPM formalism: . . . . .	16
2.6.1	Measurement . . . . .	16
2.6.2	Lindblad equation . . . . .	18
<b>3</b>	<b>Quantum entanglement and cloning</b>	<b>21</b>
3.1	Quantum entanglement . . . . .	21
3.1.1	Entanglement detection . . . . .	22
3.1.2	Quantifying entanglement . . . . .	23
3.1.3	Generalization to mixed states (Wootters, PRL 1998) . . . . .	24
3.1.4	Multipartite entanglement . . . . .	24
3.2	Quantum teleportation . . . . .	25
3.3	Entanglement of formation . . . . .	26
3.3.1	Entanglement of formation of a mixed bipartite state . . . . .	29
3.4	Bell's inequality . . . . .	29
3.5	Ekert protocol (E91) . . . . .	30

<b>A Exercises</b>	<b>31</b>
A.1 Qubit . . . . .	31
A.2 Quantum ensemble: Density operator . . . . .	31
A.3 Composite system . . . . .	31
A.4 Completely positive maps . . . . .	31
A.5 Lindblad equation . . . . .	34
A.6 Measurements . . . . .	35
A.7 Quantum Entanglement . . . . .	35
A.8 Detecting quantum entanglement . . . . .	35
A.9 Quantifying quantum entanglement . . . . .	35
A.10 Quantum teleportation . . . . .	35
A.11 Bell's inequality . . . . .	35
A.12 Quantum copying . . . . .	35
A.13 von Neumann and relative entropy . . . . .	35

# Chapter 1

## Introduction

### 1.1 Quantum Theory

One can say, that quantum theory is a probability theory where events are associated with complex numbers  $\alpha$  called probability amplitudes. There are three rules for these probability amplitudes:

- (a) Born rule:  $P = |\alpha|^2$  gives the probability of the event  $\alpha$
- (b) For a sequence of events with amplitude  $\alpha_1, \dots, \alpha_n$ , then the amplitude of the whole sequence is:  $\prod_{i=1}^n \alpha_{N-i+1}$
- (c) For two interconnected events with amplitude  $\alpha_1$  and  $\alpha_2$ , then the probability of one event occurring if the other has occurred, then the amplitude of this event is  $\alpha = \alpha_1 + \alpha_2$ . The probability of such event is given by:

$$P = |\alpha_1|^2 + |\alpha_2|^2 + 2 \operatorname{Re}(\alpha_1^* \alpha_2) \quad (1.1)$$

where the mixed term is called the interference term. This is where the difference between classical information and quantum information theory lies.

### 1.2 Qubits

A qubit is a quantum mechanical system that can be described as a two dimensional Hilbert space. In general, this can be the polarisation of a photon,

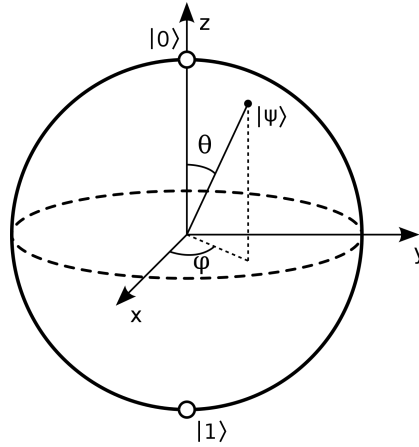
spin of an electron, of a neutron and so on. We can view a qubit as an abstract sense as  $\mathcal{H} = \text{span}\{|0\rangle, |1\rangle\}$ . An arbitrary qubit state as  $\alpha_0|0\rangle + \alpha_1|1\rangle$  with  $\alpha_i \in \mathbb{C}$ , with the normalisation condition  $|\alpha_0|^2 + |\alpha_1|^2 = 1$ . From the normalisation we can write the probability amplitudes as

$$\begin{cases} \alpha_0 = \cos \theta/2 e^{i\varphi_0} \\ \alpha_1 = \sin \theta/2 e^{i\varphi_1} \end{cases} \quad (1.2)$$

This allows us to write a general state  $|\phi\rangle$  as: #

$$\begin{aligned} |\phi\rangle &= \cos \theta/2 e^{i\varphi_0} |0\rangle + \sin \theta/2 e^{i\varphi_1} |1\rangle \\ &= e^{i\varphi_0} (\cos \theta/2 |0\rangle + \sin \theta/2 e^{i(\varphi_1 - \varphi_0)} |1\rangle) \\ &\sim \cos \theta/2 |0\rangle + \sin \theta/2 e^{i\varphi} |1\rangle \end{aligned}$$

This can be represented in a sphere called the Bloch sphere



**Fig.1.1.** Representation of a Bloch sphere

# Chapter 2

## Quantum Mechanics

### 2.1 Density operator

Suppose we have a preparation of quantum states (such as sending photons through a polariser), that are not perfect with some impurity. Say that each possible *pure* state  $|\Psi_1\rangle, \dots |\Psi_K\rangle$  with probabilities  $P_1, \dots P_K$ . Suppose we measure an observable  $A$  through the operator  $\hat{A}$  on this set of states, and we want to calculate the expectation value of this observable:

$$A_{\text{av}} = \langle \hat{A} \rangle_{\{P_k, |\Psi_k\rangle\}} = \sum_{k=1}^K P_k \langle \Psi_k | \hat{A} | \Psi_k \rangle \quad (2.1)$$

where this  $K \in \mathbb{N} \cup \{\infty\}$  *does not have to be* the same as dimension as the Hilbert space of the system. We can rewrite the equation 2.1 as:

$$\begin{aligned}
A_{\text{av}} &= \sum_{k=1}^K P_k \langle \Psi_k | \hat{A} | \Psi_k \rangle \\
&= \sum_k \sum_n P_k \langle \Psi_k | n \rangle \langle n | \hat{A} | \Psi_k \rangle \\
&= \sum_k \sum_n P_k \langle n | \hat{A} | \Psi_k \rangle \langle \Psi_k | n \rangle \\
&= \sum_k p_k \text{Tr}(\hat{A} | \Psi_k \rangle \langle \Psi_k |) \\
&= \text{Tr} \left( \hat{A} \sum_k p_k | \Psi_k \rangle \langle \Psi_k | \right) \\
&= \text{Tr}(\hat{A} \hat{\rho})
\end{aligned}$$

We define  $\hat{\rho} := \sum_k p_k | \Psi_k \rangle \langle \Psi_k |$  as the density operator representing the ensemble  $\{p_k, | \Psi_k \rangle\}$

### 2.1.1 Properties

- a) The density operator is a hermitian semi-definit operator:  $\langle \hat{\rho} \rangle \geq 0$ .

**Proof:.**

$$\langle \Psi | \hat{\rho} | \Psi \rangle = \sum_k p_k |\langle \Psi | k \rangle|^2 \geq 0 \forall \Psi \in \mathcal{H}$$

- b)  $\text{Tr} \hat{\rho} = 1$

- c)  $\hat{\rho}^2 \leq \hat{\rho}$  and  $\hat{\rho}^2 = \hat{\rho} \iff \hat{\rho} = | \Psi_1 \rangle \langle \Psi_1 |$  called a pure state.

