Quantum Information
WS 2022/2023
2SWS

english We 10:00 – 11:30 46/270

videorecordings & lecture notes via

1) OLAT
2) www.physik.uni-kl.de/agfleischhauer
   → teaching

content

1. basics from quantum mechanics
2. entanglement
3. elements of classical information theory
4. quantum computing & algorithm
5. quantum error correction & fault tolerance
(6. topological quantum computation)

not covered:

physical implementations

I. Some basics from quantum mechanics

we need two essential ingredients for q. information

- information is encoded in states (pure or mixed)
- information processing: unitary and non-unitary operations in Hilbert space + classical information transfer

I.1 Quantum states

(A) pure states $|\psi\rangle$

elements of Hilbert space $\mathcal{H}$ & scalar product

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

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

most elementary nontrivial Hilbert space $\mathbb{C}^2$

ONbasis $\{|0\rangle, |1\rangle\}$

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

(B) mixed states

How to describe quantum system if information is incomplete? $\Rightarrow$ probability p_j to be in state $|\psi_j\rangle$
($|\psi_j\rangle$ is ONB)

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

Else

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

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

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

$$\neq p_1\langle\hat{A}\rangle_1 + p_2\langle\hat{A}\rangle_2 \qquad \text{as it should}$$

However the physically meaningful object is not the state $|\psi\rangle$ but the projector onto it

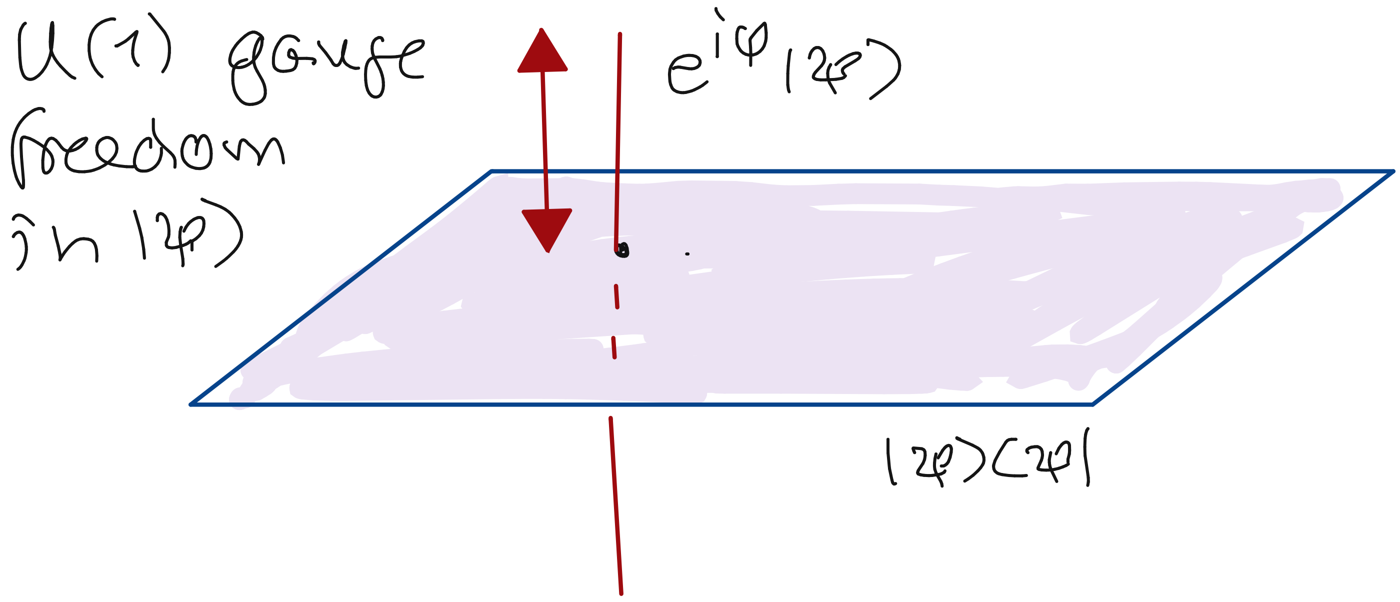
(5) $$\hat{\Pi} = |\psi\rangle\langle\psi|$$

since for all observables holds $(\dim \mathcal{H} = d)$

$$\langle \hat{A} \rangle = \langle \psi | \hat{A} | \psi \rangle = \sum_{j=1}^{d} \langle \psi | \hat{A} | \varphi_j \rangle \langle \varphi_j | \psi \rangle$$

