1. Some basics from quantum theory

two key elements: • information encoded in states
• information processing: operations (unitary and non-unitary)

1.1 quantum states

• pure states elements of Hilbertspace $\mathcal{H}$ & scalar product

(4) $$\langle \psi | \phi \rangle \in \mathbb{C}$$

norm

(5) $$\| |\psi\rangle \| = \langle \psi | \psi \rangle^{1/2}$$

most elementary Hilbertspace $\mathbb{C}^2$ basis $\{|0\rangle, |1\rangle\}$

(6) $$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \qquad |\alpha|^2 + |\beta|^2 = 1$$

• mixed states if knowledge about quantum system is incomplete $\Rightarrow$ probability p_i to be in state $|\psi_i\rangle$ ($|\psi_i\rangle$ ONB)

(7) $$|\phi\rangle \overset{?}{=} p_1 |\psi_1\rangle + p_2 |\psi_2\rangle \qquad \text{No!}$$

else

$$\langle \hat{A} \rangle = \left(p_1 \langle \psi_1 | + p_2 \langle \psi_2 | \right) \hat{A} \left(p_1 |\psi_1\rangle + p_2 |\psi_2\rangle \right)$$

(8) $$= p_1^2 \langle \psi_1 | \hat{A} | \psi_1 \rangle + p_2^2 \langle \psi_2 | \hat{A} | \psi_2 \rangle + p_1 p_2 \left(\langle \psi_1 | \hat{A} | \psi_2 \rangle + \langle \psi_2 | \hat{A} | \psi_1 \rangle \right)$$

$$\neq p_1 \langle \psi_1 | \hat{A} | \psi_1 \rangle + p_2 \langle \psi_2 | \hat{A} | \psi_2 \rangle$$

which it should be!

It holds for $\dim(\mathcal{H}) = d$

$$\langle \hat{A} \rangle = \langle \phi | \hat{A} | \phi \rangle = \sum_{i=1}^{d} \langle \phi | \hat{A} | \psi_i \rangle \langle \psi_i | \phi \rangle$$

(9) $$= \sum_{i=1}^{d} \langle \psi_i | \phi \rangle \langle \phi | \hat{A} | \psi_i \rangle = Tr\{ |\phi\rangle\langle\phi| \hat{A} \}$$

Here $|\psi\rangle\langle\psi|$ is a projector to the pure state $|\phi\rangle$.

$\Rightarrow$ Instead of (7) we should use a weighted sum of orthogonal projectors

density operator

(10) $$|\phi\rangle\langle\phi| \longrightarrow \sum_{i=1}^{d} p_i |\psi_i\rangle\langle\psi_i| = \varrho$$

properties of $\hat{\varrho}$ (partial list)

- ϱ, ϱ^+ defined on whole $\mathcal{H}$
  $\varrho = \varrho^+$ i.e. ϱ is selfadjoint
- ϱ is semi-positiv definit i.e. eigenvalues ≥ 0
- $Tr\{\varrho\} = \sum_i \lambda_i = 1$ λ_i are probabilities

The set $S(\mathcal{H})$ of all density operators is called state space, $S(\mathcal{H})$ is convex, i.e. if $\varrho_1, \varrho_2 \in S(\mathcal{H})$ and λ real with $0 \leq \lambda \leq 1$, then

(11) $$\lambda \varrho_1 + (1-\lambda)\varrho_2 \in S(\mathcal{H})$$

pure states are projectors i.e. for $\rho = |\phi\rangle\langle\phi|$

(12) $$\rho^2 = \rho$$

Every mixed state ρ can be written in the form

(13) $$\rho = \sum_{i=1}^{d} p_i |\psi_i\rangle\langle\psi_i| \qquad 0 \le p_i \le 1, \quad \sum p_i = 1$$

where $\{|\psi_i\rangle\}$ is a ONB. The p_i can be interpreted as probabilities to find the system in state $|\psi_i\rangle$.
(13) is unique if all p_i are different i.e. if ρ has a non-degenerate spectrum and the states $|\psi_i\rangle$ are an ONB

