

I. The formalism: States, measurements, and evolution^{I/1}

1. The formalism of quantum theory

a) Hilbert spaces & bra-ket notation

State of QM system described by vectors in a complex Hilbert space \mathcal{H} . For the purpose of this lecture (and almost all of QI):

\mathcal{H} is a finite dimensional Hilbert space, i.e. $\mathcal{H} \cong \mathbb{C}^d$.

Ket notation: For a vector in \mathcal{H} , we write

$$|v\rangle \in \mathcal{H}.$$

We also call $|v\rangle$ a "ket vector" or "ket".

Computational basis: In order to fix isomorphism to \mathbb{C}^d & vector notation, we define a canonical basis, the computational basis

$|0\rangle, |1\rangle, \dots, |d-1\rangle$, i.e.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots \quad |d-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

A general vector is thus of the form

$$|v\rangle = v_0|0\rangle + v_1|1\rangle + \dots + v_{d-1}|d-1\rangle$$

$$= \sum_{i=0}^{d-1} v_i |i\rangle = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{d-1} \end{pmatrix}$$

The adjoint vector $(|v\rangle)^{\dagger} \leftarrow$ transpose conjugate of the matrix/vector

is

$$(|v\rangle)^{\dagger} = (\overline{v_0}, \overline{v_1}, \dots, \overline{v_{d-1}}).$$

We write

$$(|v\rangle)^{\dagger} =: \langle v| \quad \text{"bra vector", "bra"}$$

$$|v\rangle = \sum v_i |i\rangle \iff \langle v| = \sum \overline{v_i} \langle i|$$

If \mathcal{H} is a vector space; we write linear combinations as

$$\lambda|v\rangle + \mu|w\rangle \in \mathcal{H}.$$

Scalar product:

For two vectors $|v\rangle = \sum v_i |i\rangle$, $|w\rangle = \sum w_j |j\rangle$, the

scalar product is given by

$$(|\omega\rangle)^\dagger \cdot (|\nu\rangle) = \sum \overline{\omega_i} \nu_i =: \underbrace{\langle \omega | \nu \rangle}_{\text{"bra-ket"}}$$

(Note: sesquilinear in 1st component: $(\lambda|\omega\rangle)^\dagger = \overline{\lambda} \langle \omega|$)

Canonical basis is orthonormal basis (ONB):

$$\langle i | j \rangle = \delta_{ij}.$$

$$\Rightarrow \text{for } |\nu\rangle = \sum \nu_i |i\rangle, \quad |\omega\rangle = \sum \omega_j |j\rangle,$$

$$\langle \omega | \nu \rangle = \sum \overline{\omega_j} \nu_i \underbrace{\langle j | i \rangle}_{\delta_{ij}} = \sum \overline{\omega_i} \nu_i.$$

$$\| |\nu\rangle \|_2 := \sqrt{\langle \nu | \nu \rangle} \text{ defines a } \underline{\text{norm}} \text{ (the } \underline{2\text{-norm}}).$$

Linear maps:

$\Pi : \mathcal{H} \rightarrow \mathcal{H}$ is a linear map,

- with $\Pi |\nu\rangle := \Pi(|\nu\rangle)$ -

$$\Pi(|\nu\rangle + \lambda|\omega\rangle) = \Pi|\nu\rangle + \lambda \Pi|\omega\rangle.$$

Note: Π always acts on right - i.e.,

$$\langle \omega | \Pi |\nu\rangle := \langle \omega | (\Pi |\nu\rangle)$$

The map $I = \sum |i\rangle\langle i|$ satisfies that ^{I/4}

for $|v\rangle = \sum v_j |j\rangle$,

$$\begin{aligned} I|v\rangle &= \left(\sum_i |i\rangle\langle i| \right) \left(\sum_j v_j |j\rangle \right) \\ &= \sum_{ij} v_j |i\rangle \underbrace{\langle i|j\rangle}_{\delta_{ij}} = \sum v_j |j\rangle \end{aligned}$$

$\Rightarrow I$ is the identity map.

This can also be seen in matrix form:

$$I = \sum_{i=0}^{d-1} |i\rangle\langle i| = \begin{pmatrix} 1 & & \\ & 1 & \\ & & \ddots \\ & & & 1 \end{pmatrix}$$

$i \rightarrow \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad (0 \dots 1 \dots 0) \quad \uparrow \quad i$

To express a general map Π in matrix form, we can write

$$\Pi = I \cdot \Pi \cdot I$$

$$= \sum_{ij} |i\rangle\langle i| \underbrace{\Pi |j\rangle\langle j|}_{=: \Pi_{ij} \in \mathbb{C}}$$

$$= \sum_{ij'} \pi_{ij'} \underbrace{|i\rangle\langle j|}_{\substack{\parallel \\ \begin{pmatrix} 0 & \cdots & 1 & 0 \\ \vdots & & 1 & \vdots \\ 0 & \cdots & 0 \end{pmatrix}}}$$

$$= \begin{pmatrix} \pi_{11} & \pi_{12} & \cdots & \pi_{1d} \\ \pi_{21} & & & \\ \vdots & & & \\ \pi_{d1} & & & \pi_{dd} \end{pmatrix}$$

And similarly for maps $\Pi: \mathcal{H}_1 \rightarrow \mathcal{H}_2$.

The map Π^+ is the map with entries $\overline{\pi_{ji}}$ (where $\pi_{ij} = \langle i | \Pi | j \rangle$). It holds that $(\Pi | \omega \rangle)^+ = \langle \omega | \Pi^+$, and $(AB)^+ = B^+ A^+$.

Unitary maps:

A map $U: \mathcal{H} \rightarrow \mathcal{H}$ is unitary if

$$U^+ U = I,$$

or equivalently:

- $U U^\dagger = I$

- $(U|\omega\rangle)^\dagger (U|v\rangle) = \langle\omega|U^\dagger U|v\rangle = \langle\omega|v\rangle$

$$\Rightarrow \|U|\omega\rangle\|_2 = \||\omega\rangle\|_2$$

(i.e., U preserves angles and norms)

In matrix notation:

$$\langle i|U|j\rangle = U_{ij}$$

$$\underbrace{\langle i|U \left(\sum_k |k\rangle\langle k| \right) U^\dagger |j\rangle}_{= U U^\dagger = I} = \langle i|j\rangle = \delta_{ij}$$

$$\Rightarrow \delta_{ij} = \sum_k U_{ik} (U^\dagger)_{kj} = U_{ik} \overline{U_{jk}}.$$

We call $U = (U_{ij})_{ij}$ a unitary matrix or
just a unitary.

Tensor Product:

For $|v\rangle_A \in \mathcal{H}_A \cong \mathbb{C}^{d_A}$, $|w\rangle_B \in \mathcal{H}_B \cong \mathbb{C}^{d_B}$,
 with comp. bases $\{|i\rangle_A\}_{i=0}^{d_A-1}$, $\{|j\rangle_B\}_{j=0}^{d_B-1}$

$$|v\rangle_A = \sum v_i |i\rangle_A, \quad |w\rangle_B = \sum w_j |j\rangle_B,$$

we can define the tensor product

$$|v\rangle_A \otimes |w\rangle_B \in \mathcal{H}_A \otimes \mathcal{H}_B = \mathcal{H}_{AB}$$

by defining $\mathcal{H}_A \otimes \mathcal{H}_B$ as the space with ONB
 of tuples $(|i\rangle_A, |j\rangle_B)$ with $i=0, \dots, d_A-1$,
 $j=0, \dots, d_B-1$

denoted by

$$|i\rangle_A \otimes |j\rangle_B \quad (\text{or } |i\rangle_A |j\rangle_B, |i,j\rangle_{AB}, |ij\rangle_{AB}, \\ |i\rangle \otimes |j\rangle, |i\rangle |j\rangle, |i,j\rangle, |ij\rangle),$$

$$\text{s.t. } (\langle i|_A \otimes \langle j|_B) (|k\rangle_A \otimes |l\rangle_B)$$

$$= \langle i|k\rangle_A \cdot \langle j|l\rangle_B = \delta_{ik} \delta_{jl},$$

$$(\pi_A \otimes N_B)(|v\rangle \otimes |w\rangle) := (\pi_A |v\rangle) \otimes (N_B |w\rangle)$$

(and extended linearly to the full space).

In matrix notation,

$$\pi_A \otimes N_B = \underbrace{\left(\sum |i,j\rangle \langle i,j| \right)}_{\text{res. of identity}} (\pi_A \otimes N_B) \left(\sum |k,e\rangle \langle k,e| \right)$$

$$= \sum \langle i,j | \pi_A \otimes N_B | k,e \rangle |i,j\rangle \langle k,e|$$

$$= \sum \langle i | \pi_A | k \rangle \langle j | N_B | e \rangle |i,j\rangle \langle k,e|$$

$$= \sum \underbrace{(\pi_A)_{ik} (N_B)_{je}}_{= (\pi_A \otimes N_B)_{(ij), (ke)}} |i,j\rangle \langle k,e|$$

$$= (\pi_A \otimes N_B)_{(ij), (ke)}$$

$$\Pi_A \otimes N_B =$$

$$\begin{pmatrix} \Pi_{00} N_{00} & \Pi_{00} N_{01} & \dots \\ \Pi_{00} N_{10} & & \\ \vdots & & \\ \Pi_{10} N_{00} & \Pi_{10} N_{01} & \dots \\ \Pi_{10} N_{01} & & \end{pmatrix}$$

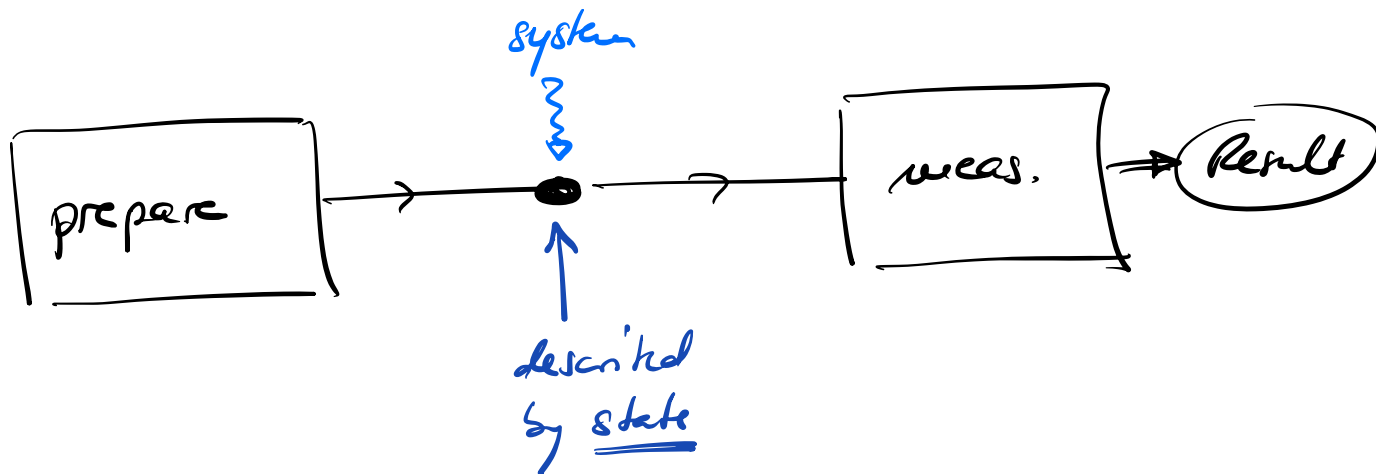
=

$$\begin{pmatrix} \Pi_{00} \cdot N & \Pi_{01} \cdot N & \dots \\ \Pi_{10} \cdot N & \Pi_{11} \cdot N & \\ \vdots & & \ddots \end{pmatrix}$$

5) The formalism of quantum theory

Quantum Theory: Framework for theories to describe tests (experiments, games) consisting of preparation and measurement.

(Another theory of this kind is probability theory — we will use it as an analogy, but that's what it is — it sometimes works and sometimes misleads.)



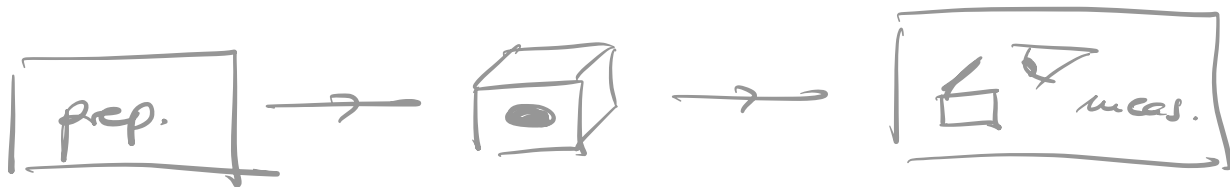
Preparation: Full set of instructions how to prepare system.

Measurement: Determine some property of phys. system.

Example / Analogy:

- Preparation:
- Put coin in box w/ p_0, p_1 ,
 - Put dice in box w/ p_1, \dots, p_6 ,

Measurement: Open box to determine head/tail,
or value of dice.
→ outcome i with prob. P_i .



State: After preparation, we can describe the complete knowledge of the system by assigning a state. The state of the system allows to predict outcomes of measurements as good as possible, given the preparation (could be probabilistic!).

Many different preparation schemes can give identical result for all measurements
→ system described by same state.

i.e.: The state carries all info about preparation relevant for measurement.

Ex: $\vec{p} = \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}$, or $\vec{p} = \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}$ is state of coin/dice. I/13

Generally: State in prob. theory is described
by vector $\vec{p} \in \mathbb{R}_{\geq 0}^d$, $\|\vec{p}\|_1 = \sum |p_i| = 1$

Measurement: outcome i w/ prob.