ONB

(6) $$= \sum_{j=1}^{d} \langle \phi_j | \psi \rangle \langle \psi | \hat{A} | \phi_j \rangle = \mathrm{Tr}\{ |\psi\rangle\langle\psi| \hat{A} \}$$



Instead of eq. (4) we should use the weighted sum of projectors

(7) $$\boxed{|\phi\rangle\langle\phi| \longrightarrow \sum_{j=1}^{d} p_j \, |\psi_j\rangle\langle\psi_j| = \hat{\rho}}$$

density operator

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

- $\rho = \rho^{+}$ defined on whole $\mathcal{H}$
  ρ is self adjoint

- ϱ is positive semi-definite i.e. its eigenvalues $\lambda_j \geq 0$ (eigenstate: $|\psi_j\rangle$)
- $\mathrm{Tr}\{\varrho\} = \sum_j \lambda_j = 1$

  λ_j are probabilities to find system in associate eigenstate $|\psi_j\rangle$

The set $S(\mathcal{H})$ of all density operators in $\mathcal{H}$ is called state space

$S(\mathcal{H})$ is convex, i.e. if $\varrho_1, \varrho_2 \in S(\mathcal{H})$ and η real with $0 \leq \eta \leq 1$, then

(8) $$\eta \varrho_1 + (1-\eta)\varrho_2 \in S(\mathcal{H})$$

I.e. convex sums of density operators are again density operators

$$\varrho = \sum_j \eta_j \varrho_j \in S(\mathcal{H}) \quad \text{if} \quad 0 \leq \eta_j \leq 1, \quad \sum_j \eta_j = 1$$

Density operators of pure states are projectors

(9) $$\varrho = |\psi\rangle\langle\psi| \implies \varrho^2 = \varrho$$

A quantitative measure of the mixedness of a state is e.g. the parity

$$\text{Tr}\{\rho^2\} = \text{Tr}\left\{\left(\sum_j p_j |\psi_j\rangle\langle\psi_j|\right)^2\right\} \tag{10}$$
$$= \sum_j p_j^2 \leq \sum_j p_j = 1$$

Every mixed state ρ can be written in the form

$$\rho = \sum_{j=1}^{d} p_j |\psi_j\rangle\langle\psi_j| \tag{11}$$

$0 \leq p_j \leq 1$

$\sum_{j=1}^{d} p_j = 1$

with $\{|\psi_j\rangle\}$ being an ONB. Then the p_j can be interpreted as probability to find the system in state $|\psi_j\rangle$

Representation (11) is unique if all p_j are different, i.e. if ρ has a non-degenerate spectrum

(c) pure two-partite states

In quantum information the separation of a quantum system into partitions plays an important role. Very often this is a separation of the Hilbert space into basis states corresponding to different spatial positions.

$\boxed{A \hat{=} \text{"Alice"}}$ $\boxed{B \hat{=} \text{"Bob"}}$

(12) $$\mathcal{H} = \mathcal{H}_A \times \mathcal{H}_B$$

$|\phi\rangle_A \in \mathcal{H}_A$ $\quad$ $\dim(\mathcal{H}_A) = n$

$|\phi\rangle_B \in \mathcal{H}_B$ $\quad$ $\dim(\mathcal{H}_A) = m$

pure states in $\mathcal{H}$ that can be represented in the form

(13) $$\boxed{|\psi\rangle = |\phi\rangle_A \otimes |\phi'_B\rangle}$$

"$\otimes$" often dropped

are called product states, separable states or factorizable.

If such a representation does not exist, the state is called entangled

Remark: The notion of entanglement requires the a-priori separation into partitions.