**Example. Qubit density operator:** In diagonal (spectral) form, we can write the density operator as:

$$\hat{\rho} = p_0 | \Psi_0 \rangle \langle \Psi_0 | + p_1 | \Psi_1 \rangle \langle \Psi_1 |$$



where  $\langle \Psi_0 | \Psi_1 \rangle = 0$  and we can define the states  $\Psi_0, \Psi_1$  as:

$$\begin{aligned}\Psi_0 &= \cos \theta/2 |0\rangle + \sin \theta/2 e^{i\varphi} |1\rangle \\ \Psi_1 &= -\sin \theta/2 e^{-i\varphi} |0\rangle + \cos \theta/2 |1\rangle\end{aligned}$$

with  $p_0 + p_1 = 1$ , so we can write these as:  $p_0 = \frac{1+r}{2}$ ,  $p_1 = \frac{1-r}{2}$ , so we can write the density operator as:

$$\hat{\rho} = \frac{1}{2} \left( \hat{I} + \vec{r} \cdot \vec{\sigma} \right) \quad (2.2)$$

where  $\vec{r}(\sin \theta \cos \varphi, \sin \theta \sin \varphi, \cos \theta)$  is a 3D-vector and  $\sigma$  are the Pauli operators, and represent a point in the Bloch ball. For  $r = 0$ , the density operator is the identity operator and we have the maximal mixed state.

## 2.2 Mixing theorem

It was formulated by Hughstom et al. in PLA (1993)

Consider  $\hat{\rho} = \sum_{k=1}^{\dim(\mathcal{H})} p_k |e_k\rangle \langle e_k|$ , where  $\langle e_k | e_\ell \rangle = \delta_{k,\ell}$  and  $\hat{\eta} = \sum_{\ell=1}^L q_\ell |\phi_\ell\rangle \langle \phi_\ell|$ . Then  $\hat{\rho} = \hat{\eta}$  iff there exists an unitary matrix  $V \in \text{Mat}(\dim(\mathcal{L}) \times \dim(\mathcal{L}))$  such that

$$\sqrt{q_\ell} |\phi_\ell\rangle = \sum_{k=1}^{\dim \mathcal{H}} \sqrt{p_k} |e_k\rangle V_{kl} \forall l = 1, \dots, \dim \mathcal{H} \quad (2.3)$$

## 2.3 Composite Systems

In quantum mechanics we use tennsor products to describe states of composite systems. Assume me have systems a, b and c with bases, then the wave function of such a composite system can be written as:

$$|\Psi_{ABC}\rangle = \sum_{k\ell m} a_{k\ell m} |a_k\rangle \otimes |b_\ell\rangle \otimes |c_m\rangle \quad (2.4)$$

where the dimension of the Hilbert space is given by

$$\dim \mathcal{H}_{ABC} = \dim \mathcal{H}_A \cdot \mathcal{H}_B \cdot \mathcal{H}_C \quad (2.5)$$

is the number of combinations of basis vectors of the subsystems. As a notation we usually write

$$|a_k\rangle \otimes |b_\ell\rangle \otimes |c_m\rangle \longrightarrow |a_k b_\ell c_m\rangle \quad (2.6)$$

As terminology: With  $N$  subsystems, we mean a  $N$  particle composite system.

Assume we have system of  $N$  qubits, then the dimension of the composite system

$$\mathcal{H}_{2D}^{\otimes N} = \bigotimes_{i=1}^N \mathcal{H}_{2D}$$

with dimension

$$\dim \mathcal{H}_{2D}^{\otimes N} = 2^N \quad (2.7)$$

we can write the basis as binary strings  $x \in \{0,1\}^N$  of length  $N$  that generate the Hilbert space. A general wave function can then be written as

$$|\Psi_{N\text{-Qubit}}\rangle = \sum_{x=1}^{2^N} c_x |x\rangle \quad (2.8)$$

### 2.3.1 Bipartite case

In the bipartite case we set  $N = 2$  with subsystems A and B, an arbitrary pure state is described by

$$|\Psi^{AB}\rangle = \sum_{k=1}^{n_A} \sum_{\ell=1}^{n_B} a_{k\ell} |k\rangle \otimes |\ell\rangle \quad (2.9)$$

with  $n_i = \dim \mathcal{H}_i$ .

**Theorem.** It states, that:

$$|\Psi^{AB}\rangle = \sum_{m=1}^{\min\{n_A, n_B\}} \sqrt{d_m} |A_m\rangle \otimes |B_m\rangle \quad (2.10)$$

where  $|A_m\rangle \in \mathcal{H}_A$  and  $\langle A_m | A_n \rangle = \delta_{mn}$  for A and B and  $\sum_m d_m = 1$ .

For the proof we need singular value decomposition: Assume  $a \in \text{Mat}(n_A \times n_B)$  matrix. Then we can write this matrix  $a$  as

$$a = U \cdot d \cdots V$$

where  $U \in U(n_A)$ ,  $V \in U(n_B)$  unitary matrices and  $d$  a “diagonal”  $n_A \times n_B$  matrix with the singular values  $\sqrt{d_i}$  on the diagonal.

**Proof:.** We view  $a_{k\ell}$  as a  $n_A \times n_B$  matrix. Then using singular value decomposition we get

$$a_{k\ell} = \sum_{m=1}^{\min\{n_A, n_B\}} U_{km} \sqrt{d_m} V_{m\ell}$$

For a general bipartite wave function we get

$$\begin{aligned} |\Psi^{AB}\rangle &= \sum_{k=1}^{n_A} \sum_{\ell=1}^{n_B} \sum_{m=1}^{\min\{n_A, n_B\}} U_{km} \sqrt{d_m} V_{m\ell} |k\rangle \otimes |\ell\rangle \\ &= \sum_m \sqrt{d_m} \sum_k U_{km} |k\rangle \otimes \sum_\ell V_{m\ell} |l\rangle \\ &= \sum_{m=1}^{\min\{n_A, n_B\}} \sqrt{d_m} |A_m\rangle \otimes |B_m\rangle \end{aligned}$$

It remains to prove, that orthonormality of the basis.

$$\begin{aligned} \langle A_m | A_n \rangle &= \sum_{k, k'}^{n_A} U_{km}^* U_{k'n} \langle k | k' \rangle \\ &= \sum_{k=1}^{n_A} U_{mk}^\dagger U_{kn} \\ &= (U^\dagger U)_{m,n} = \delta_{m,n} \end{aligned}$$

There exists no generalisation to  $N$  partite system. If it existed it would take the form:  $\Psi^{AB \cdots X} = \sum_m \sqrt{d_m} |A_m\rangle \cdots |X_m\rangle$

**Example.** Assume we have a 3-state qubit, we can write:

$$\begin{aligned} \Psi^{ABC} &= |000\rangle + a(|011\rangle + |101\rangle + |110\rangle) \\ &= |+++ \rangle + |-- \rangle = |GHZ\rangle \end{aligned}$$

where  $|\pm\rangle = |0\rangle \pm |1\rangle$ .

In comparason a state:

$$|\Psi^{ABC}\rangle = |111\rangle + a(\dots)$$

that cannot be decomposed into a Schmidt form. A similar state is

$$|W\rangle := \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$$

that has no Schmidt decomposition.