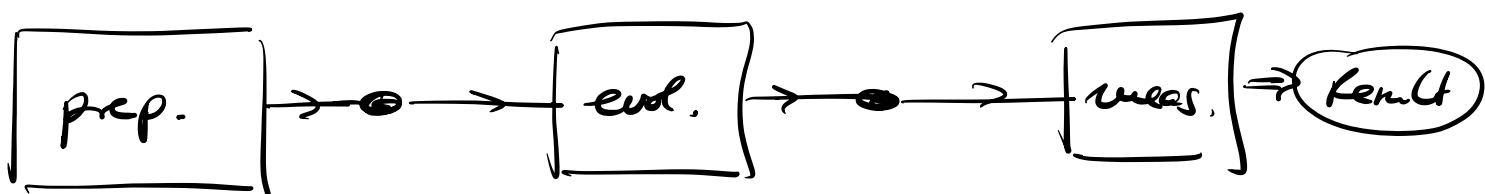
$$p_i = |\vec{e}_i \cdot \vec{p}|$$

\uparrow
 i 'th unit vector: $\vec{e}_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i$

Collapse: After the measurement, the new state
is $\vec{p}' = \vec{e}_i$: the state collapses into the outcome.

Note: The state describes our knowledge about
the system.

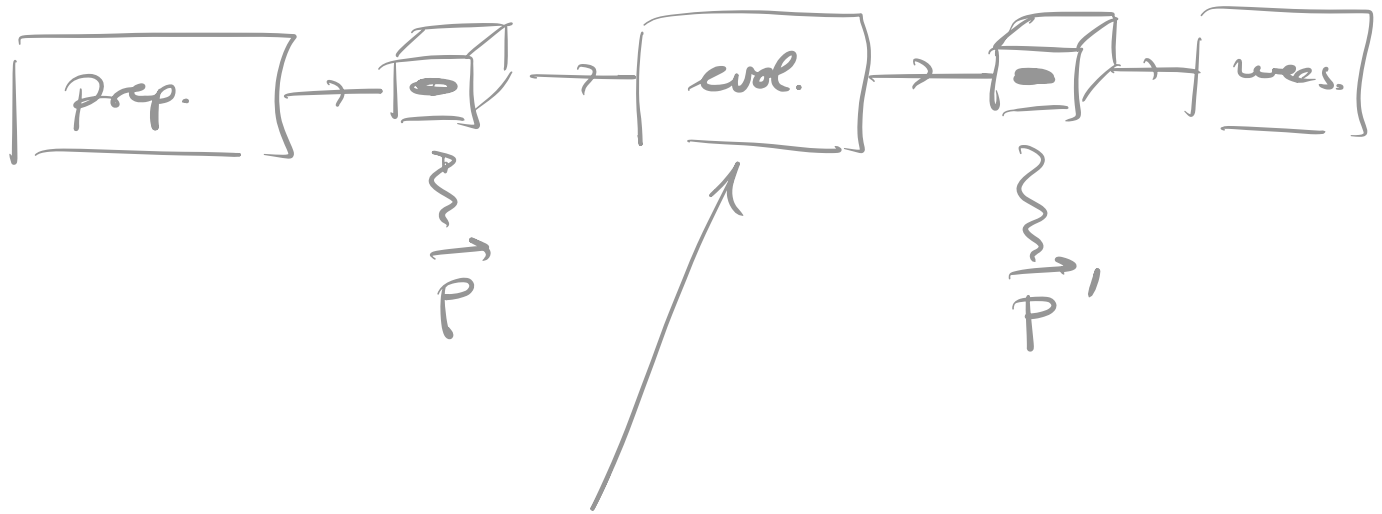
Evolution: In addition, we can "do things" with
the system betw. preparation & measurement,
i.e. evolve it:



Note: • evolution can be absorbed into prep. or meas.

• evolution can consist of a sequence of individual evolutions

Ex:



e.g.:

- shake box (\rightarrow add randomness)
- put coin heads up
- flip coin / permute dice values
- do one of the above w/ certain probability

Not general evolution:

- 1) Check value of coin/dice/... : i
- 2) Output j with prob. E_{ji} .

\rightarrow Need $\sum_j E_{ji} = 1 \quad \forall i.$

i.e. E is a stochastic matrix.

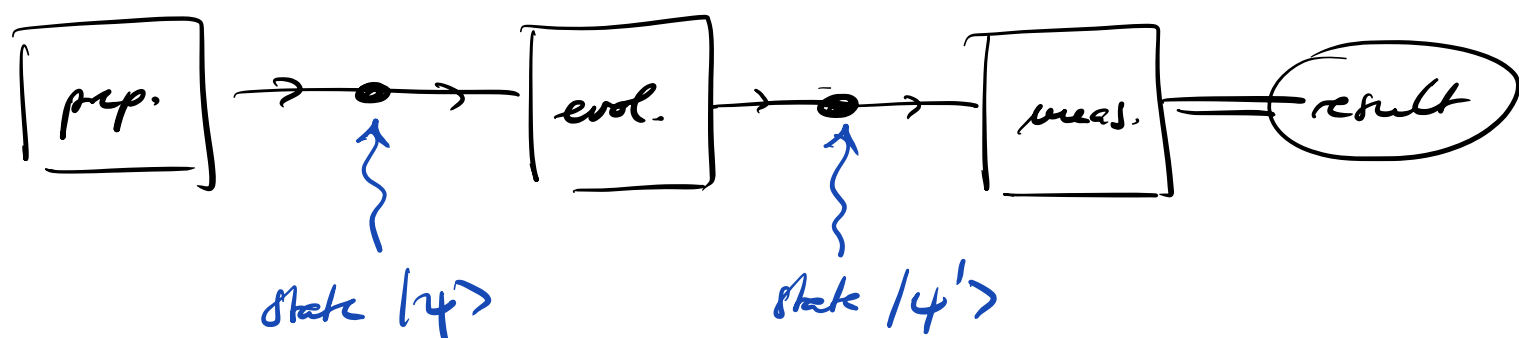
\Rightarrow Evolution maps

$$\vec{p} \mapsto \vec{p}' = E \cdot \vec{p}$$

This is the most general linear evolution
such that $\|\vec{p}\|_1 = 1 \Rightarrow \|E\vec{p}\|_1 = 1$!

Quantum Theory:

"Like probability theory, but with the $\|\cdot\|_2$ -norm instead of the $\|\cdot\|_1$ -norm." (\rightarrow Aaronson)



States: $|\psi\rangle \in \mathbb{C}^d \leftarrow$ dim. of H. space:
property of system

the only property we
care about - irrespective
of physical realization.

... such that $\| |\psi\rangle \|_2 = 1$

— often, just write $\| |\psi\rangle \|$

and where $|\psi\rangle$ and $e^{i\phi} |\psi\rangle$ represent the same state.

(i.e. more precisely, states are rays in \mathbb{C}^d , or elements of the projective space $\mathbb{C}^d / \mathbb{C}^\times$ — but we will stick to the convention above.)

Note: State is also often called wavefunction (WF) in QM!

$$\text{State: } |\psi\rangle \in \mathbb{C}^d, \quad \| |\psi\rangle \|_2 = 1, \quad |\psi\rangle \sim e^{i\phi} |\psi\rangle$$

Measurements in Q. Theory:

Let $\{ |b_i\rangle \}$ be an ONB in \mathbb{C}^d , i.e. $\langle b_i | b_j \rangle = \delta_{ij}$.

Then $\{ |b_i\rangle \}$ defines a measurement
("measurement in the basis $\{ |b_i\rangle \}$ ")

with the probability p_i of outcome i given by

$$p_i = |\langle b_i | \psi \rangle|^2$$

Note that

$$\begin{aligned}
 \sum p_i &= \sum |\langle b_i | \psi \rangle|^2 \\
 &= \sum \langle \psi | b_i \rangle \langle b_i | \psi \rangle \\
 &= \langle \psi | \underbrace{\left(\sum |b_i\rangle \langle b_i| \right)}_{=I} | \psi \rangle \\
 &= \langle \psi | \psi \rangle \\
 &= \| |\psi\rangle \|_2^2 = 1.
 \end{aligned}$$

i.e.: $\| |\psi\rangle \|_2 = 1 \iff$ total probability for some outcome is 1.

Collapse of the state:

After meas. in basis $\{|b_i\rangle\}$ and outcome i ,
the system is described by the state $|\psi_i\rangle = |b_i\rangle$.

\Rightarrow Repeat meas. immediately:

$$p_j' = |\langle b_j | \underbrace{|\psi_i\rangle}_{=|b_i\rangle} \rangle|^2 = \delta_{ij} \Rightarrow \text{same result!}$$

Note: The measurement can also be described through orthogonal projections $E_i = |b_i\rangle \langle b_i|$. Then, the state $|\tilde{\psi}_i\rangle = E_i |\psi\rangle$ gives us:

- the outcome probability

$$p_i = \|\tilde{|\psi_i\rangle}\|^2$$

- the post-measurement state

$$|\psi_i\rangle = \frac{|\tilde{\psi}_i\rangle}{\|\tilde{|\psi_i\rangle}\|} = \frac{|\tilde{\psi}_i\rangle}{\sqrt{p_i}}$$

This can be generalized to any complete set of orthogonal projections $\{E_i\}$: $E_i = E_i^\dagger$, $E_i E_j = \delta_{ij} E_i$, $\sum E_i = I$.

Evolution: QM evolution is linear:

$$|\psi\rangle \mapsto U|\psi\rangle$$

It should preserve probabilities, i.e. the total prob. for some outcome sums to 1.

We thus require

$$\|U|\psi\rangle\|_2 = \|\psi\rangle\|_2 = 1$$

i.e. U is norm-preserving.

$\Rightarrow U$ is unitary, $UU^\dagger = U^\dagger U = I$,

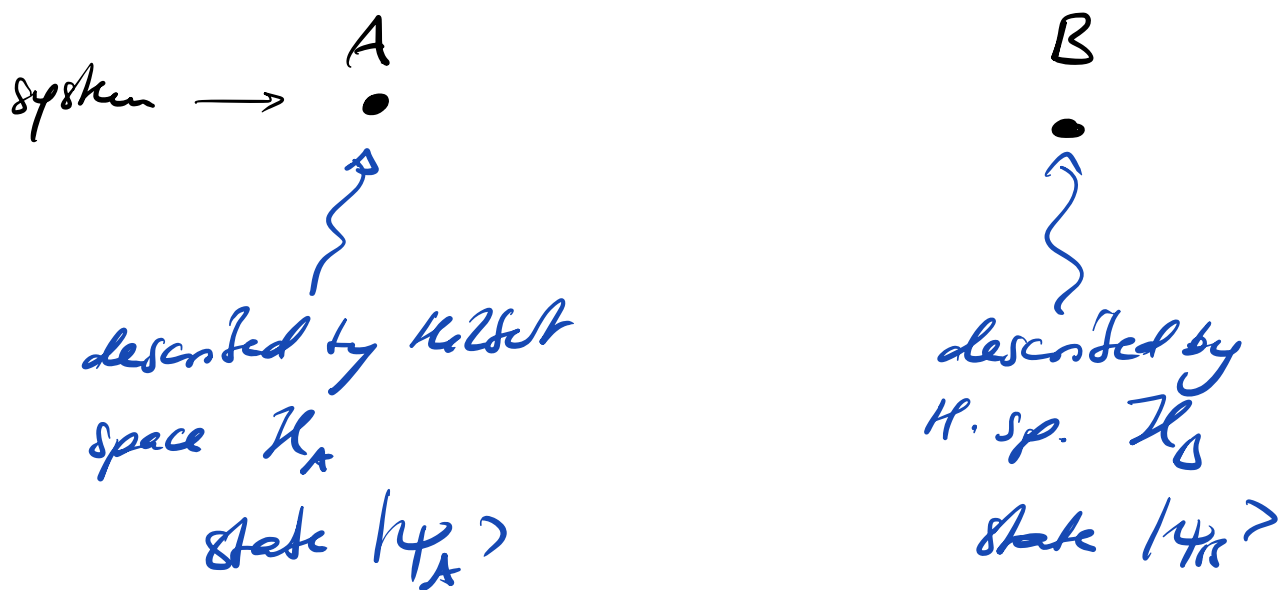
And: Any unitary U is an allowed evolution.

Evolution: $|\psi\rangle \mapsto U|\psi\rangle$, $UU^\dagger = U^\dagger U = I$

Composite systems:

What if we have two parties A & B, who each control a quantum system ("subsystem")?

How should we describe their state?



A & B should be able to describe their respective system indep. of the other party (\Leftrightarrow the rest of the world) \rightarrow states $|\psi_A\rangle, |\psi_B\rangle$.

\rightarrow Joint state of A & B described by

$$\underline{|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \in \mathcal{H}_{AB}.$$

What if Alice performs a measurement (given by $\{E_i^A\}$) or evolution (given by U_A)? (Write X_A for either.)

\rightarrow should be independent of Bob's actions (or even existence).

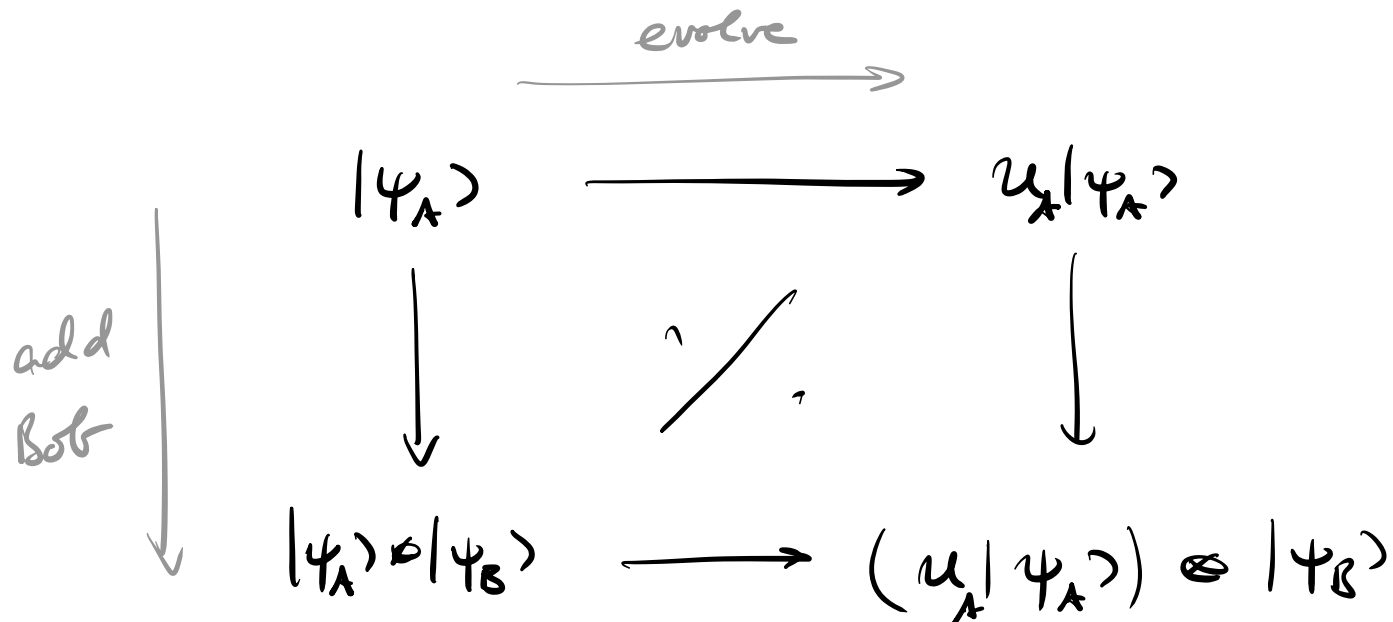
\rightarrow Action on $|\psi_{AB}\rangle$ given by

$$\underline{|\psi_{AB}\rangle \mapsto (X_A \otimes I_B) |\psi_{AB}\rangle.}$$

$$\begin{array}{c} \parallel \\ |\psi_A\rangle \otimes |\psi_B\rangle \mapsto (X_A |\psi_A\rangle) \otimes |\psi_B\rangle \quad \forall |\psi_B\rangle. \end{array}$$

Why is this a good (correct) choice?