Schmidt theorem Let $\mathcal{H} = \mathcal{H}_A \times \mathcal{H}_B$, $\dim(\mathcal{H}_A) = n$ and $\dim(\mathcal{H}_B) = m$ with $n \leq m$. Then for every (pure) state $|\psi\rangle \in \mathcal{H}$ there exists a decomposition into ONBs $\{|j\rangle_A\}$ and $\{|j\rangle_B\}$ of the form

(14) $$|\psi\rangle = \sum_{j=1}^{n} \sqrt{\lambda_j}\, |j\rangle_A |j_B\rangle \qquad 0 \leq \lambda_j \leq 1$$

Proof: it certainly holds that

$$|\psi\rangle = \sum_{j=1}^{n} \sum_{\ell=1}^{m} \alpha_{j\ell}\, |j\rangle_A |\ell\rangle_B$$

let

$$\sum_{\ell=1}^{m} \alpha_{j\ell} |\ell\rangle_B \equiv |\tilde{j}\rangle_B \qquad j = 1, 2, \dots, n$$

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

(i) $$|1\rangle_B \equiv \frac{1}{\sqrt{\sum_{\ell=1}^{m} |\alpha_{1\ell}|^2}} |\tilde{1}\rangle_B$$

(ii) $$|2'\rangle_B \equiv |\tilde{2}\rangle_B - {}_B\langle \tilde{1}|\tilde{2}\rangle_B |1\rangle_B$$

$$\hookrightarrow \quad {}_B\langle 2'|1\rangle_B = 0 \qquad \text{orthogonalized}$$

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

(iv) $$|3'\rangle_B \equiv |\tilde{3}\rangle_B - {}_B\langle \tilde{1}|\tilde{3}\rangle_B |1\rangle_B - {}_B\langle \tilde{2}|\tilde{3}\rangle_B |2\rangle_B$$

etc.

all coefficients can be made real and positive by incorporating phase factors in the definition of $|i_B\rangle$

- The number of non-vanishing λ_j is called Schmidt number s.

Any pure bi-partite state with $s > 1$ is entangled.

The ordered set of coefficients

$$\lambda_1 \geq \lambda_2 \geq \lambda_3 \cdots \geq \lambda_s$$

is called Schmidt spectrum or entanglement spectrum

(D) reduced density matrix

All properties of the subsystem A are determined by the reduced density matrix

(15) $$\rho_A = \mathrm{Tr}_B\{\rho\}$$

since for an operator $\hat{O}$ acting in $\mathcal{H}_A$ only

(16)
$$\mathrm{Tr}\{\rho\hat{O}\} = \mathrm{Tr}_{A+B}\{\rho\hat{O}\}$$
$$= \mathrm{Tr}_A\{\mathrm{Tr}_B\{\rho\}\hat{O}\} = \mathrm{Tr}_A\{\rho_A\hat{O}\}$$

Using Schmidt's theorem eq. (14) one sees that ρ_A is a proper density matrix

$$\rho_A = \mathrm{Tr}_B\{\rho\} = \mathrm{Tr}_B\left\{\sum_{\ell,j}\sqrt{\lambda_j\lambda_\ell}\,|j\rangle_A\,\underbrace{|j\rangle_B\,{}_B\langle\ell|}_{\leftrightarrow\,\delta_{j\ell}}\,{}_A\langle\ell|\right\}$$

(17)

$$= \sum_j \lambda_j\,|j\rangle_A\,{}_A\langle j|$$

The Schmidt spectrum / entanglement spectrum is thus the eigenvalue spectrum of the reduced density matrix.