## 2.4 Reduced denisty operator, partial trace

Assume we have a bipartite system with state  $|\Psi^{AB}\rangle$ . What does it mean to only have accoess to onu of the two subsystems, say A? What does it do operationally. Suppose we measure observable  $O_A$  an A, then using Schmidt decomposition

$$\begin{aligned} \langle \hat{O}_A \rangle_{\Psi^{AB}} &= \langle \Psi^{AB} | \hat{O}_A \otimes \hat{I}_B | \Psi^{AB} \rangle \\ &= \sum_{k\ell} \sqrt{d_k} \sqrt{d_\ell} \langle A_k | \hat{O}_A | A_\ell \rangle \langle B_k | \hat{I} | B_\ell \rangle \\ &= \sum_k d_k \langle A_k | \hat{O}_A | A_k \rangle \\ &= \text{Tr} \left( O_A \sum_k d_k |A_k\rangle \langle A_k| \right) \\ &= \text{Tr} (O_A \rho_B) \end{aligned}$$

where  $\rho_A$  is the reduced density operator in spectral form. A reduced density operator can be computed as a partial trace:

$$\rho_A = \text{Tr}_B |\Psi^{AB}\rangle \langle \Psi^{AB}| = \sum_m \langle B_m | \Psi^{AB} \rangle \langle \Psi^{AB} | B_m \rangle \quad (2.11)$$

## 2.5 Completely positive maps (quantum channels)

Within the space of all possible states (Bloch sphere for a single qubit), we can have maps between different quantum states. If we restrict ourselves to

only using unitary transformation, that pure states can only stay pure states (called *closed system*) whereas completely positive maps that can transform a system more generally.

**Definition.** A completely positive map (CMP)  $\rho \longrightarrow \mathcal{E}(\rho) \geq 0$  satisfies:

- (a)  $\text{Tr}[\mathcal{E}(\rho)]$  is the probability that  $\mathcal{E}$  happens:

$$\implies 0 \leq \text{Tr}[\mathcal{E}(\rho)] \leq 1, \quad (2.12a)$$

with  $\text{Tr}[\mathcal{E}(\rho)] = 1$  if the CPM is a completely positive trace perserving (CPTP) map.

- (b) A CMP should be linear, so that:  $\mathcal{E}(\sum_k p_k \rho_k) = \sum_k p_k \mathcal{E}(\rho_k)$ .

- (c) Let  $A, B$  be positive semi-definit operator, then the following inequality should hold

$$\mathcal{E}(A) \geq 0 \quad (\text{positivity}) \quad (2.12b)$$

and, if  $B$  is an operator that acts on a langer Hilbert space, then

$$\mathcal{E} \otimes \mathcal{I}(B) \geq 0 \quad (2.12c)$$

for *any* extension of the system (complete positivity). This conditions guaranties that remote systems cannot influence the physical nature of  $\mathcal{E}$

**Definition.** Transposition:

$$(|A\rangle\langle A^\perp|)^T = |A^\perp\rangle\langle A| \quad (2.13)$$

(partial transpostion)

**Example.** We have the state:

$$\begin{aligned}
|\Psi^{AB}\rangle &= \frac{1}{\sqrt{2}} (|01\rangle - |20\rangle) \longrightarrow \rho_{AB}^{T_A} = |\Psi^{AB}\rangle\langle\Psi^AB|^{T_A} \\
&= \frac{1}{2} (|01\rangle - |10\rangle)(\langle 01| - \langle 10|)^{T_A} \\
&= \frac{1}{2} (|01\rangle\langle 01| - |01\rangle\langle 10| - |10\rangle\langle 01| + |10\rangle\langle 10|)^{T_A} \\
&= \frac{1}{2} (|0\rangle\langle 0| \otimes |1\rangle\langle 1| - |0\rangle\langle 1| \otimes |1\rangle\langle 0| - |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 1| \otimes |0\rangle\langle 0|) \\
&= \begin{pmatrix} 0 & 0 & 0 & 1/2 \\ 0 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 0 \\ 1/2 & 0 & 0 & 0 \end{pmatrix}
\end{aligned}$$

with eigenvalues  $\{\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\}$

**Theorem.**  $\mathcal{E}$  is a CPM  $\iff \exists\{E_k\}$  such that

$$\sum_k E_k^\dagger E_k \leq \hat{1} \quad (2.14)$$

where the equality is given for CPTP maps in terms of which

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger \quad (2.15)$$

called the Kraus representation or operator sum representation and the  $E_k$  are called Kraus operators.

**Example.** “Decay of an atom” Let  $|e\rangle$  be the excited state of a atom and  $|g\rangle$  be its ground state. Then the Kraus operators are

$$\begin{cases} E_0 &= |g\rangle\langle g| + \sqrt{1-\gamma}|e\rangle\langle e| \\ E_1 &= \sqrt{\gamma}|g\rangle\langle e| \end{cases}$$

with  $\gamma \in [0, 1]$ . So

$$\begin{aligned}
 \rho &\longrightarrow E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger \\
 &= \left( |g\rangle\langle g| + \sqrt{1-\gamma} |e\rangle\langle e| \right) \rho \left( |g\rangle\langle g| + \sqrt{1-\gamma} |e\rangle\langle e| \right) + (\gamma |g\rangle\langle e|) \rho |e\rangle\langle g| \\
 &\xrightarrow{\gamma \rightarrow 1} |g\rangle\langle g| \rho |g\rangle\langle g| + |g\rangle\langle e| \rho |e\rangle\langle g| \\
 &= |g\rangle\langle g| \underbrace{(\langle g|\rho|g\rangle + \langle e|\rho|e\rangle)}_{\text{Tr } \rho = 1} \\
 &= |g\rangle\langle g|
 \end{aligned}$$

a decay with  $\gamma = 1 - e^{-\lambda t}$ .

### 2.5.1 Stine spring dilation

Assume we have a system  $s$  in an environment  $e$  and we want to determine the effect of the environment on the system with the time evolution operator  $U_{se}$ , then we can decompose the state:

$$\rho_{se} = \rho \otimes |e_0\rangle\langle e_0| \quad (2.16)$$

With a unitary map:

$$\rho_{se} \longmapsto U_{se} \rho \otimes |e_0\rangle\langle e_0| U_{se}^\dagger$$

The map of the system gives us:

$$\begin{aligned}
 \rho &\longmapsto \text{Tr}_e (U_{se} \rho_{se} U_{se}^\dagger) = \sum_{n=0}^{\dim \mathcal{H}_e - 1} \langle e_n | U_{se} \rho \otimes |e_0\rangle\langle e_0| U_{se}^\dagger | e_n \rangle \\
 &= \sum_n \langle e_n | U_{se} | e_0 \rangle \rho \langle e_0 | U_{se}^\dagger | e_n \rangle \\
 &= \sum_n E_n \rho E_n^\dagger
 \end{aligned}$$

To prove that  $(\langle e_n | U_{se} | e_0 \rangle)^\dagger = \langle e_n | U_{se}^\dagger | e_0 \rangle$  use:

$$\sum_{k\ell, pq} |s_k\rangle\langle s_\ell| (U_{se})_{k\ell, pq} \langle s_q| \langle p|$$

This is a CPTP map:

$$\begin{aligned}
\sum_n E_n^\dagger E_n &= \sum_n (\langle e_n | U_{se} | e_0 \rangle)^\dagger \langle e_n | U_{se} | e_0 \rangle \\
&= \sum_n \langle e_0 | U_{se}^\dagger | e_n \rangle \langle e_n | U_{se} | e_0 \rangle \\
&= \langle e_0 | U_{se}^\dagger U_{se} | e_0 \rangle \\
&= \hat{I}_s \langle e_0 | \hat{I}_e | e_0 \rangle = \hat{I}_s
\end{aligned}$$

One can use Stinespring dilation to prove that the Kraus representation is not unique. Using a basis transformation:  $|e_n\rangle \mapsto |f_n\rangle = \sum_m |e_m\rangle U_{mn}^\dagger$  with a unitary basis transformation  $U$ . As  $U$  only is unitary transformation should not affect the map. Kraus operators  $\{F_n = \langle f_n | U_{se} | e_0 \rangle\}$  define the same map as  $\{E_n = \langle e_n | U_{se} | e_0 \rangle\}$ , one finds

$$F_n = \sum_m U_{mn} E_m$$

## 2.6 Application of the CPM formalism:

### 2.6.1 Measurement

A generalized measurement is a CPTP map with the following interpretation:

- (i) Each measurement outcome  $m_k$  is associated with a Kraus operator  $E_k$ .
- (ii) The **Born rule**: the probability  $P(m_k|\rho)$  is given by:

$$P(m_k|\rho) = \text{Tr}(E_k^\dagger E_k \rho) \quad (2.17)$$

- (iii) Update the probability distribution (i.e. the state) usnig the following rule:

$$\rho \xrightarrow{m_k} E_k \rho E_k^\dagger \quad (2.18)$$

The special case called von Neumann or projective measurment we have  $E_k = |k\rangle\langle k|$  and the measurement with probability yields:

$$\begin{aligned}
P(m_k|\rho) &= \text{Tr}(|k\rangle\langle k| |k\rangle\langle k| \rho) \\
&= \text{Tr}(|k\rangle\langle k| \rho) \\
&= \langle k | \rho | k \rangle
\end{aligned}$$



if  $\rho = |\Psi\rangle\langle\Psi|$ , then:

$$\begin{aligned}\implies P(m_k|\rho) &= \langle k|\Psi\rangle\langle\Psi|k\rangle \\ &= |\langle k|\Psi\rangle|^2\end{aligned}$$

**Note.** The sum of the probability of all outcomes:

$$\begin{aligned}\sum_k P(m_k|\rho) &= \sum_k \text{Tr}(E_k^\dagger E_k \rho) \\ &= \text{Tr} \left( \sum_k \underbrace{E_k^\dagger E_k}_{\hat{I}} \rho \right) \\ &= \text{Tr} \rho = 1\end{aligned}$$

**Notation.** We define  $\{\Pi_k := E_k^\dagger E_k\}$  as a positive operator valued measure (POVM).

**Theorem.** Non-orthogonal states can not be distinguished in a general measurement

**Proof:.** Assume  $|\Phi\rangle$  and  $|\Psi\rangle$  are non-orthogonal and *can* be distinguished. If this is possible then there exists  $\Pi_1$  and  $\Pi_2$  such that  $\langle\Psi|\Pi_1|\Psi\rangle = 1$  and  $\langle\Phi|\Pi_2|\Phi\rangle = 1$ . Because probabilities must add up to 1, we must have  $\langle\Psi|\Pi_2|\Psi\rangle = 0$  where  $\Pi_k \geq 0$ , so  $\sqrt{\Pi_k} \geq 0$ . We get:

$$0 = \langle\Psi|\Pi_2|\Psi\rangle = \left\| \sqrt{\Pi_2}|\Psi\rangle \right\|^2$$

so  $\sqrt{\Pi_2}|\Psi\rangle = 0$  (0-vector).

We can write  $|\Phi\rangle = a|\Psi^\perp\rangle + b|\Psi\rangle$  where  $b \neq 0$  by assumption. This implies also that  $|a|^2 + |b|^2 = 1$ , so  $|a|^2 < 1$ . Thus

$$\begin{aligned}\sqrt{\Pi_2}|\Phi\rangle &= a\sqrt{\Pi_2}|\Psi^\perp\rangle + b\sqrt{\Pi_2}|\Psi\rangle \\ &= a\sqrt{\Pi_2}|\Psi^\perp\rangle\end{aligned}$$

So

$$\begin{cases} \left\| \sqrt{\Pi_2}|\Psi^\perp\rangle \right\| &= \langle\Phi|\Pi_2|\Phi\rangle = 1 \\ \left\| \sqrt{\Pi_2}|\Psi^\perp\rangle \right\| &= |a|^2 \langle\Psi^\perp|\Pi_2|\Psi^\perp\rangle \leq |a|^2 < 1 \end{cases}$$

### 2.6.2 Lindblad equation

So far we have only been looking at discrete maps through CPMs. How would the dynamics of an open system be described, from a time  $\rho_0$  to a time  $T$   $\rho_T$ . We can model such case through a series of small CPMs for timesteps  $\Delta t \rightarrow 0$ , where the environmental state is measured at each timesteps  $t_i$ , and the system always can be described as a product state. We can map the density operator as a sequence of CPM (Markovian approximation)

$$\rho \mapsto \mathcal{E}_{k\delta t, (k-1)\delta t} \circ \cdots \circ \mathcal{E}_{2\delta t, \delta t} \circ \mathcal{E}_{\delta t, 0}(\rho_0)$$

We do the simplifying assumption, that  $\mathcal{E}_{t+\delta t, \delta t} \equiv \mathcal{E}_{\delta t}$  (which implies that the Hamiltonian of the system is time independent). We consider the map

$$\begin{aligned} \rho_t \mapsto \rho_{t+\delta t} &= \sum_k E_k(\delta t) \rho_t E_k^\dagger(\delta t) \\ &= \mathcal{E}_{\delta t}(\rho_t) \\ \mathcal{E}_{\delta t} &\xrightarrow{\delta t \rightarrow 0} \mathcal{I} \end{aligned}$$

with  $\mathcal{I}$  being the identity map.

This allows us to make an ansatz:

$$E_0(\delta t) = 1 - i(H - iG)\delta t$$

With  $H$  and  $G$  hermitian operators.

$$E_{k>0}(\delta t) = \sqrt{\delta t} L_k$$

We assume that  $\mathcal{E}_{\delta t}$  is a CPTP since we do not extract information of the system during the evolution, in other words  $\text{Tr } \rho_t = 1$  for all  $t$ . This implies for our ansatz:

$$\begin{aligned} \hat{I} &= \sum_k E_k^\dagger(\delta t) E_k(\delta t) \\ &= E_0^\dagger(\delta t) E_0(\delta t) + \sum_{k=1} E_k^\dagger(\delta t) E_k(\delta t) \\ &= \hat{I} + 2G\delta t + \delta t \sum_{k=1} L_k^\dagger L_k + O(\delta t^2) \end{aligned}$$

So we get:

$$G = \frac{1}{2} \sum_{k=1} L_k^\dagger L_k \quad (2.19)$$

This gives us the Lindblad equation:

$$\begin{aligned} \frac{\rho_{t+\delta t} - \rho_t}{\delta t} &= -i[H, \rho_t] + \sum_k \left( L_k \rho_t L_k^\dagger - \frac{1}{2} \{L_k^\dagger L_k, \rho_t\} \right) \\ \delta t \longrightarrow 0 \implies \dot{\rho}_t &= -i[H, \rho_t] + \sum_k \left( L_k \rho_t L_k^\dagger - \frac{1}{2} \{L_k^\dagger L_k, \rho_t\} \right) \end{aligned} \quad (2.20)$$

where  $\{A, B\} = AB + BA$  is the anticommutator, and  $H$  should be interpreted as the Hamiltonian, thus the first term of the equation is called the “Schrödinger term”, the  $L_k$  are called Lindblad operators and the anticommutator term give non hermitian dynamics.

**Example.** Assume a qubit system with  $L = \sqrt{\gamma} \sigma_z$  with Hamiltonian  $H = \omega \sigma_z$ , would give a density operator:

$$\rho_t = \frac{1}{2}(\hat{I} + \vec{r}_t \cdot \vec{\sigma})$$

with the solution in the rotating frame.

$$\begin{aligned} \dot{\vec{r}} &= -2\gamma(x_t, y_t, 0) \\ \vec{r} &= (x_0 e^{-2\gamma t}, y_0 e^{-2\gamma t}, z_0) \end{aligned}$$

which for  $t \longrightarrow \infty$ , we end up with a state lying on the  $z$ -axis, and the exponential term in the  $x$  and  $y$  coordinates are called decoherence terms.