- E.g.: Alice evolves her state with U_A



• or; measure $\{E_i^A\}$. Prob.:

$$\| (E_i^A \otimes I) |\psi_A\rangle \otimes |\psi_B\rangle \|^2 =$$

$$= (\langle \psi_A| \otimes \langle \psi_B|) (E_i^A \otimes I) |\psi_A\rangle \otimes |\psi_B\rangle$$

↑
 $E_i^A = E_i$

$$= \underbrace{\langle \psi_A | E_i^A | \psi_A \rangle}_{\|E_i^A |\psi_A\rangle\|^2} \cdot \underbrace{\langle \psi_B | \psi_B \rangle}_{=1}$$

1/22

Note: If both A & B act with X_A & Y_B , the

total action is $(I \otimes Y_B)(X_A \otimes I) = X_A \otimes Y_B$.

Notes: • By linearity, this can be extended to all states on $\mathcal{H}_A \otimes \mathcal{H}_B$ (i.e. not of the form $|\psi_A\rangle \otimes |\psi_B\rangle$).

• The post-measurement state of a measurement $\{E_i^A\} \equiv \{E_i^A \otimes I_B\}$ is

$$|\psi_i\rangle \propto (E_i^A \otimes I_B) |\psi\rangle.$$

• Works the same for composition of more systems (e.g. inductively!)

Analogy - probability:

2 coins with $\vec{p}_A = (\frac{1}{3}, \frac{2}{3})$, $\vec{p}_B = (\frac{1}{4}, \frac{3}{4})$

\Rightarrow total prob. distr. has 4 possible results

00, 01, 10, 11, with

$$\underbrace{(p_{00}, p_{01}, p_{10}, p_{11})}_{\vec{p}_{AB}} = \left(\frac{1}{3} \cdot \frac{1}{4}, \frac{1}{3} \cdot \frac{3}{4}, \frac{2}{3} \cdot \frac{1}{4}, \frac{2}{3} \cdot \frac{3}{4} \right) = \vec{p}_A \otimes \vec{p}_B.$$

Flipping the first coin — i.e. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ — acts on \vec{p}_{AB} as $X \otimes I = \begin{pmatrix} & 1 & & \\ 1 & & & \\ & & 1 & \\ & & & \end{pmatrix}$.

Measuring the value of the 1st coin — given by projections $E_0^A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $E_1^A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, amounts on \vec{p}_{AB} to $E_0 = E_0^A \otimes I = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & \\ & & & 0 \end{pmatrix}$ etc.

Quantum mechanical axioms (practical version):

- Systems are described by Hilbert spaces $\mathcal{H} \cong \mathbb{C}^d$.
- States are normalized vectors
 $|\psi\rangle \in \mathcal{H}$, $\| |\psi\rangle \| = 1$, $|\psi\rangle \sim e^{i\phi} |\psi\rangle$
- Evolutions $|\psi\rangle \mapsto U|\psi\rangle$ are unitary, $U^\dagger U = U U^\dagger = I$
- Measurements are given by complete sets of orth. projectors $\{E_i\}$, $E_i = E_i^\dagger$, $E_i E_j = \delta_{ij} E_i$,

$\sum E_i = I$, by virtue of

$$|\tilde{\psi}_i\rangle := E_i |\psi\rangle$$

with prob. $p_i = \| |\tilde{\psi}_i\rangle \|^2 = \langle \tilde{\psi}_i | \tilde{\psi}_i \rangle$

and post-meas. state $|\psi_i\rangle = \frac{|\tilde{\psi}_i\rangle}{\| |\tilde{\psi}_i\rangle \|}$

- Composite systems are described by tensor products $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Independent states $|\psi_A\rangle, |\psi_B\rangle$ give a state $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \in \mathcal{H}_{AB}$, and indep. operations (evol., meas.) X_A, Y_B act as $X_A \otimes Y_B$ (where "doing nothing" = I).

Notes: • In "traditional" physics teaching, measurements are described by hermitian "observable" $O = O^\dagger$, where the measurement returns an "expectation value" $\langle \psi | O | \psi \rangle$.

If we write O as its spectral decomposition, 1/25

$$O = \sum \lambda_i E_i \quad \text{non-degenerate!}$$

then $\langle \psi | O | \psi \rangle = \sum \lambda_i \langle \psi | E_i | \psi \rangle =$

$$= \sum p_i \lambda_i$$

— i.e., outcome i has the value λ_i assigned, and we measure the average value (and weights of a measurement).

In Quantum Information, when we say "we measure O ", we in fact mean "We measure $\{E_i\}$ ".

• In physics, evolutions are generated by a Hamiltonian, i.e. by a Hermitian operator $H = H^\dagger$, by virtue of

$$U = \exp(-iHt),$$

where t is time (i.e., evolutions are continuous!)

(\rightarrow Schrödinger equation $\frac{d}{dt} |\psi\rangle = -iH |\psi\rangle$)

c) Examples:

I/26

$$\text{Qubits } \mathcal{H} = \mathbb{C}^2;$$

"computational basis" $\{|0\rangle, |1\rangle\}$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

Measurement in basis $\{|0\rangle, |1\rangle\}$, i.e.

$$E_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

(Corresponds e.g. to observable $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$)

Measurement:

Outcome 0: $|\tilde{\psi}_0\rangle = E_0 |\psi\rangle = \alpha|0\rangle$

$$\begin{aligned} \rightarrow \text{prob. } p_0 &= \|\alpha|0\rangle\|^2 = |\alpha|^2 \\ &= \langle \psi | E_0 | \psi \rangle = |\alpha|^2 \\ &= |\langle 0 | \psi \rangle|^2 = |\alpha|^2 \end{aligned}$$

$$\text{Post-meas. state } |\psi_0\rangle = \frac{|\tilde{\psi}_0\rangle}{\| |\tilde{\psi}_0 \rangle \|} = |0\rangle$$

Outcome 1 : $|\tilde{\psi}_1\rangle = E_1 |\psi\rangle = \beta |1\rangle$

$$p_1 = \|\tilde{\psi}_1\|^2 = |\beta|^2$$

$$|\psi_1\rangle = |1\rangle$$

Measurement "in X basis", i.e. of observable

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |+\rangle\langle+| - |-\rangle\langle-|, \text{ with}$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

$$\begin{aligned} |\tilde{\psi}_{\pm}\rangle &= |\pm\rangle\langle\pm|\psi\rangle = |\pm\rangle \left(\frac{1}{\sqrt{2}}(\alpha|\pm\rangle + \beta|\mp\rangle) \right) \\ &= |\pm\rangle \left(\frac{1}{\sqrt{2}}(\alpha \pm \beta) \right) \end{aligned}$$

$$\Rightarrow p_{\pm} = \frac{1}{2} |\alpha \pm \beta|^2 \quad \leftarrow \text{prob.}$$

$$|\psi_{\pm}\rangle = |\pm\rangle$$

\leftarrow post-meas. state

Note: Outcomes can also be labelled by eigenvalues, e.g. outcomes $+1$ and -1 for X & Z .

Important: Pauli matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- often also written $\sigma_x = X, \sigma_y = Y, \sigma_z = Z,$

or $\sigma_1 = X, \sigma_2 = Y, \sigma_3 = Z.$ Sometimes

also $\sigma_0 = I,$

• satisfy $XY = iZ$ & cyclic: $YZ = iX$
 $ZX = iY$

• def. Pauli's anti-comm: $XY = -YX$ etc

• in addition $X^2 = Y^2 = Z^2 = I$

• summarized as $\sigma_\alpha \sigma_\beta = i \sum_\gamma \epsilon_{\alpha\beta\gamma} \sigma_\gamma + \delta_{\alpha\beta} I$
 \uparrow
 fully anti-symmetric tensor.

The Pauli matrices are Hermitian and

unitary, i.e. can describe both measurements
and evolution!

Evolution:

Consider $U = H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ "Hadamard gate"

$$U|q\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} (\alpha|0\rangle + \beta|1\rangle)$$

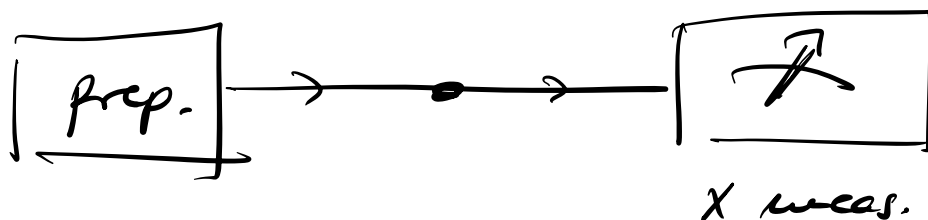
$$= \frac{\alpha + \beta}{\sqrt{2}} |0\rangle + \frac{\alpha - \beta}{\sqrt{2}} |1\rangle$$

Measurement in z -basis $\{|0\rangle, |1\rangle\}$:

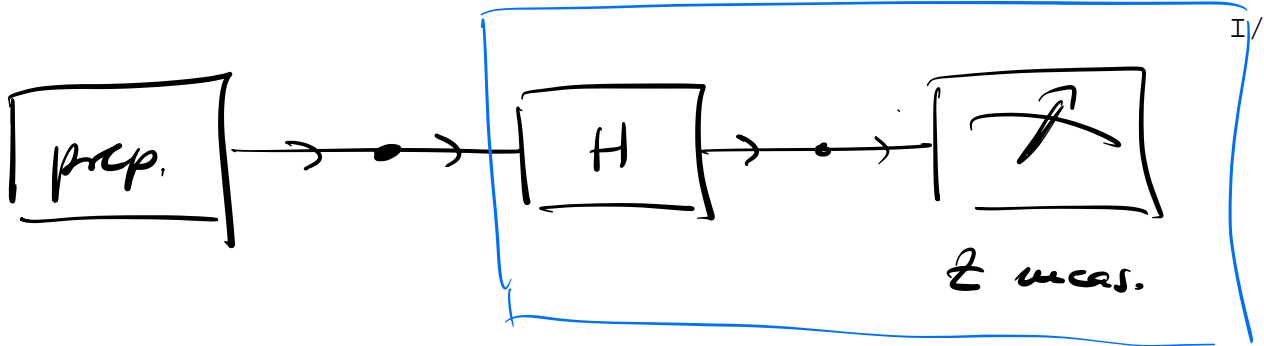
outcome 0 w/ $p_0 = \frac{|\alpha + \beta|^2}{2}$

outcome 1 w/ $p_1 = \frac{|\alpha - \beta|^2}{2}$

\Rightarrow corresponds to meas. outcome in X -basis!



...equals...



can be regarded as
a specific way to
realize X meas.

In fact, H transforms between X and Z eigenbasis back and forth:

$$H = |+\rangle\langle 0| + |-\rangle\langle 1| = |0\rangle\langle +| + |1\rangle\langle -| = H^\dagger$$

i.e.: $H X H = Z, \quad H Z H = X \quad (\text{note } H^2 = I).$

Measurement on a bipartite state:

$$|4\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$$

Alice and Bob measure Z :

project onto $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

$$\Rightarrow p_{01} = p_{10} = \frac{1}{2}, \quad p_{00} = p_{11} = 0$$

Alice and Bob measure X :

project onto $\{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$:

(use $\langle +|0\rangle = \langle +|1\rangle = \langle -|0\rangle = \frac{1}{\sqrt{2}}, \langle -|1\rangle = -\frac{1}{\sqrt{2}}$)

$$|\langle ++|\psi\rangle|^2 = \left| \frac{1}{2\sqrt{2}} - \frac{1}{2\sqrt{2}} \right|^2 = 0$$

$$|\langle +-|\psi\rangle|^2 = \left| -\frac{1}{2\sqrt{2}} - \frac{1}{2\sqrt{2}} \right|^2 = \frac{1}{2}$$

$$|\langle -+|\psi\rangle|^2 = \dots = \frac{1}{2}$$

$$|\langle --|\psi\rangle|^2 = \dots = 0$$

\Rightarrow perfect anti-correlation!

In fact, outcomes anti-correlated for same measurement in any basis! (\rightarrow homework)

(But the outcomes of A or B alone are completely random.)