In contrast to pure bi-partite states the definition and the derivation of calculable criteria for entanglement of mixed states is much more involved

I.2 operations

In quantum physics we distinguish between two classes of operations on a state

- unitary evolution
- measurements (with sub classes)

(A) unitary evolution (dynamical map)

(18) $$\boxed{\rho(0) \longrightarrow \rho(t) = U(t)\,\rho(0)\,U^\dagger(t)}$$

where

(19) $$U^\dagger(t) = U^{-1}(t)$$

is a unitary operator.

unitary evolution conserves purity of a state

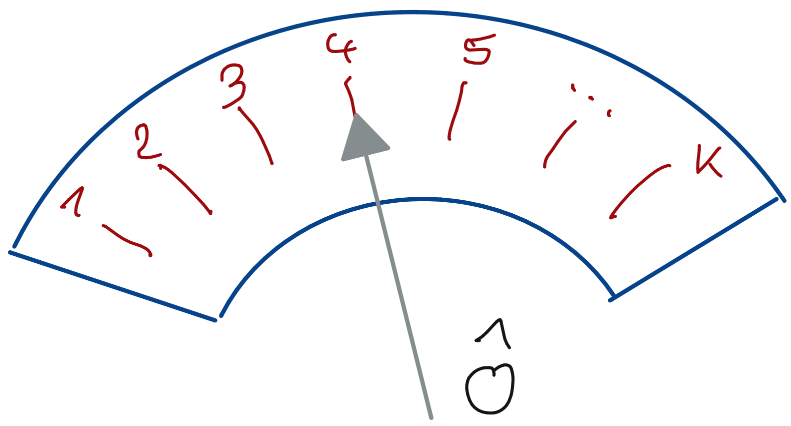
$$\mathrm{Tr}\{\rho(t)^2\} = \mathrm{Tr}\{(U\rho(0)U^\dagger)^2\}$$

(20) $$= \mathrm{Tr}\{U\rho(0)\underbrace{U^\dagger U}_{=\mathbb{1}}\rho(0)U^\dagger\} = \mathrm{Tr}\{U^\dagger U\rho(0)^2\}$$

$$= \mathrm{Tr}\{\rho(0)^2\}$$

(B) projective measurements

Let $i = 1, 2, \ldots, k$ be an index that characterizes the outcome of a measurement of a certain observable $\hat{O}$



The measurement outcomes are eigenvalues of $\hat{O}$ $\lambda_1, \lambda_2, \ldots, \lambda_k$ and Π_i is the projector to the eigenstates or in case of degeneracies to the subspace of eigenstates $\{|\lambda_j^\alpha\rangle\}$ corresponding to λ_j

If λ_j is non-degenerate:

(21) $$\hat{\Pi}_j = |\lambda_j\rangle\langle\lambda_j|$$

If λ_j is d-fold degenerate than $\hat{\Pi}_j$ is d-dimensional projector. It always holds

(22) $$\hat{\Pi}_i \hat{\Pi}_j = \delta_{ij} \hat{\Pi}_i$$
$$\sum_{i=1}^{k} \hat{\Pi}_i = \mathbb{1}$$

One distinguishes a selective projective measurement (measurement outcome is known)

(23) $$\boxed{\rho \rightarrow \rho' = \frac{\hat{\Pi}_i \rho \hat{\Pi}_i}{\mathrm{Tr}\{\hat{\Pi}_i \rho \hat{\Pi}_i\}}}$$

and a non-selective projective measurement (measurement outcome unknown)

(24) $$\boxed{\rho \rightarrow \rho'' = \sum_{j=1}^{k} \hat{\Pi}_j \rho \hat{\Pi}_j}$$

Note that $\mathrm{Tr}\{\rho''\} = 1$ since

$$\mathrm{Tr}\{\rho''\} = \mathrm{Tr}\left\{\sum_{j=1}^{k} \hat{\Pi}_j \rho \hat{\Pi}_j\right\} = \mathrm{Tr}\left\{\sum_j^{k} \hat{\Pi}_j^2 \rho\right\}$$

$$= \mathrm{Tr}\left\{\sum_j^K \hat{\pi}_j \rho\right\} = \mathrm{Tr}\{\rho\} = 1$$

The a-priori probability of outcome λ_i in a selective measurement is

$$\boxed{p_i = \mathrm{Tr}\{\hat{\pi}_i \rho \hat{\pi}_i\} = \mathrm{Tr}\{\hat{\pi}_i \rho\}} \tag{25}$$

in the non-degenerate case $\hat{\pi}_j = |\lambda_j\rangle\langle\lambda_j|$

$$p_i = \langle\lambda_i|\rho|\lambda_i\rangle \tag{26}$$

If all projectors $\hat{\pi}_j$ are 1-dimensional a measurement is called complete. After a complete measurement the quantum system is always in a pure state! An incomplete measurement can leave the system in a mixed state even if the original state was pure. In the extreme case of a non-selective measurement