# Chapter 3

## Quantum entanglement and cloning

### 3.1 Quantum entanglement

In the beginning, we only talk about the bipartite case. We can divide our system into two subsystems.

**Definition.** A state  $|\Psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$  is entangled iff it cannot be written as a product state  $|\phi_A\rangle \otimes |\phi_B\rangle$

**Example.** Given a 2 qubit system

$$|\Psi_{AB}\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

with  $a, b, c, d \in \mathbb{C}$  and  $\langle \Psi_{AB} | \Psi_{AB} \rangle = 1$ . How do determine if this state can be written as a product state.

- We can put this into Schmidt form, so that:

$$|\Psi_{AB}\rangle = \sum_{k=1}^2 \sqrt{d_k} |A_k\rangle \otimes |B_k\rangle$$

then,  $|\Psi_{AB}\rangle$  is entangled iff  $d_1 \cdot d_2 \neq 0$ .

- We can compute the reduced density operator  $\rho_A = \text{Tr}_B |\Psi_{AB}\rangle \langle \Psi_{AB}| = \sum_{k=1}^2 d_k |A_k\rangle \langle A_k|$ , then if  $d_1 \cdot d_2 \neq 0$  implies  $\rho_A$  is a non-pure state. Thus, if  $\rho_A$  is non-pure, then  $|\Psi_{AB}\rangle$  is mixed and vice versa.

- In this example, there is an easy way to determine entanglement. If  $ad - bc \neq 0$ , then  $|\Psi_{AB}\rangle$  is entangled.

Let us consider a mixed state with  $\rho_{AB} \geq 0$  and  $\text{Tr } \rho_{AB} = 1$ .

$$\rho_{AB} = \rho_A \otimes \rho_B \quad \longrightarrow \quad \text{Tr}_B \rho_{AB} = \rho_A \quad \text{Tr } \rho_B = \rho_A \quad (3.1)$$

How do we determine entanglement for  $\rho_{AB}$ ?

**Idea.** Suppose we have many copies of  $\rho_A \otimes \rho_B$  and suppose that Alice and Bob can perform “coordinated” local operations  $\{p_k, \mathcal{E}_k \otimes \mathcal{F}_k\}$  leading to:

$$\begin{aligned} \rho_{AB} &= \sum_k p_k \mathcal{E}_k \otimes \mathcal{F}_k(\rho_A \otimes \rho_B) \\ &= \sum_k p_k \mathcal{E}_k(\rho_A) \otimes \mathcal{F}_k(\rho_B) \\ &= \sum_k p_k \rho_A^k \otimes \rho_B^k \end{aligned}$$

Since we only use local operations and classical communication (LOCC) starting from a product state, the output will *not* be entangled such a state is called separable.

**Definition.** A state  $\rho_{AB}$  is entangled iff it *cannot* be written in the form  $\sum_k p_k \rho_A^k \otimes \rho_B^k$ .

### 3.1.1 Entanglement detection

We are given a state  $\rho_{AB}$ , how do we determine if it is entangled or not?

**Theorem** (Horodecki family : Phy. Lett. A (1996)).  $\rho_{AB}$  is separable  $\iff$  for every “positive” map  $\mathcal{A}$  on one of the subsystems  $\mathcal{A} \otimes I_B(\rho_{AB}) \geq 0$ .

- *Useful test:* (PPT = positive partial transposition)

$$\rho^{AB} \text{ is separable} \implies (\rho^{AB})^{T_A} \geq 0 \quad (3.2)$$

The implication to the other side only holds for  $2 \otimes 2$  or  $2 \otimes 3$  systems.

### 3.1.2 Quantifying entanglement

**Definition.** We can quantifying entanglement by using a measurment function

$$\mu : \mathcal{H}_A \otimes \mathcal{H}_B \longrightarrow \mathbb{R} : \rho^{AB} \longmapsto \mu(\rho^{AB})$$

This measurement function should fulfill:

- $\mu \geq 0$
- $\mu = 0$  for separable states
- $\mu$  is be non-increasing under LOCC
- $\mu$  is invariant under local unitary operations.

There are *two* measures:

(a) *Negativity*: Based on PPT:

$$\mathcal{N}_e(\rho^{AB}) = \frac{\text{Tr} \left| (\rho^{AB})^{T_A} \right| - 1}{2} = \frac{\left\| (\rho^{AB})^{T_A} \right\| - 1}{2}$$

where  $\|\rho\| := \text{Tr} \sqrt{A^\dagger A}$

**Example.** We look at the state  $|\Psi^{AB}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$  where the eigenvalues of  $(|\Psi^{AB}\rangle\langle\Psi^{AB}|)^{T_A}$  are  $\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}$ . so the negativity is non-zero.

(b) *Concurrence*: Only works for  $2 \times 2$  systems from its definition.

Based on the univeral flip:  $\Theta(\alpha|0\rangle + \beta|1\rangle) = -\beta^*|0\rangle + \alpha^*|1\rangle$ , that is orthogonal to the initial state (such an aperation cannot be made, because we cannot make compled conjugation).

A pure state of two qubits written in Schmidt decomposition:

$$\begin{aligned} |\Psi_{AB}\rangle &= \sum_{k=0}^1 \sqrt{d_k} |A_k\rangle \otimes |B_k\rangle \\ &= \sqrt{d_0} |A_0\rangle \otimes |B_0\rangle + \sqrt{d_1} |A_1\rangle \otimes |B_1\rangle \xrightarrow{\Theta_A \otimes \Theta_B''} \\ &\longrightarrow \sqrt{d_0} |A_1\rangle \otimes |B_1\rangle + \sqrt{d_1} |A_0\rangle \otimes |B_0\rangle =: |\tilde{\Psi}_{AB}\rangle \\ &\implies \left| \langle \tilde{\Psi}_{AB} | \Psi_{AB} \rangle \right| = 2\sqrt{d_0 d_1} = 2\sqrt{d_0(1-d_0)} \leq 1 \end{aligned}$$

with equality if  $d_0 = \frac{1}{2}$ .

The concurrence  $C(\Psi_{AB})$

### 3.1.3 Generalization to mixed states (Wootters, PRL 1998)

Given a state  $\rho_{AB}$

- Qubit flip:  $\rho_{AB} \mapsto \tilde{\rho}_{AB} = \sigma_y \otimes \sigma_y \mathcal{K}(\rho_{AB}) \sigma_y \otimes \sigma_y$  where  $\mathcal{K}$  is the complex conjugation with regard to the product basis  $|00\rangle, \dots, |11\rangle$ .
- Compute the eigenvalues  $\lambda_k$  of  $\rho_{AB} \tilde{\rho}_{AB}$ .
- We compute:  $\max\{0, \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}\} = C(\rho_{AB})$ , where  $\lambda_1$  is the largest eigenvalue.

### 3.1.4 Multipartite entanglement

Say we have a  $N$ -partite state  $|\Psi^{A_1 \dots A_N}\rangle$ , then the definition of entanglement is not trivial. We can define the state as:

$$|\Psi^{A_1 \dots A_N}\rangle = \sum_{n_{A_1} \dots n_{A_N}} a_{n_{A_1} \dots n_{A_N}} |n_{A_1} \dots n_{A_N}\rangle \quad (3.3)$$

The probability amplitude coefficients  $\{a_{n_{A_1} \dots n_{A_N}}\} \mapsto \text{Polynomial}\{a_{n_{A_1} \dots n_{A_N}}\}$  that is general invariant under local transformation  $U_{A_i} \otimes \dots \otimes U_{A_N}$ .