- <u>pure two-partite states</u>

In quantum information science two-partite systems play an important role

(14) $$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \qquad A \mathrel{\hat{=}} \text{"Alice"}, \quad B \mathrel{\hat{=}} \text{"Bob"}$$

Pure states which can be represented in the form

(15) $$|\psi\rangle = |\phi\rangle_A \otimes |\phi'\rangle_B$$

are called <u>product states</u>, <u>separabel states</u> or <u>factorizable</u>
If such a representation does not exist, the state is called <u>entangled</u>

Schmidt theorem: Let $\dim(\mathcal{H}_A) = N$ and $\dim(\mathcal{H}_B) = M$ with $N \leq M$. Then there exist for every state $|\psi\rangle$ a decomposition into ONB $\{|i\rangle_A\}$ and $\{|i\rangle_B\}$ of the following form:

(16) $$|\psi\rangle = \sum_{i=1}^{N} c_i \, |i\rangle_A |i\rangle_B \qquad c_i \geq 0$$

proof: $$|\psi\rangle = \sum_{i=1}^{N} \sum_{j=1}^{M} \alpha_{ij} \, |i\rangle_A |j\rangle_B$$

Let (17) $$\sum_{j=1}^{M} \alpha_{ij} |j\rangle_B \equiv |\tilde{i}\rangle_B$$

$\{|\tilde{i}\rangle_B\}$ $i = 1, .., N$ is a non-normalized, non-orthogonal set of states in $\mathcal{H}_B$. These states can be orthonormalized by the Schmidt algorithm

(i) $$|1\rangle_B = \frac{1}{\sqrt{\sum_{j=1}^{M} |\alpha_{ij}|^2}} \sum_{j=1}^{M} \alpha_{1j} |j\rangle_B$$

orthogonalization

(ii) $$|2\rangle'_B = |\tilde{2}\rangle_B - {}_B\langle 1|\tilde{2}\rangle_B \, |1\rangle_B \Rightarrow {}_B\langle 2'|1\rangle_B = 0$$

(iii) $$|2\rangle_B = \frac{1}{\sqrt{{}_B\langle 2'|2'\rangle_B}} |2'\rangle_B$$ normalization

etc.

$$\Rightarrow |\psi\rangle = \sum_{i=1}^{N} c_i \, |i\rangle_A |i\rangle_B$$

The number of non-vanishing coefficients c_i is called Schmidt number s. Any pure bi-partite state with $s > 1$ is entangled. The ordered set of coefficients

$$C_1 \geq C_2 \geq C_3 \geq \cdots \geq C_s$$

is called the Schmidt spectrum.

In contrast to pure states the definition and calculable criteria for entanglement of mixed states is much more involved as we will see later.

1.2 Operations

In Quantum theory two classes of operations:

- unitary evolution
- measurements (with sub classes)

- unitary evolution (dynamical map)

(18) $$\varrho(0) \longrightarrow \varrho(t) = U(t)\,\varrho(0)\,U^{+}(t)$$

maps pure states to pure states

$$\varrho^2(0) = \varrho(0) \quad \Rightarrow \quad \varrho^2(t) = U\varrho(0)U^{+}U\varrho(0)U^{+}$$
$$= U\varrho(0)^2U^{+} = U\varrho(0)U^{+} = \varrho(t)$$

- projective measurement

Let $i = 1, 2, \ldots, k$ be an index that characterizes the outcome of a measurement of a certain observable. The measurement outcomes are the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_k$. $\hat{\Pi}_i$ is the projector to the subspace of eigenstates $\{|\lambda_i^e\rangle\}$ corresponding to λ_i. If λ_i is <u>non-degenerate</u> then $\hat{\pi}_i$ is one dimensional

$$(20) \qquad \hat{\pi}_i = |\lambda_i\rangle\langle\lambda_i|$$

If λ_i is <u>degenerate</u> with degree d then $\hat{\pi}_i$ is a d-dimensional projector, but in any case

$$(21) \qquad \hat{\pi}_i \hat{\pi}_j = \delta_{ij}\, \hat{\pi}_i \qquad \sum_{i=1}^{k} \hat{\pi}_i \equiv \mathbb{1}$$