(C) Other operations

extension by anzilla

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

anzilla $\omega \in S(\mathcal{H}_B)$

(27) $\quad \varrho \longrightarrow \varrho \otimes \omega \quad$ is called extension with anzilla

purification

Any mixed state ϱ, eq. (11), can be represented as the partial trace of a pure state in an enlarged Hilbert space. This representation called purification is not unique

$$\varrho = \sum_j p_j \, |\phi_j\rangle\langle\phi_j| \quad \in \mathcal{H}_S$$

(28) $$\varrho = \mathrm{Tr}_A \{ |\psi_{SA}\rangle\langle\psi_{SA}| \}$$

with

(29) $$|\psi_{SA}\rangle = \sum_j \sqrt{p_j} \, |\phi_j\rangle |a_j\rangle$$

and $\{|a_j\rangle\}$ is an ONB in $\mathcal{H}_A$

All possible purifications with the same auxiliary space are unitarily equivalent

(30) $$|\psi'_{SA}\rangle = (\mathbb{1} \otimes U_A) |\psi_{SA}\rangle$$

(D) completely positive, linear and trace conserving maps

All operations in (A) and (B) are complete positive, linear, trace conserving maps

$$(31) \qquad \mathcal{E}: \quad S(\mathcal{H}) \longrightarrow S(\mathcal{H})$$

"linear" to conserve convexity of states ρ

"positive" to conserve positivity of states ρ

"trace conserving" to conserve probability

the map must however also be completely positive, i.e. for all values of $N \in \mathbb{N}$

$$(32) \qquad \mathcal{E} \otimes \mathbb{1}_N \quad \text{is positive}$$

This is more stringent than positivity!

example: transposition

$$(33) \qquad \mathcal{E}(\rho) = \rho^T \quad \text{is obviously positive}$$

but is not necessarily completely positive! Consider Spin 1/2 i.e. $\mathcal{H} = \mathbb{C}^2$ and extension by a second Spin 1/2 i.e. $\rho = |\psi\rangle\langle\psi| \in \mathbb{C}^4$ with $|\psi\rangle$

being an entangled state

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

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

transposition of 2nd spin

$$0 \longleftrightarrow 1$$

Then

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

which has the eigenvalues

$$\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right)$$

$\Rightarrow$ transposition of ρ is <u>not</u> a physical operation

every completely positive, linear and trace conserving map (physically allowed operation) can be written in the form

$$(34) \quad \mathcal{E}(\rho) = \sum_{j=1}^{K} E_j \rho E_j^\dagger \qquad \sum_{j=1}^{K} E_j^\dagger E_j = \mathbb{1} \quad (35)$$

Rem.: Eq. (35) guarantees trace conservation

$$\mathrm{Tr}\{\mathcal{E}(\rho)\} = \mathrm{Tr}\{\sum_{j=1}^{k} E_j \rho E_j^\dagger\} = \mathrm{Tr}(\underbrace{\sum_{j=1}^{k} E_j^\dagger E_j}_{=1} \rho)$$