**Example.** We can write a 2-qubit:  $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$  the polynomial is  $ad - bc$ .

**Example.** Say we have 3 qubits: Consider the states

$$\begin{aligned} |GHZ\rangle &= \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle) \\ |W\rangle &= \frac{1}{\sqrt{3}} (|001\rangle + |010\rangle + |100\rangle) \end{aligned}$$

We can write decompose these states as

$$\begin{aligned} |GHZ\rangle &= \frac{1}{\sqrt{2}} |0\rangle |00\rangle + \frac{1}{\sqrt{2}} |1\rangle |11\rangle \\ |W\rangle &= \frac{\sqrt{2}}{\sqrt{3}} |0\rangle \left( \frac{|01\rangle + |10\rangle}{\sqrt{2}} \right) + \frac{1}{\sqrt{3}} |1\rangle |00\rangle \end{aligned}$$



The traces and concurrence are

$$\begin{aligned}
\rho_{GHZ} &= \text{Tr}_3(|GHZ\rangle\langle GHZ|) \\
&= \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11| \\
C(\rho_{GHZ}) &= 0 \\
C(W) &= 2 \frac{\sqrt{2}}{\sqrt{3}} \frac{1}{\sqrt{3}} = \frac{2\sqrt{2}}{3} \neq 0 \\
\rho_W &= \text{Tr}_1 |W\rangle\langle W| \\
&= \frac{2}{3}|\Psi_+\rangle\langle \Psi_+| + \frac{1}{3}|00\rangle\langle 00| \\
C(\rho_W) &= \frac{2}{3}
\end{aligned}$$

Note:  $C^2(\rho_W) = \frac{4}{9}$  and  $C^2(W) = \frac{8}{9} = 2C^2(\rho_W)$ . We can see, that

$$\begin{aligned}
\tau_{ABC}^W &= C^2(W) - C^2(\rho_W^{AB}) - C^2(\rho_W^{AC}) = 0 \\
\tau_{ABC}^{GHZ} &= C^2(GHZ) - C^2(\rho_{GHZ}^{AB}) - C^2(\rho_{GHZ}^{AC}) = 1
\end{aligned}$$

In this example, we chose  $A$  as a reference frame. One can show, that for all tripartite states of three qubits,

$$\tau_{A|BC} = \tau_{B|AC} = \tau_{C|AB}$$

This implies that  $\tau$ , called 3-tangel or residual entanglement, is measure of *genuine* 3-qubit entanglement just as concurrence is the measure 2-qubit entanglement.  $\tau$  is a polynomial of degree 4 in the probability amplitudes.  $\tau$  is the hyperdeterminant of the  $2 \times 2 \times 2$  cube matrix.

## 3.2 Quantum teleportation

**Definition.** We define the Bell basis as

$$|\Phi_{\pm}\rangle = \frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle) \quad (3.4)$$

$$|\Psi_{\pm}\rangle = \frac{1}{\sqrt{2}} (|01\rangle \pm |10\rangle) \quad (3.5)$$

The key message from quantum teleportation is that entanglement can be used as a resource.

Assume, we have a that 2 persons, say Alice and Bob, and Alice has some state  $|\phi\rangle = a|0\rangle + b|1\rangle$ . How can Alice transfer the information on her state to Bob?

A protocol can be, that they share any maximally entangled state, say  $|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ , where each party has one qubit of this state. The total state of the system is then, rewritten in the Bell basis,

$$\begin{aligned} |\Gamma\rangle &= |\phi\rangle \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{a}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{b}{\sqrt{2}}(|100\rangle + |111\rangle) \\ &= \frac{1}{2}|\Phi_+\rangle(a|0\rangle + b|1\rangle) + \frac{1}{2}|\Phi_-\rangle(a|0\rangle - b|1\rangle) \\ &\quad + \frac{1}{2}|\Psi_+\rangle(a|1\rangle + b|0\rangle) + \frac{1}{2}|\Psi_-\rangle(a|1\rangle - b|0\rangle) \end{aligned}$$

Alice measures the Bell basis (i.o.w., she distinguished between the 4 states, above). If she obtains:

- $\Phi_+$ :  $|\Gamma\rangle \longrightarrow |\Phi_+\rangle(a|0\rangle + b|1\rangle) = |\Phi_+\rangle|\phi\rangle$
- $\Phi_-$ :  $|\Gamma\rangle \longrightarrow |\Phi_-\rangle(a|0\rangle - b|1\rangle) \xrightarrow{\sigma_z} |\Phi_-\rangle\sigma_z(a|0\rangle - b|1\rangle) = |\Phi_-\rangle|\phi\rangle$
- $\Psi_+$ :  $|\Gamma\rangle \longrightarrow |\Psi_+\rangle(a|1\rangle + b|0\rangle) \xrightarrow{\sigma_x} |\Psi_+\rangle\sigma_x(b|0\rangle + a|1\rangle) = |\Psi_+\rangle|\phi\rangle$
- $\Psi_-$ :  $|\Gamma\rangle \longrightarrow |\Psi_-\rangle(a|1\rangle - b|0\rangle) \xrightarrow{\sigma_y} |\Psi_-\rangle\sigma_y(b|0\rangle - a|1\rangle) = |\Psi_-\rangle|\phi\rangle$

### 3.3 Entanglement of formation

**Definition.** The entropy is the gain of information of an event associated to a set of probabilities  $\{p_k\}$ . The canonic way, called Shannon entropy, the entropy is given by:

$$H(\{p_k\}) = - \sum_k p_k \log p_k \quad (3.6)$$

For a quantum system, the entropy formula can be given by the von Neumann entropy for some state  $\rho = \sum_k p_k |\Psi_k\rangle\langle\Psi_k|$ . is given by:

$$S(\rho) = -\text{Tr}(\rho \log \rho) = -\sum_k \lambda_k \log \lambda_k \quad (3.7)$$

for  $\lambda_k$  the eigenvalues of  $\rho$ , and  $\log \rho = \sum_k |e_k\rangle\langle e_k| \log \lambda_k$

Consider a state:  $|\Phi_{AB}\rangle \mapsto \rho_A = \sum_{k=1}^{n_A \leq n_B} d_k |A_k\rangle\langle A_k|, \rho_B = \sum_k d_k |B_k\rangle\langle B_k|$ .  
Then

$$\begin{aligned} S(\rho_A) &= -\sum_{k=1}^{n_A} d_k \log d_k \\ S(\rho_B) &= -\sum_{k=1}^{n_B} d_k \log d_k = -\sum_{k=1}^{n_A} d_k \log d_k - 0 \log 0 \end{aligned}$$

For a product state  $|\Psi_{AB}\rangle = |A_1\rangle \otimes |B_1\rangle$ . The entropy is

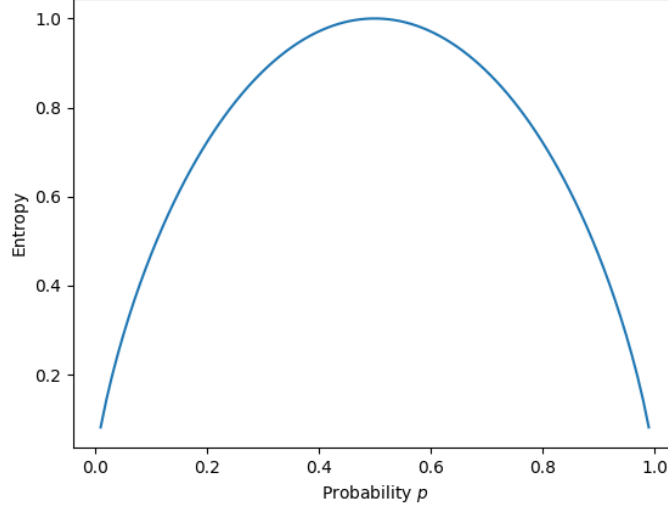
$$\rho_A = |A_1\rangle\langle A_1| \implies S(\rho_A) = -1 \log 1 - 0 \log 0 = 0$$