One distinguishes <u>selective projective measurements</u>

$$(22) \qquad \rho \rightarrow \rho' = \frac{\hat{\pi}_i \rho \hat{\pi}_i}{Tr\{\hat{\pi}_i \rho \hat{\pi}_i\}}$$

and <u>non-selective measurements</u> (measurement is done but the result got lost)

$$(23) \qquad \rho \rightarrow \rho' = \sum_{i=1}^{k} \hat{\pi}_i \rho \hat{\pi}_i$$

remark: $Tr\{\rho'\}=1$

$$Tr\{\sum_{i=1}^{k} \hat{\pi}_i \rho \hat{\pi}_i\} = \sum_{i=1}^{K} Tr\{\hat{\pi}_i \rho \hat{\pi}_i\} = \sum_{i=1}^{k} Tr\{\hat{\pi}_i^2 \rho\}$$

$$= \sum_{i=1}^{k} Tr\{\hat{\pi}_i \rho\} = Tr\{\sum_{i=1}^{k} \hat{\pi}_i \rho\} = Tr\{\mathbb{1}\cdot\rho\} = 1$$

The probability of an outcome λ_i in a selective measurement is

(24) $$p_i = Tr\{\hat{\pi}_i \rho \hat{\pi}_i\} = Tr\{\hat{\pi}_i \rho\}$$

In the non-degenerate case $\hat{\pi}_i = |\lambda_i\rangle\langle\lambda_i|$

(25) $$p_i = Tr\{|\lambda_i\rangle\langle\lambda_i|\rho\} = \langle\lambda_i|\rho|\lambda_i\rangle$$

If all projectors $\hat{\pi}_i$ are one-dimensional the measurement is called complete. After a complete measurement the system is always in a pure state. An incomplete measurement can leave the system in a mixed state even if the initial state was pure.

- extension by an ancilla

$\rho \in S(\mathcal{H}_A)$ and $\omega \in S(\mathcal{H}_B)$ (ancilla)

(26) $$\rho \longrightarrow \rho \otimes \omega$$ is called extension with ancilla

- reduction to a subspace

$\rho \in S(\mathcal{H}_A \otimes \mathcal{H}_B)$

(27) $$\rho \longrightarrow \sigma = Tr_B\{\rho\} \in S(\mathcal{H}_B)$$

If B is a large reservoir the dynamics of σ

describes e.g. dissipation

All of these allowed operations can be summarized in the set of <u>completely positive, linear, trace-conserving maps</u>

(28) $$\mathcal{E} : \ S(\mathcal{H}) \longrightarrow S(\mathcal{H})$$

"linear" to conserve convexity of states ρ
"positive" to conserve positivity of states ρ
"trace-conserving" to conserve probability

However, the map must also be <u>completely positive</u>
This is the case if for all values of $N \in \mathbb{N}$

(29) $$\mathcal{E} \otimes \mathbb{1}_N \quad \text{is positive}$$

This is indeed more stringent than positivity!

<u>example</u> transposition

(30) $$\mathcal{E}(\rho) = \rho^T \qquad \text{is obviously positive}$$

but it is not completely positive. Consider spin 1/2 particles i.e. $\mathbb{C}^2$ and extension by a second spin 1/2 system

(31) $$(\mathbb{1} \otimes \mathcal{E})(\rho)$$

for $\rho = |\psi\rangle\langle\psi| \in \mathbb{C}^4$ with $|\psi\rangle$ an entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle|1\rangle\right) \Rightarrow$$

$$(32) \qquad \rho = \frac{1}{2}\begin{array}{c c} & \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

$\Rightarrow$

$$(33) \quad (\mathbb{1} \otimes \mathcal{E})(\rho) = \frac{1}{2}\begin{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}^T & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^T \\ \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^T & \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}^T \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

which has the eigenvalues $\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right)$!