$$= \mathrm{Tr}\{\rho\} = 1$$

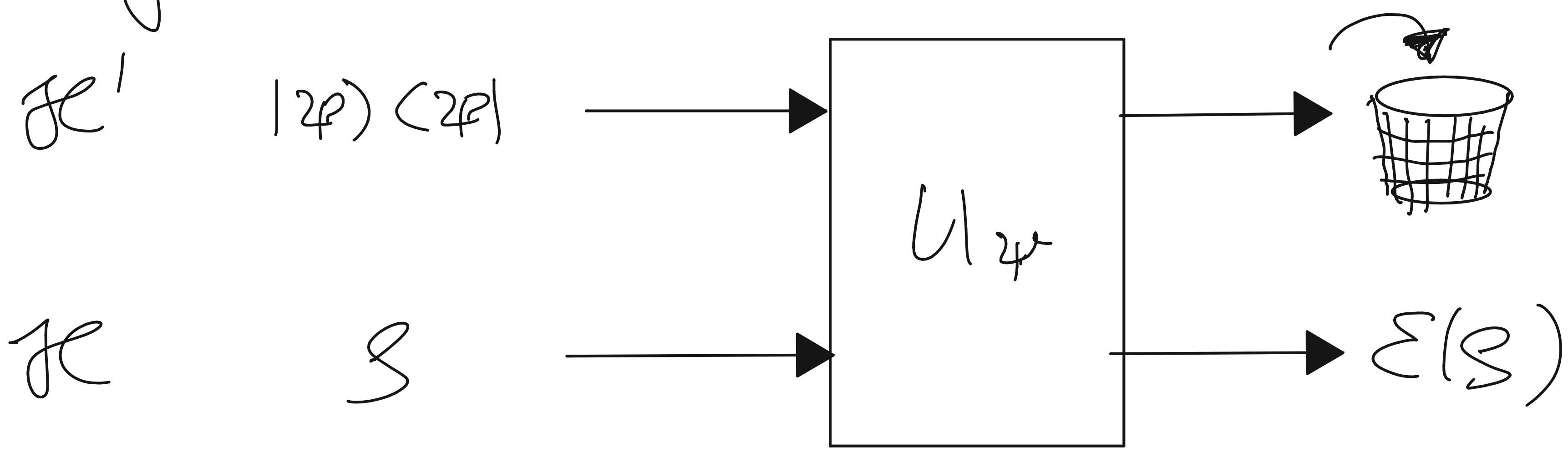
The operators E_j are called Krauss operators, they are not hermitian

theorem of Stinespring

Given Hilbert space $\mathcal{H}$ with $\dim(\mathcal{H}) = n$ and $\mathcal{E}: S(\mathcal{H}) \to S(\mathcal{H})$. Then there exists a Hilbert space $\mathcal{H}'$ with $\dim(\mathcal{H}') \leq n^2$ such that for any state $|\psi\rangle \in \mathcal{H}'$ there is a unitary U_ψ in $\mathcal{H}'$ such that

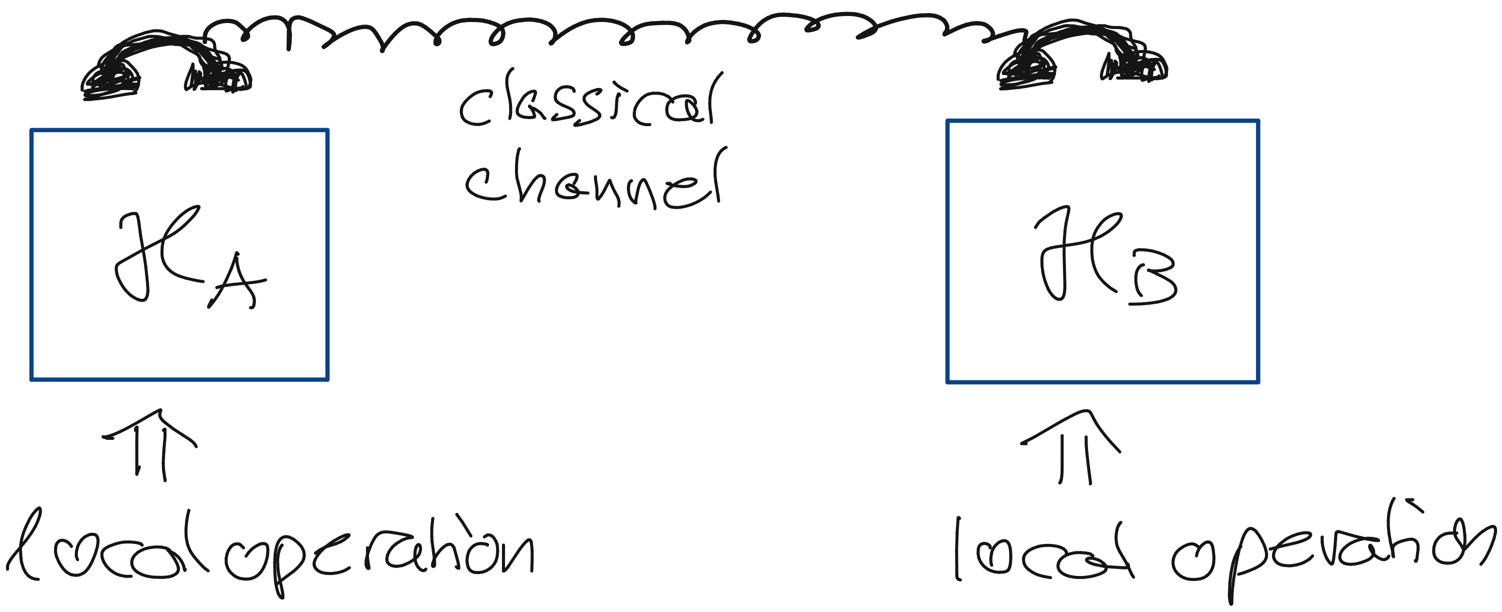
$$\mathcal{E}(\rho) = \mathrm{Tr}_{\mathcal{H}'}\{U_\psi \left[\rho \otimes |\psi\rangle\langle\psi|\right] U_\psi^\dagger\} \tag{36}$$