But: Alice measures X , Bob Z :

$$|\langle +0 | \psi \rangle|^2 = \left| -\frac{1}{2} \right|^2 = \frac{1}{4}$$

$$|\langle +1 | \psi \rangle|^2 = \left| +\frac{1}{2} \right|^2 = \frac{1}{4}$$

$$|\langle -0 | \psi \rangle|^2 = \dots = \frac{1}{4}$$

$$|\langle -1 | \psi \rangle|^2 = \dots = \frac{1}{4}$$

Outcomes of A & B are completely independent.

d) The Bloch sphere:

Consider state of one qubit:

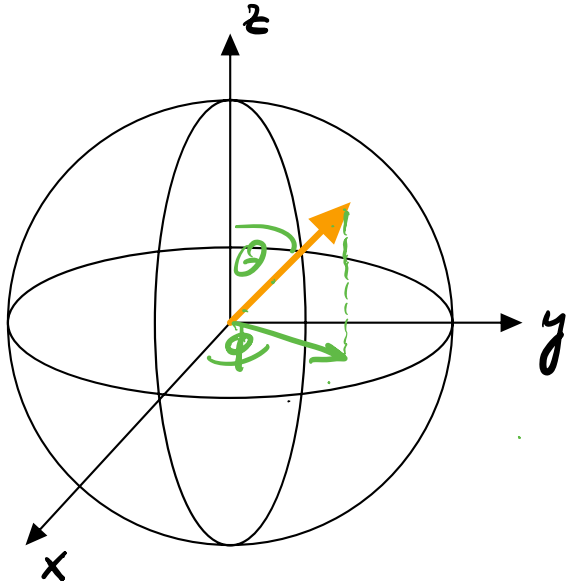
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

Define $\theta \in [0; \pi]$: $\cos \theta/2 = |\alpha|$; $\sin \theta/2 = |\beta|$.

Let $\alpha = e^{i\chi} |\alpha|$; $\beta = e^{i(\chi+\phi)} |\beta|$.

Then $|\psi\rangle = \underbrace{e^{i\chi}}_{\substack{\uparrow \\ \text{irrelevant} \\ \text{global phase}}} \underbrace{\left(\cos \theta/2 |0\rangle + e^{i\phi} \sin \theta/2 |1\rangle \right)}_{\substack{\downarrow \\ \text{depict on sphere'}}$



"Bloch sphere"

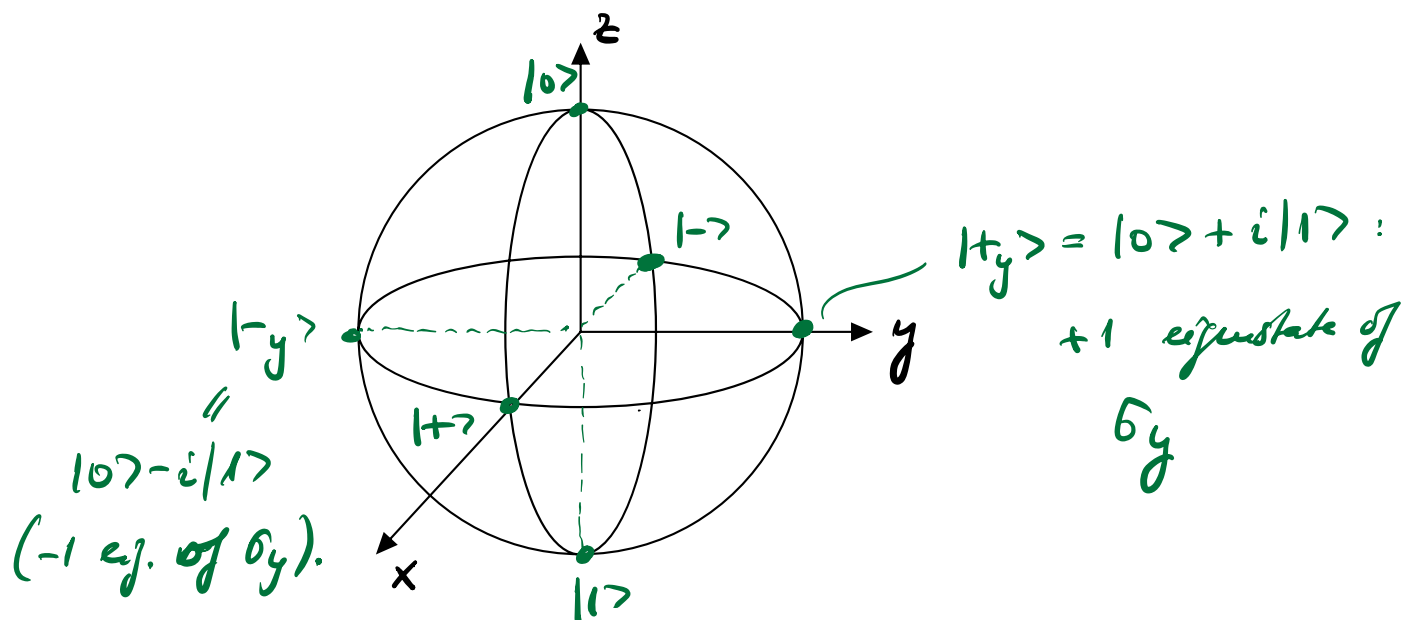
unit vector \vec{r} , $|\vec{r}| = 1$,
with angle θ to z axis
& angle ϕ in eq. plane
for x axis.

1-to-1 correspondence betw. states of qubit and points \vec{r} ("Bloch vector") on the sphere ("Bloch sphere").

Powerful visualization for qubit states.

Properties (just stated \rightarrow proof of HWork):

Important states:



Orthogonal states are anti-parallel on Bloch sphere.

For a state $|\psi\rangle$ w/ Bloch vector \vec{r} ,

$$\langle\psi|\sigma_i|\psi\rangle = r_i,$$

i.e. $|\psi\rangle$ can be interpreted as a spin $\frac{1}{2}$ pointing in direction \vec{r} (note that $\vec{S} = \frac{1}{2}\vec{\sigma}$ is the spin operator).

General hermitian matrix w/ eigenvalues ± 1 is of the form $\Pi = \underbrace{\vec{u} \cdot \vec{\sigma}}$, $\vec{u} \in \mathbb{R}^3$, $|\vec{u}| = 1$.

\uparrow Denotes $u_1 \sigma_1 + u_2 \sigma_2 + u_3 \sigma_3$
 $\equiv u_x \sigma_x + u_y \sigma_y + u_z \sigma_z$.

(Lesson: $\{I, \sigma_x, \sigma_y, \sigma_z\}$ is a basis of herm. matrices over \mathbb{R} , and all untx. over $\mathbb{C} \rightarrow$ cf. Homework.)

\Rightarrow eigenstates ± 1 of Π have Bloch vectors $\pm \vec{u}$.

Measurement of qubit:

Observable w/ eigenvalues ± 1 (most gen. up to shift & rescaling!) is of form $\Pi = \vec{u} \cdot \vec{\sigma}$, with eigenspace projectors $E_{\pm 1} = \frac{I \pm \vec{u} \cdot \vec{\sigma}}{2}$.

Prob. for outcome ± 1 is then

$$P_{\pm 1} = \langle \psi | E_{\pm 1} | \psi \rangle = \frac{1 \pm \vec{u} \cdot \vec{r}}{2}.$$

(Note: $\vec{u} \cdot \vec{r}$ is projection of \vec{r} onto axis \vec{u} !)

E.g. meas in z basis:

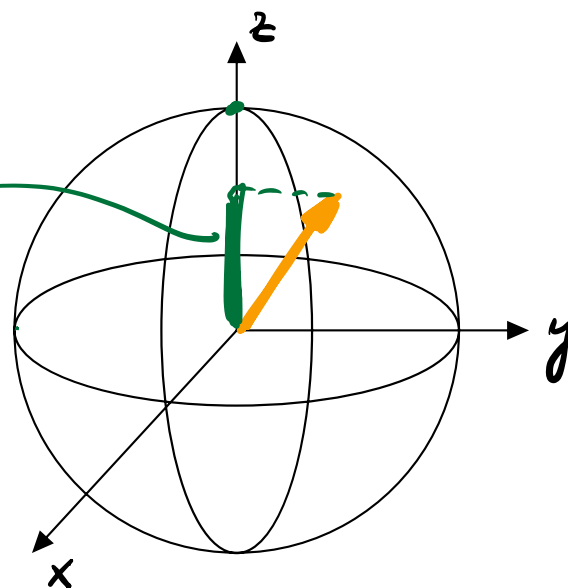
Result ± 1 w/ prob. $P_{\pm} = \frac{1 \pm r_z}{2}$

Projection onto \vec{u} : $\vec{u} \cdot \vec{r}$

Probability changes

linearly along z axis

for 1 to 0, or 0 to 1.



$$\Leftrightarrow P = \frac{1 \pm \vec{u} \cdot \vec{r}}{2}$$

Evolution:

Unitaries on qubits are of the form

$$U = e^{i\chi} \exp\left[-i \vec{\tau} \cdot \vec{\sigma} / 2\right]$$

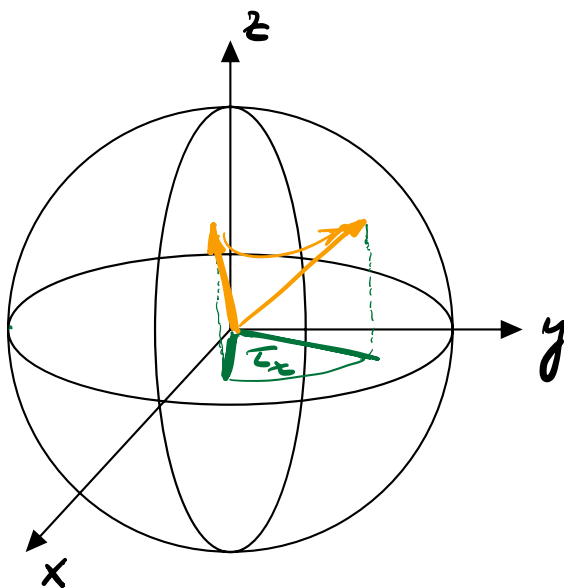
(Proof idea: Go from U to generator $G = G^\dagger$, $U = e^{-iG}$,

and write G as $G = \vec{u} \cdot \vec{\sigma} + c \cdot I$.)

on Bloch sphere:

U rotates Bloch vector by angle $|\vec{\tau}|$ about the axis $\vec{\tau}/|\vec{\tau}|$.

E.g.: $U_z(\tau_z) = \exp(-i \tau_z \sigma_z/2)$:



This is a manifestation of the double cover

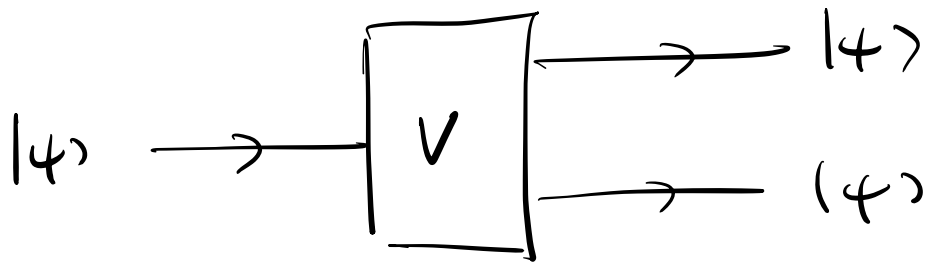
$$su(2)/\mathbb{Z}_2 \cong so(3)$$

(The $1/\mathbb{Z}_2$ comes from the fact that a 2π rotation gives $\exp(-2\pi i \sigma_z/2) = -I$)
↑ or other $\vec{\tau} \cdot \vec{\sigma}$, $|\vec{\tau}|=1$.

Question: What rotation is $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$?

e) A fundamental consequence: The no-cloning theorem³⁸

Given an unknown quantum state $|\psi\rangle \in \mathcal{H}$, can we build a device which does



i.e. a transformation

$$V: \mathcal{H} \rightarrow \mathcal{H} \otimes \mathcal{H}$$

$$|\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle \quad ?$$

How to build V - dim. of \mathcal{H} and $\mathcal{H} \otimes \mathcal{H}$ are different!

→ Add an auxiliary system ("ancilla") of same dimension:

$$U: \mathcal{H} \otimes \mathcal{H} \rightarrow \mathcal{H} \otimes \mathcal{H}$$

$$|\psi\rangle \otimes |0\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$$

↑ any suitable fiducial state

Note: $V := U(I_A \otimes |0\rangle_B)$ is an isometry:

$$\begin{aligned} V^\dagger V &= (\langle 0|_B \otimes I_A) \underbrace{U^\dagger U}_{I_{AB}} (I_A \otimes |0\rangle_B) \\ &= \langle 0|_B I_{AB} |0\rangle_B = I_A \end{aligned}$$

No-cloning - Theorem:

Quantum information cannot be copied, i.e. a

$$U: |\psi\rangle \otimes |0\rangle \mapsto |\psi\rangle \otimes |\psi\rangle \quad \otimes$$

cannot exist.

Proof: By contradiction:

$$U(|0\rangle \otimes |0\rangle) \stackrel{\otimes}{=} |0\rangle \otimes |0\rangle$$


$$U(|1\rangle \otimes |0\rangle) \stackrel{\otimes}{=} |1\rangle \otimes |1\rangle$$

$$\Rightarrow U\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle\right) = \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

A

But, from (*):

$$U \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle \right) = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$= \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$


→ Contradiction!

→ U cannot exist (note: we only used linearity!) □

Quantum information cannot be copied!

But; A classical copier is consistent w/
quantum theory, i.e. a device

$$U: |i\rangle \otimes |0\rangle \mapsto |i\rangle \otimes |i\rangle$$

for the comp. basis, or any other ONB $|i\rangle$.

(Proof: Homework)

2. Mixed States

I/41

a) The density operator

Consider a bipartite state $|\psi\rangle_{AB} = \sum c_{ij} |i\rangle |j\rangle$.

We have access to A only.

Can we characterize the measurement outcomes for meas. on A in a simple way?

(i.e. without having to consider B, which we anyway cannot access!)

Consider measurement operator Π .

(e.g. $\Pi = E_i$ projector, or exp. value, ...)