$\Rightarrow$ transposition of ρ is not a physical operation

Every completely positive, linear, trace conserving map can be written in the form

$$(34) \qquad \mathcal{E}(\rho) = \sum_{i=1}^{K} E_i \rho E_i^+ \qquad \sum_{i=1}^{N} E_i^+ E_i = \mathbb{1} \quad (35)$$

(35) guarantees trace conservation

$$(36) \quad Tr(\mathcal{E}(\rho)) = Tr\left\{\sum_{i=1}^{k} E_i \rho E_i^+\right\} = Tr\left\{\sum_{i=1}^{k} E_i^+ E_i \rho\right\} = Tr\{\rho\}$$

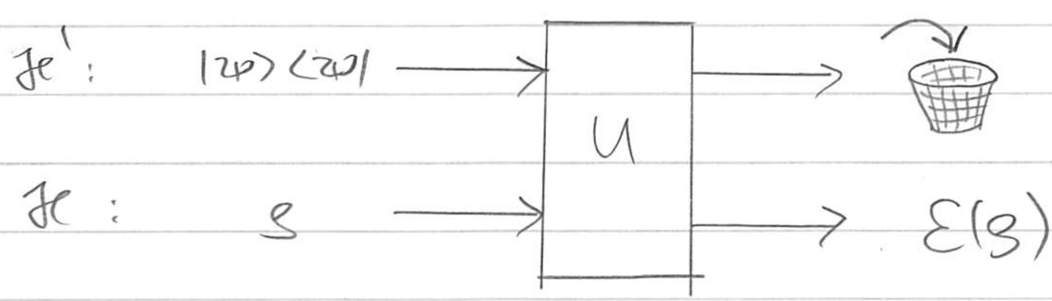
The operators E_i, called <u>Krauss operators</u> are not hermitian.

theorem of Stinespring

Given a Hilbertspace $\mathcal{H}$ with $\dim(\mathcal{H}) = N$ and a completely positive, linear, trace conserving map $\mathcal{E} : S(\mathcal{H}) \to S(\mathcal{H})$. Then there exists a Hilbertspace $\mathcal{H}'$ with $\dim(\mathcal{H}') \leq N^2$ such that for any state $|\psi\rangle \in \mathcal{H}'$ there is a unitary operation U on the combined space $\mathcal{H} \otimes \mathcal{H}'$ with

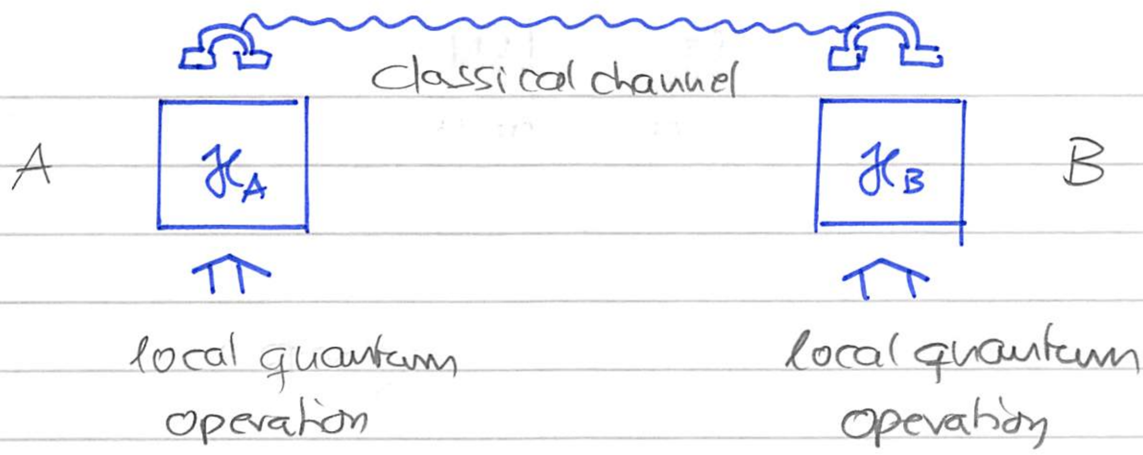
$$\mathcal{E}(\rho) = \mathrm{Tr}_{\mathcal{H}'} \left\{ U \left[\rho \otimes |\psi\rangle\langle\psi| \right] U^\dagger \right\} \tag{37}$$

This means any (allowed) operation in state space can be lifted to a unitary evolution in an extended Hilbert space