I.e. any allowed operation can be described by a unitary evolution in an extended Hilbert space



I.3 Operations in bi-partite systems

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



local operation

$$(37)\quad \rho \rightarrow \mathcal{E}(\rho) = \sum_{i=1}^{K} \sum_{j=1}^{L} (\hat{A}_i \otimes \hat{B}_j)\, \rho \,(\hat{A}_i \otimes \hat{B}_j)^{\dagger}$$

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

local operation with one-way classical communication

Now Alice sends information to Bob, e.g. about the outcome of her measurements. Then Bob can make operations that depend on these results

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

$$\varrho \longrightarrow \mathcal{E}(\varrho) = \sum_{i=1}^{K} \sum_{\ell=1}^{L} (\mathbb{1}_A \otimes \hat{B}_j^{(i)}) \tag{38}$$

$$\cdot \left[(\hat{A}_i \otimes \mathbb{1}_B)\, \varrho\, (\hat{A}_i^{\dagger} \otimes \mathbb{1}_B) \right] (\mathbb{1}_A \otimes \hat{B}_j^{(i)})^{\dagger}$$

local operations with two-way classical communicati

$\boxed{\text{LOCC}}$

I.4 measurability of unknown quantum states & no cloning

(i) An unknown quantum state (of a single copy) of a quantum system cannot be completely determined by a measurement

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

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

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

$$\varrho = |\psi\rangle\langle\psi| \quad \begin{cases} \lambda = 0 & \dfrac{\hat{\Pi}_0 \varrho \hat{\Pi}_0}{\mathrm{Tr}\{\hat{\Pi}_0 \varrho \hat{\Pi}_0\}} \\[2ex] \lambda = 1 & \dfrac{\hat{\Pi}_1 \varrho \hat{\Pi}_1}{\mathrm{Tr}\{\hat{\Pi}_1 \varrho \hat{\Pi}_1\}} \end{cases}$$

yields only one bit of information

full state reconstruction $\Rightarrow \alpha, \beta$

$$|\alpha|^2 \;;\; \arg(\alpha^* \beta)$$

note $|\beta|^2 = 1 - |\alpha|^2$ and total phase irrelevant

remark: with a large number of copies there are optimal strategies to determine $|\psi\rangle$ with least ressources ("state estimation")

(ii) An unknown quantum state can in general not be duplicated (no cloning theorem)

proof: duplication $|\alpha\rangle|0\rangle \xrightarrow{U} |\alpha\rangle|\alpha\rangle$ for arbitrary α

assume U exists $\quad U[|\alpha\rangle|0\rangle] \stackrel{!}{=} |\alpha\rangle|\alpha\rangle$

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

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

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

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

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

$\Rightarrow$ non-orthogonal states cannot be duplicated