Measurement of $\Pi \equiv \Pi_A$ on A

\iff measurement of $\Pi_A \otimes I_B$ on $A \otimes B$.

$$\begin{aligned} \langle \psi | \Pi_A \otimes I_B | \psi \rangle &= \sum_{\substack{i,j \\ i',j'}} \overline{c_{i'j'}} \langle i' | \langle j' | (\Pi_A \otimes I_B) | i \rangle | j \rangle c_{ij} \\ &= \sum \overline{c_{i'j'}} c_{ij} \langle i' | \Pi_A | i \rangle \underbrace{\langle j' | j \rangle}_{= \delta_{j'j}} \end{aligned}$$

$$= \sum_{ii'} \left(\sum_j \overline{c_{ij}} c_{ij} \right) \langle i' | \Pi_A | i \rangle = (*)$$

Now: Define P_A - a $d_A \times d_A$ matrix - via

$$(P_A)_{ii'} = \sum_j c_{ij} \overline{c_{ij'}} = (C \cdot C^\dagger)_{ii'},$$

with the matrix $C = (c_{ij})_{ij}$,

or equivalently $P_A = \sum_{i,i',j} c_{ij} \overline{c_{ij'}} |i\rangle\langle i'|$

and introduce the trace

$$\text{tr}(X) = \sum_k \langle k | X | k \rangle$$

can be any ONB,
not necessarily comp.
basis.

Note: The trace is

• cyclic: $\text{tr}(AB) = \sum_k \langle k | AB | k \rangle$

$$= \sum_k \langle k | A \left(\sum_e |e\rangle\langle e| \right) B | k \rangle$$

$$= \sum_{ke} \langle k | A | e \rangle \langle e | B | k \rangle$$

$$= \sum_{ke} \langle e | B | k \rangle \langle k | A | e \rangle = \text{tr}(BA)$$

Note: A, B

need not
be square!

- and thus basis-independent:

$$\text{tr}(u^\dagger X u) = \text{tr}(X u u^\dagger) = \text{tr}(X),$$

and thus $\text{tr}(X) = \sum \langle k | X | k \rangle$

$$= \sum \underbrace{(\langle k | u^\dagger)}_{\langle v_k |} X \underbrace{(u | k \rangle)}_{| v_k \rangle}$$

$$= \sum \langle v_k | X | v_k \rangle \text{ for any ONB,}$$

- the sum of the eigenvalues:

$$\text{tr}(X) = \text{tr}(X A A^\dagger) = \text{tr}(A^\dagger X A),$$

with $A^\dagger X A$ the eigenvalue decomposition.

- and of course linear:

$$\text{tr}(A) + \lambda \text{tr}(B) = \text{tr}(A + \lambda B).$$

Then,

$$\begin{aligned}
 (*) &= \sum_{ii'} \left(\sum_j \overline{c_{ij'}} c_{ij} \right) \langle i' | \Pi_A | i \rangle \\
 &= \sum_{ii'} \left(\sum_j \overline{c_{ij'}} c_{ij} \right) \text{tr} \left[\langle i' | \Pi_A | i \rangle \right] \quad \text{trace of a number is itself!} \\
 &= \sum_{ii'} \left(\sum_j c_{ij} \overline{c_{ij'}} \right) \text{tr} \left[|i\rangle \langle i'| \Pi_A \right] \quad \text{cyclicity of trace!} \\
 &\stackrel{\text{linearity of trace!}}{=} \text{tr} \left[\underbrace{\left(\sum_{ii'} c_{ij} \overline{c_{ij'}} |i\rangle \langle i'| \right)}_{= P_A} \Pi_A \right] \\
 &= P_A
 \end{aligned}$$

$$= \text{tr} [P_A \Pi_A].$$

i.e.: $\langle \psi | \Pi_A \otimes I_B | \psi \rangle = \text{tr} [P_A \Pi_A],$

where $P_A = \sum_{ii'} c_{ij} \overline{c_{ij'}} |i\rangle \langle i'|,$

or $P_A = C C^\dagger$, with $C = (c_{ij})_{ij}.$

ρ_A is called the density operator, density matrix^{IX.45}, or mixed state. It characterizes systems where we only have partial knowledge, such as access to only part of the system.

In contrast, a state $|\psi\rangle \in \mathcal{H}$ is called a pure state.

If we want to highlight that ρ_A comes from a larger system, we can also refer to it as the reduced density matrix of system A.

Properties of ρ_A :

- $\rho_A = CC^\dagger \Rightarrow \rho_A^\dagger = (CC^\dagger)^\dagger = CC^\dagger = \rho_A$

- ρ_A is positive semidefinite:

$$\begin{aligned}\langle \phi | \rho_A | \phi \rangle &= \langle \phi | CC^\dagger | \phi \rangle = (C^\dagger | \phi \rangle)^\dagger \underbrace{(C^\dagger | \phi \rangle)}_{=: |\phi'\rangle} \\ &= \langle \phi' | \phi' \rangle \geq 0 \quad \forall \phi.\end{aligned}$$

We write $\rho_A \geq 0$.

Note: $X \geq 0$, i.e. $\langle \phi | X | \phi \rangle \geq 0 \quad \forall |\phi\rangle$

$$\iff X = X^\dagger \text{ \& all eigenvalues of } X \text{ are } \geq 0.$$

(In part., $X \geq 0 \Rightarrow X = X^\dagger$)

$$\bullet \operatorname{tr}(\rho_A) = \sum_i (C C^\dagger)_{ii} = \sum_{ij} c_{ij} \bar{c}_{ij} = \sum |c_{ij}|^2 = 1. \quad \text{I/46}$$

Properties of density operators:

- $\rho_A \geq 0$ (implies $\rho_A = \rho_A^\dagger$)
- $\operatorname{tr}(\rho_A) = 1.$

Will see soon: This provides an alternative fundamental definition of a state — i.e., any ρ_A with the properties above can arise if we only have access to part of the system.

Note: All ρ_A with the above property form a convex set S , i.e.:

$$\rho, \sigma \in S \Rightarrow p\rho + (1-p)\sigma \in S, \quad 0 \leq p \leq 1.$$

Is there an ambiguity in ρ_A , just as the phase ambiguity for pure states?

Theorem: ρ_A is uniquely determined by all measurement outcomes $\text{tr}[\rho_A \Pi]$ for $\Pi = \Pi^\dagger$.

(i.e., by all overlaps, though probabilities, i.e. Π orth. proj., also suffices.)

Proof: Let $V = \{ \Pi \mid \Pi = \Pi^\dagger \}$. V is a vector space over \mathbb{R} .

$(\Pi, N) := \text{tr}[\Pi^\dagger N]$ defines a scalar product on V (the "Hilbert-Schmidt scalar product").

Pick an ONB $\{ \Pi_i \}$ of V , $\text{tr}[\Pi_i^\dagger \Pi_j] = \delta_{ij}$.

Then, the map $X \mapsto \sum \Pi_i \text{tr}[\Pi_i^\dagger X]$
 $= \sum \Pi_i (\Pi_i, X)$

acts as the identity on V . Thus,

$$\rho_A = \sum \Pi_i \text{tr}[\Pi_i \rho_A],$$

i.e., ρ_A is fully specified by all meas. outcomes

(and thus, there must be a unique ρ_A for any given physical state. \square)

(Note: We didn't really use that we have hermitian matrices — the same ideas work for $V_{\mathbb{C}} = \{\pi\}$ over \mathbb{C} . Then the \cdot^+ are important — and we must show that $V_{\mathbb{C}}$ has a hermitian basis over \mathbb{C} — which it does.)

In particular: No ambiguity in P_A
 \Rightarrow all numbers meaningful!

Where did the phase $|\psi_A\rangle \sim e^{i\phi}|\psi_A\rangle$ go?

Density matrix for a pure state $|\psi_A\rangle$:

$$\langle \psi_A | \pi | \psi_A \rangle = \text{tr}[\langle \psi_A | \pi | \psi_A \rangle]$$

number
↓

$$= \text{tr}[\pi \underbrace{|\psi_A\rangle\langle\psi_A|}_{=P_A}]$$

cyc.

$$\Rightarrow P_A = |\psi_A\rangle\langle\psi_A| : \text{projector onto } |\psi_A\rangle.$$

(Phase naturally drops out!)

b) The partial trace

Just seen: Pure state on $AB \rightarrow$ Mixed state on A .

What if AB itself is already mixed
(e.g. from a pure ABC ?)

Same approach: How to describe most general measurement on A , given a state ρ_{AB} ?

$$\text{tr}[(\Pi_A \otimes I_B) \rho_{AB}] = \sum \underbrace{\langle ij | \Pi \otimes I | i'j' \rangle}_{=\delta_{jj'}} \langle i'j' | \rho_{AB} | ij \rangle$$

$$= \sum_{ii'} \langle i | \Pi | i' \rangle \langle i'j' | \rho_{AB} | ij \rangle$$

$$= \text{tr} \left[\Pi \cdot \left(\sum_{ii'} |i'\rangle_A \langle i'j' | \rho_{AB} | ij \rangle \langle i | \right) \right]$$

$$= \text{tr}[\Pi \cdot \rho_A]$$

where we define

$$\rho_A = \sum |i'\rangle_A \langle i'j' | \rho_{AB} | ij \rangle \langle i |$$

$$= \sum_j (I_A \otimes \langle j|_B) \rho_{AB} (I_A \otimes |j\rangle_B)$$

$$= \sum_j \langle j|_B \rho_{AB} |j\rangle_B$$

$$=: \text{tr}_B(\rho_{AB}) : \text{ the } \underline{\text{"partial trace"}}$$

In components:

$$(\text{tr}_B(\rho_{AB}))_{ii'} = \langle i|_A \left(\sum_j \langle j|_B \rho_{AB} |j\rangle_B \right) |i'\rangle$$

$$= \sum_j (\rho_{AB})_{(ij), (i'j)}$$

(Note: The partial trace can also be seen as the canonical extension of

$$\text{tr}: B(\mathcal{H}_A) \rightarrow \mathbb{C}$$

into $B(\mathcal{H}_A) \otimes B(\mathcal{H}_B)$

linear ("bounded") operators on \mathcal{H}_A .

Note: ρ_A is also called reduced density matrix (or operator) of ρ_{AB} (or $|\psi_{AB}\rangle$).

c) Purifications

Is any density matrix ρ ($\rho \geq 0$, $\text{tr} \rho = 1$) physical (i.e., coming from a pure state, as by our axioms)?

Purification of mixed state ρ :

Consider any decomposition $\rho = \sum \lambda_i |\phi_i\rangle\langle\phi_i|$, $\lambda_i \geq 0$, e.g. the eigenvalue decomposition, and define

$$|\psi\rangle_{AB} := \sum \sqrt{\lambda_i} |\phi_i\rangle_A |i\rangle_B$$

any ONB

$$\text{Then } \text{tr}_B[|\psi\rangle\langle\psi|] = \text{tr}_B\left[\sum_{ij} \sqrt{\lambda_i \lambda_j} |\phi_i\rangle\langle\phi_j| \otimes |i\rangle\langle j|\right]$$

$$= \sum_{ij} \sqrt{\lambda_i \lambda_j} |\phi_i\rangle\langle\phi_j| \otimes \underbrace{\text{tr}_B[|i\rangle\langle j|]}_{= \delta_{ij}}$$

$$= \sum \lambda_i |\phi_i\rangle\langle\phi_i| = \rho$$

Yes, every ρ is physical (in the sense above).

\Rightarrow Density operator ρ can serve as an alternative fundamental definition of a state in quantum theory.

Definition: A $|\psi\rangle_{AB}$ s.t. $\text{tr}_B(|\psi\rangle\langle\psi|) = \rho$ is called a purification of ρ .

Note: The ambiguity of purifications - i.e., how are two purifications $|\psi\rangle, |\phi\rangle$ of ρ , $\text{tr}_B(|\psi\rangle\langle\psi|) = \text{tr}_B(|\phi\rangle\langle\phi|) = \rho$, related - will be addressed later.

d) Ensemble interpretation of the density matrix ^{I/53}

Consider $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$:

$$\Rightarrow \rho_A = \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix} = |\alpha|^2 |0\rangle\langle 0| + |\beta|^2 |1\rangle\langle 1|$$

$$\Rightarrow \text{tr}[\Pi \rho_A] = |\alpha|^2 \langle 0|\Pi|0\rangle + |\beta|^2 \langle 1|\Pi|1\rangle.$$

\Rightarrow Can be interpreted as having the pure state $|0\rangle$ with probability $p_0 = |\alpha|^2$, and $|1\rangle$ w/ $p_1 = |\beta|^2$.

"ensemble interpretation" of density matrix

However: We have derived ρ_A from a pure state

$|\psi\rangle_{AB}$ — are these two perspectives consistent?

Imagine B does a measurement in the Z basis:

$$\begin{array}{l} |\psi\rangle = \alpha|00\rangle + \beta|11\rangle \\ \begin{array}{l} p_0 = |\alpha|^2 \rightarrow |\psi_0\rangle_A = |0\rangle_A \\ p_1 = |\beta|^2 \rightarrow |\psi_1\rangle_A = |1\rangle_A \end{array} \end{array}$$

I/54

The post-measurement state of Alice is $|\psi_0\rangle = |0\rangle$
with $p_0 = |\alpha|^2$, and $|\psi_1\rangle = |1\rangle$ with $p_1 = |\beta|^2$.

But: Alice does not know outcome of Bob

\Rightarrow meas. of B produces an ensemble

$$\{ (p_0, |0\rangle), (p_1, |1\rangle) \} =$$

$$= p_0 |0\rangle\langle 0| + p_1 |1\rangle\langle 1| = \begin{pmatrix} p_0 & \\ & p_1 \end{pmatrix} = \begin{pmatrix} |\alpha|^2 & \\ & |\beta|^2 \end{pmatrix}.$$

(But note: Bob knows outcome \Rightarrow his description
is different: he would describe Alice's state
either as $|0\rangle\langle 0|$ or as $|1\rangle\langle 1|$!

i.e.: State assigned dep. on knowledge!

But: Bob could also measure in different bases,
e.g. $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$!

I/55

$$p_+ = \frac{|\alpha|^2 + |\beta|^2}{2} = \frac{1}{2} \rightarrow |\psi_+\rangle_A = \frac{\alpha|0\rangle + \beta|1\rangle}{|\alpha|^2 + |\beta|^2}$$

$$|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$$

X-meas.
on B

$$p_- = \frac{|\alpha|^2 + |\beta|^2}{2} = \frac{1}{2} \rightarrow |\psi_-\rangle_A = \frac{\alpha|0\rangle - \beta|1\rangle}{|\alpha|^2 + |\beta|^2}$$

non-orthogonal!