We get maximum entanglement for  $d_1 = \dots = d_{n_A} = \frac{1}{n}$ , and the state vector would be  $|\Psi_{AB}\rangle = \sum_k \frac{1}{\sqrt{d}} |A_k\rangle \otimes |B_k\rangle$ , with entropy

$$S(\rho_A) = -\sum_{k=1}^{n_A} \frac{1}{n_k} \log \frac{1}{n_k} = -n_A \cdot \frac{1}{n_A} \log \frac{1}{n_A} = \log n_A$$

**Example.** Say we have two qubits, chose  $\log = \log_2$ , then for any state  $\rho_A$ , we have  $0 \leq S(\rho_A) \leq 1$ . The entropy is given by:

$$S(\rho_A) = -\lambda_0 \log \lambda_0 - \lambda_1 \log \lambda_1 = -\lambda_0 \log \lambda_0 - (1 - \lambda_0) \log(1 - \lambda_0) =: h(\lambda_0)$$

**Fig.3.1.** Plot of the thing

It can be show, that

$$h(\lambda_0) = h\left(\frac{1 + \sqrt{1 - C(\Psi_{AB})^2}}{2}\right) \quad (3.8)$$

The concurrence is given by:

$$\begin{aligned} C(\Psi_{AB}) &= 2\sqrt{\lambda_0\lambda_1} = 2\sqrt{\lambda_0(1 - \lambda_0)} \\ C^2 &= 4\lambda_0 - 4\lambda_0^2 \\ \lambda_0 &= \frac{1}{2} \pm \sqrt{\frac{1}{4} - \frac{C^2}{4}} \end{aligned}$$

And the entropy is related to:

$$E_F(\Psi_{AB}) \equiv S(\rho_A) = h\left(\frac{1 + \sqrt{1 - C^2(\Psi_{AB})}}{2}\right) \quad (3.9)$$

### 3.3.1 Entanglement of formation of a mixed bipartite state

**Definition.** For the density operator  $\rho_{AB} = \sum_k p_k |\Psi_{AB}^k\rangle\langle\Psi_{AB}^k|$ , the entropy is defined as

$$E_F(\rho_{AB}) = \min_{\{p_k|\Psi_{AB}^k\rangle\}} \sum_k p_k \delta(p_A^k) = \sum_k \text{Tr}_B(|\Psi_{AB}^k\rangle\langle\Psi_{AB}^k|) \quad (3.10)$$

For two qubits. we know  $E_F(\rho_{AB}) = h\left(\frac{1+\sqrt{1-C(\Psi_{AB})^2}}{2}\right)$ , and

$$\begin{aligned} \rho_{AB} &\longrightarrow \tilde{\rho}_{AB} = \sigma_y \otimes \sigma_y \rho_{AB}^* \sigma_y \otimes \sigma_y \\ &\longrightarrow \rho_{AB} \tilde{\rho}_{AB} \\ &\longrightarrow \lambda_1 \leq \lambda_2 \leq \lambda_3 \leq \lambda_4 \\ &C \end{aligned}$$

## 3.4 Bell's inequality

Or CHSH (standing for John Clauser, Michael Horne, Abner Shimony, and Richard Holt): We need four measurements with outcomes  $a, a', b, b' = \pm 1$ . We then construct the measurement:

$$a(b + b') + a'(b - b') = \pm 2 \quad (3.11)$$

Averaging leads to the following inequality:

$$-2 \leq \langle a(b + b') + a'(b - b') \rangle \leq 2$$

which leads to:

$$|\langle a(b + b') + a'(b - b') \rangle| \leq 2$$

This is the CHSH inequality for a classical form. For quantum mechanics, we need a source, sending out entangled qubits, where each have a certain measurement angle. Assume, that the state of the qubits is initiality:

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \implies \langle \Psi_- | \vec{a} \vec{\sigma} \otimes \vec{b} \vec{\sigma} | \Psi_- \rangle = -\vec{a} \cdot \vec{b}$$

We want to calculate for the right angles:

$$\begin{aligned}
 B_{CHSH} &= \left| \vec{a} \cdot \vec{b} + \vec{a} \cdot \vec{b}' + \vec{a}' \cdot \vec{b} - \vec{a}' \cdot \vec{b}' \right| \\
 &= \cos \frac{\pi}{4} + \cos \frac{\pi}{4} + \cos \frac{\pi}{4} - \cos \frac{3\pi}{4} \\
 &= \frac{4}{\sqrt{2}} = 2\sqrt{2} > 2
 \end{aligned}$$

The Werner state

$$\rho_{\text{Werner}} = \frac{1-p}{4} \hat{1} \otimes \hat{1} + p |\Psi_{-}\rangle \langle \Psi_{-}| \quad (3.12)$$

The Concurrence of this state:  $C(\rho_{\text{Werner}}) \neq 0$ , if  $p > \frac{1}{3}$ , but the CHSH is only broken for  $p > \frac{1}{\sqrt{2}}$ , which shows that entanglement is not the same as breaking locality

### 3.5 Ekert protocol (E91)

Published on 1991. This is a key distribution: Alice and Bob want to share a secret key. Alice and Bob share a pair of entangled qubit. They chose 3 measuring direction, where 2 pairs are equal. They announce each in which order they will measure. They look at the states pairs using the first two direction, they are used to check if CHSH, if it is broken, they know, that the set of pairs, where they have measured in the same direction are secure. If CHSH is not broken, then the key cannot be trusted.

# Appendix A

## Exercices

### A.1 Qubit

### A.2 Quantum ensemble: Density operator

### A.3 Composite system

### A.4 Completely positive maps

18.

- (a) The phase damping completely positive map:  $\mathcal{E}(\rho) = (1-p)\rho + p\sigma_z\rho\sigma_z$  for  $p \in [0, 1]$ . The Kraus operators are

$$\begin{cases} E_0 &= \sqrt{1-p}\hat{I} \\ E_1 &= \sqrt{p}\hat{\sigma}_z \end{cases}$$

- (b) The bit flip map  $\mathcal{E}(\rho) = (1-p)\rho + p\sigma_x\rho\sigma_x$  for  $p \in [0, 1]$ . The Kraus operators are

$$\begin{cases} E_0 &= \sqrt{1-p}\hat{I} \\ E_1 &= \sqrt{p}\hat{\sigma}_x \end{cases}$$

- (c) The phase shift and bit shift map  $\mathcal{E}(\rho) = (1-p)\rho + p\sigma_y\rho\sigma_y$  for  $p \in [0, 1]$ .