1.3 Operations in bi-partite systems

A special class of allowed operations in a bi-partite system A, B (Alice, Bob) which plays a key role in quantum information are LOCC operations ("local quantum operations with classical communication")



- <u>local operations</u> A, B totally independent

$$(38)\quad \rho \to \mathcal{E}(\rho) = \sum_{i=1}^{k} \sum_{j=1}^{L} (\hat{A}_i \otimes \hat{B}_j)\, \rho\, (\hat{A}_i \otimes \hat{B}_j)^{\dagger}$$

$\hat{A}_i$ acts only in $\mathcal{H}_A$; $\hat{B}_j$ acts only in $\mathcal{H}_B$

- <u>local operations with one-way classical communication</u>

Now Alice sends information to Bob, e.g. about the outcomes of her measurements. Then Bob can perform operations on his system part that depend on these results

$$\hat{A}_i \longrightarrow \hat{B}_j^{(i)}$$

$$(39)\quad \rho \to \mathcal{E}(\rho) = \sum_{i=1}^{k} \sum_{j=1}^{L} (\mathbb{1}_A \otimes \hat{B}_j^{(i)}) \left[(\hat{A}_i \otimes \mathbb{1}_B)\, \rho\, (\hat{A}_i^{\dagger} \otimes \mathbb{1}_B) \right] \cdot (\mathbb{1}_A \otimes \hat{B}_j^{(i)})^{\dagger}$$

- <u>local operations with two-way classical comm.</u>

$\boxed{\text{LOCC}}$

1.4 measurability of unknown quantum states and no-cloning theorem

(i) $\boxed{\text{an entirely unknown quantum state of a single quantum system cannot be completely determined by a measurement}}$

example: $\mathbb{C}^2$: $\{|0\rangle, |1\rangle\}$ arbitrary ONB

complete measurement $\hat{\Pi}_0 = |0\rangle\langle 0|$, $\hat{\Pi}_1 = |1\rangle\langle 1|$

$$\rho = |\psi\rangle\langle\psi| \begin{array}{l} \nearrow \quad \lambda = 0 \qquad \dfrac{\hat{\Pi}_0 \rho \hat{\Pi}_0}{\mathrm{Tr}\{\hat{\Pi}_0 \rho\}} \\ \searrow \quad \lambda = 1 \qquad \dfrac{\hat{\Pi}_1 \rho \hat{\Pi}_1}{\mathrm{Tr}\{\hat{\Pi}_1 \rho\}} \end{array}$$

yields only one bit of information

full state in general contains much more than 1 bit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

remark: if one possesses a large number of quantum systems prepared in the same state then optimal strategies exist to determine $|\psi\rangle$ with least ressources ("state estimation")

(ii) $\boxed{\text{an entirely unknown quantum state can in general not be duplicated (no cloning theorem)}}$

proof: copy machine $|\alpha\rangle|0\rangle \xrightarrow{?} |\alpha\rangle|\alpha\rangle$
for arbitrary $|\alpha\rangle$

assume

$$U\left[|\alpha\rangle|0\rangle\right] = |\alpha\rangle|\alpha\rangle$$

$|\alpha\rangle, |\beta\rangle$ orthogonal

$$U\left[|\beta\rangle|0\rangle\right] = |\beta\rangle|\beta\rangle$$

consider now $|\gamma\rangle = \frac{1}{\sqrt{2}}\left(|\alpha\rangle + |\beta\rangle\right)$

$|\gamma\rangle$ is neither orthogonal to $|\alpha\rangle$ nor to $|\beta\rangle$!

$$U\left[|\gamma\rangle|0\rangle\right] = U\left[\frac{1}{\sqrt{2}}|\alpha\rangle|0\rangle + \frac{1}{\sqrt{2}}|\beta\rangle|0\rangle\right]$$

$$= \frac{1}{\sqrt{2}}|\alpha\rangle|\alpha\rangle + \frac{1}{\sqrt{2}}|\beta\rangle|\beta\rangle \neq |\gamma\rangle|\gamma\rangle$$

$\Rightarrow$ only orthogonal states can be duplicated

remark: there are optimal strategies for approximate cloning ("optimum cloning")