Ensemble $\{(p_+, |\psi_+\rangle), (p_-, |\psi_-\rangle)\}$

Indeed, $p_+ |\psi_+\rangle \langle \psi_+| + p_- |\psi_-\rangle \langle \psi_-| = \rho_A!$

Different ensemble for same state

\Rightarrow ensemble interpretation is ambiguous!

(Even # of terms can vary, etc. \rightarrow HWS)

Definition: We call a system (or a collection of systems) which is in state $|\psi_i\rangle$ (or ρ_i) with prob. p_i an ensemble. (We write $\{(p_i, |\psi_i\rangle)\}$, or $\{(p_i, \rho_i)\}$).

Observation: Measurement outcomes for an ensemble^{7/56}

$\{p_i, \rho_i\}$ are described by

$$\begin{aligned} \langle \rho \rangle &:= \sum p_i \operatorname{tr}[\rho_i] = \operatorname{tr}[\rho] \quad \underbrace{\left(\sum p_i \rho_i \right)}_{=:\rho} \\ &\uparrow \\ &\text{avg.} \end{aligned} = \operatorname{tr}[\rho]$$

\Rightarrow Different ensembles $\sum p_i \rho_i = \sum p'_i \rho'_i$ are indistinguishable.

How are two different ensemble decompositions related?

Theorem: $\sum_i p_i |\psi_i\rangle\langle\psi_i| = \sum_j q_j |\phi_j\rangle\langle\phi_j|$

\curvearrowright no need for orth.!!

if and only if there exists $U = (u_{ij})$ s.t.

$$\sqrt{p_i} |\psi_i\rangle = \sum_j u_{ij} \sqrt{q_j} |\phi_j\rangle,$$

where $U = (u_{ij})$ satisfies

(i) If $\sum q_j |\phi_j\rangle\langle\phi_j|$ is an eigenvalue decomposition:
and all $q_j \neq 0$:

$$U^\dagger U = I, \text{ i.e. } U \text{ is an isometry}$$

(ii) general case: $U = V \cdot W^\dagger$, $V^\dagger V = W^\dagger W = I$, i.e.,
 U is a partial isometry
(i.e. $U^\dagger U$, $U U^\dagger$ are projections)

Proof: We will first prove case (i).

" \Leftarrow ": Let $\sqrt{p_i} |\psi_i\rangle = \sum_j u_{ij} \sqrt{q_j} |\phi_j\rangle$.

$$\begin{aligned} \text{Then } \sum_i p_i |\psi_i\rangle\langle\psi_i| &= \sum_i \left(\sum_j u_{ij} \sqrt{q_j} |\phi_j\rangle \right) \left(\sum_{j'} \overline{u_{ij'}} \sqrt{q_{j'}} \langle\phi_{j'}| \right) \\ &= \sum_{jj'} \sqrt{q_j} |\phi_j\rangle\langle\phi_{j'}| \sqrt{q_{j'}} \underbrace{\left(\sum_i \overline{u_{ij'}} u_{ij} \right)}_{(U^\dagger U)_{j'j} = \delta_{j'j}} \\ &= \sum_j q_j |\phi_j\rangle\langle\phi_j|. \end{aligned}$$

" \Rightarrow ": Assume $|\phi_j\rangle$ is an eigenbasis of p .
Recall that all $q_j \neq 0$.

Define $u_{ij} = \langle \phi_j | \psi_i \rangle \frac{\sqrt{p_i}}{\sqrt{q_j}}$.

Then,
$$\sum_j u_{ij} \sqrt{q_j} |\phi_j\rangle = \sum_j \sqrt{q_j} |\phi_j\rangle \langle \phi_j | \psi_i \rangle \frac{\sqrt{p_i}}{\sqrt{q_j}}$$

$$= \sqrt{p_i} |\psi_i\rangle,$$

and
$$\sum_i u_{ij} \overline{u_{ij'}} = \sum_i \langle \phi_j | \psi_i \rangle \langle \psi_i | \phi_{j'} \rangle \frac{p_i}{\sqrt{q_j q_{j'}}$$

$$= \underbrace{\langle \phi_j | \sum_i p_i |\psi_i\rangle \langle \psi_i|}_{= q_j \delta_{jj'}} | \phi_{j'} \rangle \frac{1}{\sqrt{q_j q_{j'}}} = \delta_{jj'}$$

$\Rightarrow (u_{ij})$ is an isometry.



General case: First, restrict to $\text{supp}(p)$, since all $|\phi_j\rangle, |\psi_i\rangle \in \text{supp}(p)$; then, all $q_i, p_j \neq 0$. Then, take

$$\sum p_i |\psi_i\rangle \langle \psi_i| \xleftrightarrow{v_{ik}} \underbrace{\sum r_k |e_k\rangle \langle e_k|}_{\text{eigenbasis}} \xleftrightarrow{w_{jk}} \sum q_j |\phi_j\rangle \langle \phi_j|$$

& combine the isometries v_{ik} & w_{jk}

→ Homework



e) Unitary evolution & projective measurement for mixed states

How does a mixed state evolve under a unitary U ?

— Can be assessed in diff. ways, e.g. through purifications (here), or ensemble interpretation, or "Heisenberg picture" (= evolving meas. operators).

Consider state ρ & unitary U .

Let $|\psi\rangle = |\psi\rangle_{AB}$ be a purification of ρ ,

$$\text{tr}_B | \psi \rangle \langle \psi | = \rho_A.$$

Then, $| \psi \rangle \longmapsto (U_A \otimes I_B) | \psi \rangle$

$$\Rightarrow \rho_A = \text{tr}_B | \psi \rangle \langle \psi |$$

$$\longmapsto \text{tr}_B \left[(U_A \otimes I_B) | \psi \rangle \langle \psi | (U_A^\dagger \otimes I_B) \right]$$

$$= U_A \text{tr}_B \left[(I_A \otimes I_B) | \psi \rangle \langle \psi | (I_A \otimes I_B) \right] U_A^\dagger$$

$$= U_A \rho_A U_A^\dagger.$$

How does proj. measurement $\{E_u\}$ act on ρ_A ?

By construction of ρ_A , $p_u = \text{tr} [E_u \rho_A]$.

Post-meas. state:

$$\rho_{A,u} = \frac{1}{p_u} \text{tr}_B \left[(E_u \otimes I) | \psi \rangle \langle \psi | (E_u^\dagger \otimes I) \right]$$

$$= \frac{1}{p_u} E_u \rho_A E_u^\dagger.$$

□

(Note: Both derivations indep. of chosen purification
 \rightarrow well-defined.)

3. The Schmidt decomposition & purifications

a) The Schmidt decomposition

Consider a bipartite state $|\psi\rangle_{AB}$, and let

$$\text{tr}_B |\psi\rangle\langle\psi| = \rho_A = \sum_i p_i |a_i\rangle\langle a_i| \text{ be the}$$

eigenvalue decomposition (including $p_i = 0$),
i.e. $|a_i\rangle_A$ is an ONB.

Let $|x_i\rangle_B$ be any ONB of B , and expand

$$|\psi\rangle_{AB} \text{ in } |a_i\rangle_A |x_j\rangle_B:$$

$$|\psi\rangle_{AB} = \sum c_{ij} |a_i\rangle_A |x_j\rangle_B$$

$$= \sum |a_i\rangle_A |\tilde{b}_i\rangle_B$$

$$\text{with } |\tilde{b}_i\rangle_B := \sum_j c_{ij} |x_j\rangle_B.$$

↖ no ONB etc. (a priori)

We have

I/62

$$\begin{aligned}\sum p_i |a_i \chi_{a_i}| &= \text{tr}_0 |\psi \chi \psi| \\ &= \text{tr}_0 \left[\sum_{i,i'} |a_i \chi_{a_i}|_A \otimes |\tilde{b}_i \chi_{\tilde{b}_i}|_B \right] \\ &= \sum_{i,i'} |a_i \chi_{a_i}| \text{tr} [|\tilde{b}_i \chi_{\tilde{b}_i}|_B] \\ &= \sum \langle \tilde{b}_{i'} | \tilde{b}_i \rangle |a_i \chi_{a_i}| \end{aligned}$$

Since the $|a_i \chi_{a_i}| \forall i'$ are lin. indep.

(in fact, H-S-orthonormal!), we must have

$$\langle \tilde{b}_{i'} | \tilde{b}_i \rangle = p_i \delta_{ii'} !$$

\Rightarrow For all i s.t. $p_i \neq 0$:

$$|b_i\rangle_B := \frac{1}{\sqrt{p_i}} |\tilde{b}_i\rangle_B \text{ are } \underline{\text{orthonormal!}}$$

\Rightarrow

$$|\psi\rangle_{AB} = \sum_{i: p_i \neq 0} \sqrt{p_i} |a_i\rangle_A |b_i\rangle_B$$

with $\{|a_i\rangle_A\}, \{|b_i\rangle_B\}$ orthonormal!

(Note: Can be padded w/ $i: p_i = 0$ as long as \mathcal{H}_B is large enough.)

Definition: A decomposition $|\psi\rangle_{AB} = \sum p_i |a_i\rangle_A |b_i\rangle_B$ with ONS $\{|a_i\rangle_A\}$, $\{|b_i\rangle_B\}$, $p_i \geq 0$, is called Schmidt decomposition of $|\psi\rangle_{AB}$, with Schmidt coefficients p_i . The number of non-zero p_i is called Schmidt rank (or Schmidt number).

Theorem: Any bipartite state $|\psi\rangle_{AB}$ has a Schmidt decomposition, i.e. there exist p_i and ONS $\{|a_i\rangle_A\}$ and $\{|b_i\rangle_B\}$ s.t. $|\psi\rangle_{AB} = \sum p_i |a_i\rangle_A |b_i\rangle_B$.

(Proof: Construction from before.)

Note: $p_B = \text{tr}_A |\psi\rangle\langle\psi| = \sum_i p_i |b_i\rangle\langle b_i|$, and (by construction) $p_A = \sum_i p_i |a_i\rangle\langle a_i|$.

- \Rightarrow
- (i) $\{|a_i\rangle_A\}$ and $\{|b_i\rangle_B\}$ are the eigenbases of p_A & p_B (except $p_i = 0$), respectively.
 - (ii) p_A & p_B have the same eigenvalues (!).
 - (iii) If the p_i are non-degenerate, the

Schmidt decomp. can be found by simply piling up the eigenvectors of P_A & P_B !

(iv) $\{|a_i\rangle_A\}$ and $\{|b_i\rangle_B\}$ ($p_i \neq 0$) are ONBs of $\text{supp } P_A$ and $\text{supp } P_B$, respectively.

(Note: If $\dim A = \dim B$, we can include the zero eigenvalues & extend $\{|a_i\rangle_A\}$, $\{|b_i\rangle_B\}$ to ONBs of the full space.)

Notational convention:

Often, the bases $\{|a_i\rangle_A\}$ and $\{|b_i\rangle_B\}$ are simply denoted as

$$|i\rangle_A := |a_i\rangle_A, \text{ and}$$

$$|i\rangle_B := |b_i\rangle_B.$$

These are not the computational basis, and generally different bases on A & $B \Rightarrow$ CAREFUL!!

How is the Schmidt decomposition related to expansion of $|\psi\rangle$ in a different pair of orbs $\{|x_i\rangle_A\}, \{|y_j\rangle_B\}$?

$$\begin{aligned} \text{We have } |\psi\rangle &= \sum c_{ij} |x_i\rangle_A |y_j\rangle_B \\ &= \sum \sqrt{p_k} |a_k\rangle_A |b_k\rangle_B. \end{aligned} \quad (*)$$

\Rightarrow There exist matrices $U=(u_{ik}), V=(v_{jk})$ s.t.

$$|a_k\rangle_A = \sum u_{ik} |x_i\rangle_A, \quad |b_k\rangle_B = \sum \overline{v_{jk}} |y_j\rangle_B,$$

$$\begin{aligned} \text{and } \delta_{ke} &= \langle a_k | a_e \rangle = \sum_{ij} \overline{u_{ik}} u_{je} \underbrace{\langle x_i | x_j \rangle}_{=\delta_{ij}} \\ &= \sum \overline{u_{ik}} u_{ie} = (u^\dagger u)_{ke}, \end{aligned}$$

$$\text{and equally } (V^\dagger V)_{ke} = \delta_{ke}$$

$\Rightarrow U, V$ are isometries.

If we insert this in (*):

$$\sum_{ij} c_{ij} |x_i\rangle_A \langle y_j|_B = \sum_{ij} \sum_k \sqrt{p_k} u_{ik} \overline{v_{jk}} \underbrace{|x_i\rangle_A \langle y_j|_B}_{\substack{\uparrow \\ \text{lin. indep.}}}$$

$$\Rightarrow c_{ij} = \sum_k \sqrt{p_k} u_{ik} \overline{v_{jk}} \quad \forall i, j, \quad \text{or}$$

Theorem:

Any matrix $C = (c_{ij})$, $i=1, \dots, u$, $j=1, \dots, u$,
can be written in the form

$$C = U \cdot D \cdot V^+, \quad \text{or}$$

$$c_{ij} = \sum_{k=1}^r \lambda_k u_{ik} \overline{v_{jk}}$$

with $r = \text{rank}(C) \leq u, u$, $\lambda_k > 0$, and

$$U = (u_{ik}), \quad V = (v_{jk}), \quad D = \begin{pmatrix} \lambda_1 & \lambda_2 & & 0 \\ & \ddots & & \\ 0 & & \lambda_r & \\ & & & \ddots \end{pmatrix},$$

$i=1, \dots, u$; $k=1, \dots, r$; $j=1, \dots, u$, and

$$U^+ U = I_r, \quad V^+ V = I_r \quad \text{isometries.}$$

This is called the singular value decomposition (SVD) of C ,
with singular values λ_i .

If the λ_i are ordered descendingly,
 $\lambda_1 \geq \lambda_2 \geq \dots$, U and V are unique up
to sign choices in subspaces with degenerate
singular values.