The Kraus operators are

$$\begin{cases} E_0 &= \sqrt{1-p}\hat{I} \\ E_1 &= \sqrt{p}\hat{\sigma}_y \end{cases}$$

22. Consider a two level atom with ground state  $|g\rangle$  and excited state  $|e\rangle$ . The atom is placed in a cavity, which includes decay of an atom modeled by the unitary transformation

$$\begin{aligned} |e\rangle \otimes |n\rangle &\mapsto \sqrt{1-p}|e\rangle \otimes |n\rangle + \sqrt{p}|g\rangle \otimes |n+1\rangle \\ |g\rangle \otimes |n\rangle &\mapsto |g\rangle \otimes |n\rangle \end{aligned}$$

where  $|n\rangle$  and  $|n+1\rangle$  are the states of the quantised field corresponding to the  $n$  and  $n+1$  photons in the cavity. Suppose the atom+cavity field start in the pure states

$$|\Psi\rangle = (\cos \theta/2 |g\rangle + \sin \theta/2 |e\rangle) \otimes |n\rangle$$

and undergoes a decay. Compute the average number of photons in the cavity as a function of the decay probability  $p$ .

The expectation value is  $\langle N \rangle = \langle a^\dagger a \rangle = \text{Tr}(\mathcal{E}(\rho_\gamma)N)$ . The density of the composite system is:

$$\rho_{a\gamma} = |\Psi\rangle\langle\Psi| = |\Psi_0\rangle\langle\Psi_0| \otimes |n\rangle\langle n| \quad (\text{A.1})$$

Now applying the positivity map and calculate the partial trace.

$$\begin{aligned} \mathcal{E}(\rho_{a\gamma}) &= [\mathcal{E}(|\Psi\rangle)] [\mathcal{E}(|\Psi\rangle)]^\dagger \\ &= \text{Tr}_a(\mathcal{E}(\rho_{a\gamma})) = \dots \end{aligned}$$

An alternative: From the lecture, we know, that a composite system evolves as  $\rho_{se} \longrightarrow U_{se}\rho_{se}U_{se}^\dagger$ , then the system has a Kraus decomposition

$$\rho \longrightarrow \sum E_n \rho E_n^\dagger$$

where  $E_n = \langle E_n | U_{se} | E_0 \rangle$  with  $E_n$  an orthogonal basis for the environment. On our atom system, we need to determine the basis for the composite system



$\{|g\rangle|0\rangle, |g\rangle|1\rangle, \dots, |g\rangle|n\rangle, \dots, |e\rangle|0\rangle, \dots, |e\rangle|n\rangle, \dots\}$ . As a matrix, the time evolution operator looks like:

$$U = \begin{pmatrix} 1 & & & 0 & & \\ & 1 & & \sqrt{p} & \ddots & \\ & & \ddots & & \ddots & \\ & & & 1 & & 0 \\ & & & & \ddots & \sqrt{p} \\ & & & & & \sqrt{1-p} \\ & & & & & & \ddots \\ & & & & & & & \sqrt{1-p} \\ & & & & & & & & \ddots \end{pmatrix} = \begin{pmatrix} I & B \\ 0 & C \end{pmatrix}$$

We can calculate the Kraus coefficients:

$$\begin{cases} E_g &= \langle g|U_{ac}|\Psi_0\rangle \\ E_e &= \langle e|U_{ac}|\Psi_0\rangle \end{cases}$$

with  $|\Phi_0\rangle = \cos \theta/2 |g\rangle + \sin \theta/2 |e\rangle$  and get:

$$\begin{aligned} E_g &= \cos \theta/2 \langle g|U_{ac}|g\rangle + \sin \theta/2 \langle g|U_{ac}|e\rangle \\ &= \cos \theta/2 I + \sin \theta/2 B \\ E_e &= \cos \theta/2 \langle e|U_{ac}|g\rangle + \sin \theta/2 \langle e|U_{ac}|e\rangle \\ &= \sin \theta/2 C \end{aligned}$$

So we get:

$$\begin{aligned} \mathcal{E}(\rho) &= \mathcal{E}(|n\rangle\langle n|) \\ &= E_g |n\rangle\langle n| E_g^\dagger + E_e |n\rangle\langle n| E_e^\dagger \\ &= \cos^2 \theta/2 |n\rangle\langle n| + \cos \theta/2 \sin \theta/2 (|n\rangle\langle n| B^\dagger + B |n\rangle\langle n|) \\ &\quad + \sin^2 \theta/2 B |n\rangle\langle n| B^\dagger + \sin^2 \theta/2 \sin C |n\rangle\langle n| C^\dagger \\ &= [\cos^2 \theta/2 + (1-p) \sin^2 \theta/2] |n\rangle\langle n| + p \sin^2 \theta/2 |n+1\rangle\langle n+1| \\ &\quad + \sqrt{p} \sin \theta/2 \cos \theta/2 [|n\rangle\langle n+1| + |n+1\rangle\langle n|] \end{aligned}$$

We can now calculate the expectation value of  $N$  with  $N|n\rangle = a^\dagger a|n\rangle = n|n\rangle$

$$\begin{aligned}\langle N \rangle &= \text{Tr}(\mathcal{E}(\rho_c)N) \\ &= n [\cos^2 \theta/2 + (1-p) \sin^2 \theta/2] + (n+1)p \sin^2 \theta/2 \\ &= n + p \sin^2 \theta/2\end{aligned}$$

## A.5 Lindblad equation

26. Let  $H$  be the Hamiltonian:

$$H = \sum E_k |\Phi_k\rangle\langle\Phi_k|$$

with an error  $L = \sqrt{\gamma}H$ . Let  $\rho(t)$  be the state of the system at time  $t$ , then:

$$\dot{\rho}(t) = -i[H, \rho] + \sum \left( L_n \rho L_n^\dagger - \frac{1}{2} \{L_n^\dagger L_n, \rho\} \right)$$

We want to show, that it reduced to

$$\dot{\rho}(t) = -[H, \rho] - \frac{\gamma}{2} [H, [H, \rho]]$$

We only need to show, that:

$$\begin{aligned}L\rho L^\dagger - \frac{1}{2}\{LL^\dagger, \rho\} &= \gamma \left( H\rho H - \frac{1}{2}(H^2\rho + \rho H^2) \right) \\ -\gamma[H, [H, \rho]] &= -\gamma(H, H\rho - \rho H) \\ &= -\gamma(H^2\rho - H\rho H - H\rho H + \rho H^2) \\ &= \frac{\gamma}{2} \left( H\rho H - \frac{1}{2}(H^2\rho + H^2\rho) \right)\end{aligned}$$

This is the damping equation used in magnetism. We can write the density operator as

$$\rho = \sum_{\ell k} \rho_{k\ell}(t) |\Phi_k\rangle\langle\Phi_\ell|$$

that, because of linearity, we only need to solve them for one of the  $\rho_{k\ell}$

$$\begin{aligned}\dot{\rho}_{k\ell}(t) &= -\rho_{k\ell}[H, |\Phi_k\rangle\langle\Phi_\ell|] - \frac{\gamma}{2} \rho_{k\ell}[H, [H, |\Phi_k\rangle\langle\Phi_\ell|]] \\ &= \rho_{k\ell}(t) \left( -i(E_k - E_\ell) - \frac{\gamma}{2}(E_k - E_\ell)^2 \right) |\Phi_k\rangle\langle\Phi_\ell|\end{aligned}$$

And we get

$$\rho_{k\ell}(t)e^{t(-i(E_k-E_\ell))}e^{-\frac{\gamma t}{2}(E_k-E_\ell)^2}$$

For  $\gamma t \rightarrow \infty$ ,  $\rho_{k\ell}$  goes to 0.

## A.6 Measurements

### A.7 Quantum Entanglement

### A.8 Detecting quantum entanglement

### A.9 Quantifying quantum entanglement

### A.10 Quantum teleportation

### A.11 Bell's inequality

### A.12 Quantum copying

### A.13 von Neumann and relative entropy