Alternatively, one can choose U and V
square $n \times n$ and $m \times m$ unitaries, and

$$D = \left(\begin{array}{cc|c} \lambda_1 & & 0 \\ & \ddots & \\ & & \lambda_r & 0 \\ \hline 0 & & & 0 \end{array} \right),$$

but the additional degrees of freedom are
arbitrary.

Proposition: Any two states $|\phi\rangle, |\psi\rangle$ with identical Schmidt coefficients $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_r > 0$ are related by local unitaries, i.e.

$$\exists U, V: |\phi\rangle = (U \otimes V) |\psi\rangle.$$

Thus: The ordered Schmidt coefficients $\lambda_1 \geq \lambda_2 \geq \dots$ encode all non-local properties.

Proof: $|\phi\rangle = \sum_{i=1}^r \lambda_i |\phi_i^A\rangle \otimes |\phi_i^B\rangle$

$$|\psi\rangle = \sum_{i=1}^r \lambda_i |\psi_i^A\rangle \otimes |\psi_i^B\rangle$$

$\{|\phi_i^A\rangle\}, \{|\psi_i^A\rangle\}$ orthonormal $\Rightarrow \exists U: |\phi_i^A\rangle = U |\psi_i^A\rangle \forall i.$

$\{|\phi_i^B\rangle\}, \{|\psi_i^B\rangle\}$ orthonormal $\Rightarrow \exists V: |\phi_i^B\rangle = V |\psi_i^B\rangle \forall i.$



(Note that also vice versa, the Schmidt coefficients cannot be changed at all by local unitaries - all information in them is non-local.)

b) Purifications (again)

Reminder: Given ρ_A on A , a state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$

s.t. $\text{tr}_B |\psi\rangle\langle\psi| = \rho_A$ is called a purification of ρ_A .

Given two purifications

$$|\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$$

$$|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_{B'}$$

potentially
different spaces

of ρ_A , what is their relation?

Write both $|\phi\rangle$ and $|\psi\rangle$ in their Schmidt form
(not a basis basis!):

$$|\phi\rangle = \sum \lambda_i |\phi_i^A\rangle |\phi_i^B\rangle$$

$$|\psi\rangle = \sum \mu_i |\psi_i^A\rangle |\psi_i^{B'}\rangle$$

(wlog λ_i, μ_i descending; $\dim B' \geq \dim B$.)

We have

$$\begin{aligned}\sum \lambda_i^2 |\phi_i^A\rangle\langle\phi_i^A| &= \text{tr}_B |\phi\rangle\langle\phi| = \rho_A = \\ &= \text{tr}_B |\psi\rangle\langle\psi| = \sum \mu_i^2 |\psi_i^A\rangle\langle\psi_i^A|\end{aligned}$$

$|\phi_i^A\rangle, |\psi_i^A\rangle$ orthonormal

\Rightarrow if λ_i, μ_i non-degenerate, then

$$\lambda_i = \mu_i, \quad |\phi_i^A\rangle = |\psi_i^A\rangle \quad \forall i$$

(If degen.: Schmidt decomp. can be constructed from any eigendecomposition $\sum \lambda_i |\phi_i\rangle\langle\phi_i|$ of ρ_A - see sec. a) - so we can construct it with the same eigenvectors $|\phi_i^A\rangle = |\psi_i^A\rangle$.)

Now construct a $U: \mathcal{H}_B \rightarrow \mathcal{H}_B$

$$\text{s.t.} \quad |\phi_i^B\rangle \mapsto |\psi_i^{B'}\rangle,$$

U is a unitary between span $\{|\phi_i^B\rangle\}$

and span $\{|\psi_i^{B'}\rangle\}$. If $\dim B' > \dim B$,
it can be extended to an isometry. Then:

$$|\psi\rangle = (I_A \otimes U_B) |\phi\rangle.$$

Theorem: All purifications of a given ρ_A are
related by a unitary (or isometry) on the
purifying system.

Note: This is closely linked to the unitary/
isometric ambiguity of the ensemble decomposition:

Any ensemble $\rho = \sum p_i |\phi_i\rangle\langle\phi_i|$ is related
← not an ONS

to a purification $|\psi\rangle = \sum \sqrt{p_i} |\phi_i\rangle_A |i\rangle_B$,

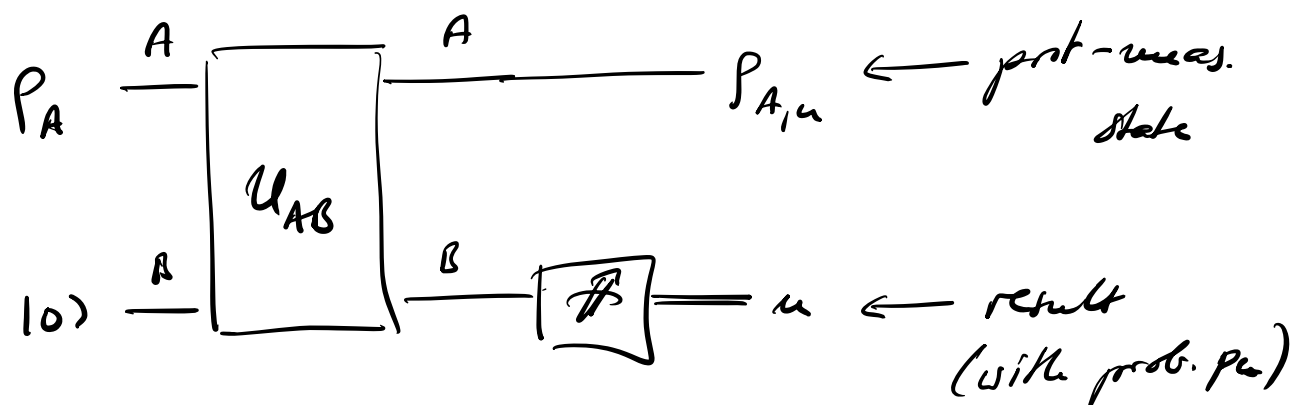
from where it can be obtained by measuring B
in the computational basis.

4. POVM measurements

Seen previously: Adding a 2nd system B gives more rich situation.

Then natural question: What measurements can we do by adding an extra system?

- Idea:
- i) Add auxiliary system ("ancilla") B in state $|0\rangle$
 - ii) Act w/ unitary U_{AB} on system + ancilla
 - iii) measure B in $\{|0\rangle, |1\rangle, \dots, |d_B-1\rangle\}$



Analyze scheme:

Post-meas. state (unnormalized) is:

$$\tilde{\rho}_u^A = \langle u |_B U (\rho_A \otimes |0\rangle\langle 0|_B) U^\dagger |u\rangle_B$$

$$= \langle u |_B \langle u |_B \rangle_B \quad P_A \langle 0 |_B \langle u ^\dagger |_B \rangle_B$$

$$= \Pi_u P_A \Pi_u^\dagger,$$

where we have defined

$$\Pi_u := \langle u |_B \langle u |_B \rangle_B \equiv (I_A \otimes \langle u |_B) U (I_A \otimes |0\rangle_B)$$

Then, $p_u = \text{tr} \tilde{p}_u^A = \text{tr} (\Pi_u P_A \Pi_u^\dagger) = \text{tr} (\Pi_u^\dagger \Pi_u P_A)$,

is the probability for outcome u ,

and $\tilde{p}_u^A = \frac{1}{p_u} \Pi_u^\dagger \Pi_u \tilde{p}_u^A$ the post-measurement state.

It holds that

$$\sum_u \Pi_u^\dagger \Pi_u = \sum_u \langle 0 |_B \langle u ^\dagger |_B \rangle_B \langle u |_B \langle u |_B \rangle_B$$

$$= \langle 0 |_B \langle u ^\dagger u |_B \rangle_B$$

$$= I_A,$$

and further $\Pi_u^\dagger \Pi_u \geq 0$.

(Note: The former implies

$$\sum p_u = \sum \text{tr} (\Pi_u^\dagger \Pi_u \rho) = \text{tr} (\sum \Pi_u^\dagger \Pi_u \rho) = \text{tr} (\rho) = 1).$$

Definition: A set $\{F_u\}$ of operators, $F_u \geq 0$,

$\sum F_u = I$, is called a positive operator-valued

measure (POVM).

Note: $F_u := \Pi_u^\dagger \Pi_u$ forms a POVM. If we only

care about the post-meas. prob. $p_u = \text{tr}(F_u \rho)$,

then the measurement is fully characterized by

the POVM $\{F_u\}$.

Definition: A POVM measurement is given by

a set of operators $\{\Pi_u\}$ with $\sum \Pi_u^\dagger \Pi_u = I$,

with outcome probabilities $p_u = \text{tr}(\Pi_u^\dagger \Pi_u \rho)$

and post-measurement states $\rho_u = \frac{1}{p_u} \Pi_u \rho \Pi_u^\dagger$.

Alternative Definition: A POVM measurement is

given by a set of operators $\{F_u\}$, $F_u \geq 0$, $\sum F_u = I$,

with outcome probabilities $p_u = \text{tr}(F_u \rho)$.

Relation of the two definitions, & with the initial ^{I/75} unitary + ancilla construction:

i) Can any $F_n \geq 0$ be written as $F_n = \Pi_n^\dagger \Pi_n$?

Yes - e.g., take $\Pi_n = \sqrt{F_n}$.

(Unique up to isometric degree of freedom, since

$\Pi_n = U_n \sqrt{\Pi_n^\dagger \Pi_n}$ (the polar decomposition).

ii) Can any POVM meas. $\{\Pi_n\}_{n=0}^{N-1}$, $\sum_{n=0}^{N-1} \Pi_n^\dagger \Pi_n = I$,
be realized via ancilla + unitary?

$$X := \begin{pmatrix} \Pi_0 \\ \Pi_1 \\ \vdots \\ \Pi_{N-1} \end{pmatrix}$$

$\sum \Pi_n^\dagger \Pi_n = I \iff X$ has orthogonal columns

$\implies X$ can be extended to a unitary U by adding further columns,

... this can be understood as a unitary acting on system + ancilla B with dim. $d_B = N$.

$$U = \begin{pmatrix} \langle 0|_B \\ \langle 1|_B \\ \vdots \\ \langle d-1|_B \end{pmatrix} \begin{pmatrix} \Pi_0 & & & \\ & \Pi_1 & & \\ & & \ddots & \\ & & & \Pi_{N-1} \end{pmatrix}$$

$$\Rightarrow \langle u|_B U|0\rangle_B = \Pi_u.$$

\Rightarrow Any POVM meas. $\{\Pi_u\}$ can be realized by adding ancilla, doing a unitary U on system + ancilla, and projectively measuring ancilla in $\{|0\rangle, \dots, |d-1\rangle\}$ basis.

This is also known as Neumaier's Theorem.

Note: The "old-style" measurements where the $\Pi_u \equiv E_u$ (or equivalently $F_u \equiv E_u$) are also called projective measurements.

Is this the most general type of measurement? ^{1/77}

i) Minimal requirements for g.m. measurements:

Measurements are linear functionals

$$\rho \mapsto p_\mu(\rho),$$

which map states to outcome probabilities,
such that

$$p_\mu(\rho) \geq 0 \quad \forall \rho \geq 0, \text{tr}(\rho) = 1$$

and

$$\sum p_\mu(\rho) = 1 \quad \forall \rho \geq 0, \text{tr}(\rho) = 1.$$

ii) Linear functionals $\rho \mapsto f(\rho)$ ($\rho \geq 0$) can be
uniquely extended (over \mathbb{C}) to all matrices X ,

$$X \mapsto f(X), \text{ as } X = \underbrace{\frac{X+X^\dagger}{2}}_{\text{hermitian}} + i \cdot \underbrace{\frac{X-X^\dagger}{2i}}_{\text{hermitian}},$$

and any hermitian $H = \underbrace{P}_{\geq 0} - \underbrace{N}_{\geq 0}$

(e.g. P, N from pos./neg. eigenvalues).

iii) Linear functionals $X \mapsto p_u(X)$ are of

the form $p_u(\rho) = \text{tr}(F_u \rho)$,

$$\begin{aligned} \text{(E.g. from } p_u(\rho) &= p_u(\sum p_{ij} |i\rangle\langle j|) \\ &= \text{tr}\left(\underbrace{\left[\sum p_u(|i\rangle\langle j|) |i\rangle\langle j|\right]}_{=: F_u} \rho\right) \end{aligned}$$

and F_u is unique (as $\text{tr}(A^\dagger B)$ is a scalar product.)

$$\text{iv) } \text{tr}(I\rho) = \text{tr}(\rho) = 1 = \sum p_u(\rho) = \text{tr}\left(\sum F_u \rho\right)$$

$$\Rightarrow \sum F_u = I,$$

v) $F_u \geq 0$ — otherwise, $\exists |\phi\rangle: \langle\phi|F_u|\phi\rangle \neq 0$,

and thus for $\rho = |\phi\rangle\langle\phi|$,

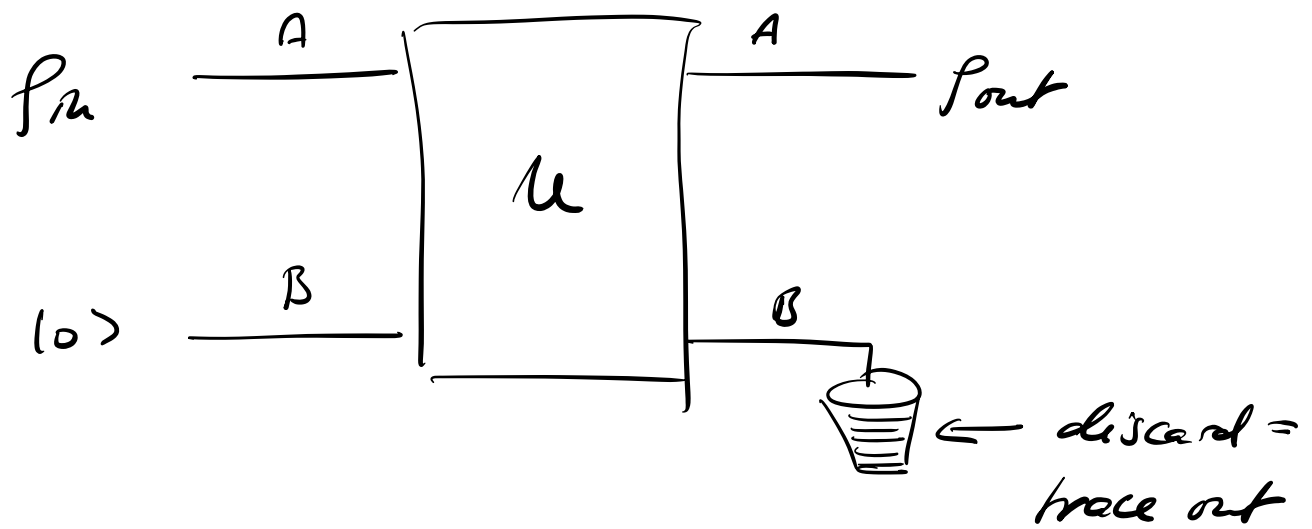
$$p_u(\rho) = \text{tr}[F_u, |\phi\rangle\langle\phi|] = \langle\phi|F_u|\phi\rangle \neq 0$$

Thus: POVM measurement is the most
general linear measurement on density
 matrices.

5. General evolution: Completely positive maps

What is the most general physical evolution of density matrices (a "superoperator")?

Same idea as for measurement — add ancilla:



... but now ancilla is simply discarded,

Analyze:

$$\begin{aligned}
 \rho &\mapsto \mathcal{E}(\rho) = \text{tr}_B [U (\rho \otimes |0\rangle_B \langle 0|) U^\dagger] \\
 &= \sum_u \langle u |_B U | 0 \rangle_B \rho \langle 0 |_B U^\dagger | u \rangle_B \\
 &= \sum_u \Pi_u \rho \Pi_u^\dagger
 \end{aligned}$$

with $\Pi_u := \langle u |_\mathcal{B} u |_0 \rangle_\mathcal{S}$ (as for POVM).

Properties of Π_u : As before, $\sum \Pi_u^\dagger \Pi_u = I$.

(Note: We can write the trace in a different

basis $|\tilde{u}\rangle := \sum v_{um} |u\rangle$, (v_{um}) unitary

$\Rightarrow \tilde{\Pi}_u = \sum \overline{v_{um}} \Pi_u$ represents same
evolution (cf. other ambiguities!)).

Definition (Kraus representation):

We call $\mathcal{E}(\rho) = \sum \Pi_u \rho \Pi_u^\dagger$, $\sum \Pi_u^\dagger \Pi_u = I$,

a Kraus representation of \mathcal{E} .

The Π_u are called Kraus operators.

(Note: Not all maps have a Kraus representation.

But we will see that all physical maps
have a Kraus representation.)

(Note: As discussed above, the Kraus rep.
is not unique.)

Relation to POVM: Any such map can be under-

stood as a POVM measurement where we discard the meas. outcome. In particular:

Relation to unitary + ancilla: Any map \mathcal{E} with a Kraus form can be realized by adding an ancilla, evolving both, and discarding the ancilla. ("Stinespring dilation of \mathcal{E} ")

Is this the most general physical map?

Minimal conditions on physical maps:

- i) linear: $\mathcal{E}(\rho + \lambda \sigma) = \mathcal{E}(\rho) + \lambda \mathcal{E}(\sigma)$.
(required for ensemble interpretation)
- ii) trace-preserving: $\text{tr}(\mathcal{E}(\rho)) = \text{tr}(\rho)$
(preserves probabilities)
- iii) positive: $\rho \geq 0 \Rightarrow \mathcal{E}(\rho) \geq 0$.
(ii + iii \Leftrightarrow maps density matrices to density matrices)

Is this sufficient?

NO!

\mathcal{E} should still be physical even if it acts on part of a larger system, i.e.,

$\mathcal{E}_A \otimes \mathcal{I}_B$ should still satisfy (i) - (iii).

(i), (ii) are implied by the above. But we get a new condition:

minimal conditions for phys. maps (cont'd):

(iv) complete positivity:

For any dimension d_B of B ,

$$\rho_{AB} \geq 0 \implies (\mathcal{E}_A \otimes \mathcal{I}_B)(\rho_{AB}) \geq 0.$$

(Note: The map $\mathcal{E} \otimes \mathcal{I}$ is yet again defined

through linearity, i.e. $(\mathcal{E} \otimes \mathcal{I})(N \otimes \pi) = \mathcal{E}(N) \otimes \mathcal{I}(\pi)$,
+ linearity).

Definition: We call a map $E: \rho \mapsto E(\rho)$ ^{I/83}

satisfying the conditions (i)-(iv) above

a completely positive trace-preserving
(CPTP) map, or a quantum channel.

Are there maps which are positive ((i)-(iii)) but not completely positive?


YES! E.g. "transposition map"

$$E(\rho) = \rho^T$$

$$(E \otimes I)(\rho_{AB}) =: \rho_{AB}^{T_A} \quad \text{"partial transpose"}$$

Consider action of $E \otimes I$ on $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

- since $(|i\rangle\langle j|)^T = |j\rangle\langle i| \Rightarrow (|i\rangle\langle k| |j\rangle\langle l|)^T = |j\rangle\langle i| |k\rangle\langle l|$



$$(\mathcal{E} \otimes I)(|\mathcal{R}\rangle\langle\mathcal{R}|) = (|\mathcal{R}\rangle\langle\mathcal{R}|)^{T_A}$$

$$= \frac{1}{2} \left[|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11| \right]$$

$$= \frac{1}{2} \left[|00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11| \right]$$

$$= \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \not\geq 0 !$$

Note: Positive but not completely positive maps are important tools to detect entanglement, since they satisfy $(\mathcal{E} \otimes I)(\rho) \geq 0$ for any unentangled state. i.e.: $(\mathcal{E} \otimes I)(\rho) \not\geq 0 \Rightarrow \rho$ entangled!
(\rightarrow Chapter II!)

Lemma: Any \mathcal{E} in Kraus form is CPTP.

Proof: Either by construction, or by direct inspection of

$$(\mathcal{E} \otimes I)(\rho) = \sum \underbrace{(\pi_u \otimes I) \rho (\pi_u \otimes I)}_{\geq 0}^\dagger \geq 0 \quad \square$$

Can conversely all CPTP maps be written in Kraus form? If yes, how can we obtain the Kraus operators?

Key tool: The Choi-Jamiołkowski isomorphism.

Theorem (Choi-Jamiołkowski isomorphism) reminds:
 $B(X) = B_H$.
maps on X .

Let $\mathcal{C} := \{\mathcal{E} \mid \mathcal{E} \text{ CPTP}\} \subset B(B(\mathbb{C}^d))$ the space of all CPTP maps on the density operators on \mathbb{C}^d , and

$$\mathcal{J} := \{\sigma_{AB} \mid \sigma_{AB} \geq 0, \text{tr}_A(\sigma_{AB}) = \frac{1}{d} I\} \subset B(\mathbb{C}^d \otimes \mathbb{C}^d)$$

the space of all bipartite states with $\text{tr}_A(\sigma_{AB}) = \frac{1}{d} I$.

Then, the map

$$\hat{\chi} : B(B(\mathbb{C}^d)) \longrightarrow B(\mathbb{C}^d \otimes \mathbb{C}^d)$$

$$\mathcal{E} \longmapsto \sigma_{AB} = (\mathcal{E}_A \otimes I_B)(|\Omega\rangle\langle\Omega|),$$

$$|\mathcal{L}\rangle := \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i, i\rangle$$

defines an isomorphism between \mathcal{C} and \mathcal{F} ,
the Choi-Jamiołkowski isomorphism, with
 σ_{AB} the Choi state of \mathcal{E} . The inverse map is

$$\hat{\gamma} : \mathcal{B}(\mathcal{C}^d \otimes \mathcal{C}^d) \longrightarrow \mathcal{B}(\mathcal{B}(\mathcal{C}^d))$$

$$\sigma_{AB} \longmapsto F,$$

$$\text{where } F(\rho) = d \cdot \text{tr}_B [\sigma_{AB} \cdot (\mathbb{I}_A \otimes \rho^T)].$$

(Note: A physical interpretation of $\hat{x}, \hat{\gamma}$, and
the theorem will be given in Chapter II.)

Proof: We need to show:

$$(i) \quad \hat{\gamma} \circ \hat{x} = \mathbb{I}$$

$$(ii) \quad \hat{x} \circ \hat{\gamma} = \mathbb{I}$$

$$(iii) \quad \text{Im}(\hat{x}|_{\mathcal{C}}) = \{ \hat{x}(\varepsilon) \mid \varepsilon \in \mathcal{C} \} \subset \mathcal{F}$$

$$(iv) \quad \text{Im}(\hat{\gamma}|_{\mathcal{F}}) \subset \mathcal{C}.$$

Together, (i) - (iv) imply

a) (i) $\Rightarrow \hat{X}$ injective

b) $s \in f \Rightarrow c := \hat{Y}_s \stackrel{(iv)}{\in} \mathcal{C} \text{ \& } \hat{X}c \stackrel{(ii)}{=} s$

$$\left. \begin{array}{l} \Rightarrow \text{Im } \hat{X}|_{\mathcal{C}} \supset f \\ \text{and from (iii):} \\ \text{Im } \hat{X}|_{\mathcal{C}} \subset f \end{array} \right\} \Rightarrow \text{Im } \hat{X}|_{\mathcal{C}} = f, \\ \text{i.e. } \hat{X}|_{\mathcal{C}} \text{ surjective}$$

$$\Rightarrow \hat{X}|_{\mathcal{C}} : \mathcal{C} \rightarrow f = \text{Im } \hat{X}|_{\mathcal{C}}$$

is a linear bijection!

Proof of (i): $\hat{Y} \cdot \hat{X} = I$:

Need to show $\hat{Y}(\hat{X}(\varepsilon)) = \varepsilon$ for all $\varepsilon \in \mathcal{B}(\mathcal{B}(\mathbb{C}^d))$.

$$\hat{Y}(\hat{X}(\varepsilon))(p) \stackrel{\text{any } p \in \mathcal{B}(\mathbb{C}^d)}{=} d \cdot \text{tr}_{\mathcal{B}} \left[\underbrace{\hat{X}(\varepsilon)}_{\equiv G_{AB}} \cdot (\mathbb{I}_A \otimes p^T) \right]$$

$$= d \cdot \frac{1}{d} \sum_{ij} \text{tr}_{\mathcal{B}} \left[\underbrace{((\varepsilon \otimes \mathbb{I}_B)(|i\rangle\langle j| \otimes |i\rangle\langle j|))}_{\varepsilon(|i\rangle\langle j|) \otimes |i\rangle\langle j|} (\mathbb{I}_A \otimes p^T) \right]$$

$$\begin{aligned}
&= \sum_{ij} \mathcal{E}(|i\rangle\langle j|) \cdot \underbrace{\text{tr}[|i\rangle\langle j| \rho^T]}_{= \langle j| \rho^T | i \rangle = \rho_{ji}} \\
&= \mathcal{E}\left(\sum_{ij} \rho_{ji} |i\rangle\langle j|\right) \\
&= \underline{\mathcal{E}(\rho)}.
\end{aligned}$$

i.e.: $\hat{Y}(\hat{X}(\varepsilon))(\rho) = \mathcal{E}(\rho) \quad \forall \rho, \varepsilon$

$$\Rightarrow \hat{Y}(\hat{X}(\varepsilon)) = \mathcal{E} \quad \forall \varepsilon \quad \mathbb{R}$$

Proof of (ii): $\hat{X} \circ \hat{Y} = I$.

Since $\dim B(\mathbb{C}^d \otimes \mathbb{C}^d) = \dim(B(B(\mathbb{C}^d)))$,
this is equivalent to (i) \mathbb{R}

(Explicit proof:

For any $\sigma_{AB} \in B(\mathbb{C}^d \otimes \mathbb{C}^d)$,

$$\begin{aligned}
\underbrace{\hat{X}(\hat{Y}(\sigma_{AB}))}_{\equiv \mathcal{F}} &= \left(\underbrace{\hat{Y}(\sigma_{AB})}_{\equiv \mathcal{F}_A} \otimes I_B \right) (|i\rangle\langle j|) \\
&= \frac{1}{d} \sum_{ij} \underbrace{\hat{Y}(\sigma_{AB})}_{\equiv \mathcal{F}_A} (|i\rangle\langle j|_A) \otimes |i\rangle\langle j|_B
\end{aligned}$$

$$= \frac{1}{d} \sum_{ij} d \cdot \text{tr}_B \left[\sigma_{AB} \cdot (\mathbb{I}_A \otimes |i\rangle\langle j|)_B^T \right] \otimes |i\rangle\langle j|_B \quad \text{I/89}$$

$$= \sum_{ij} \langle i|_B \sigma_{AB} |j\rangle_B \otimes |i\rangle\langle j|_B$$

$$= \sigma_{AB}.$$

$$\Rightarrow \hat{X} \circ \hat{Y} = \mathbb{I}.)$$

Proof of (iii): $\text{Im } \hat{X}|_{\mathcal{C}} \subseteq \mathcal{J}.$

Let $\mathcal{E} \in \mathcal{C}$, i.e., \mathcal{E} is a CPTP map.

$$\text{Then, } \sigma_{AB} := \hat{X}(\mathcal{E}) = (\mathcal{E}_A \otimes \mathbb{I}_B)(| \Omega_X \Omega |) \geq 0$$

Since \mathcal{E} is completely positive.

$$\text{Further, } \underline{\text{tr}_A(\sigma_{AB})} = \frac{1}{d} \sum \text{tr}_A \left[(\mathcal{E}_A \otimes \mathbb{I}_B)(|i\rangle\langle j|) \right]$$

$$= \frac{1}{d} \sum \text{tr} \left[\mathcal{E}(|i\rangle\langle j|) \right] |i\rangle\langle j|_B = \underline{\underline{\frac{1}{d} \mathbb{I}_B.}}$$

$$= \text{tr}[|i\rangle\langle j|] = \delta_{ij}.$$

\mathcal{E} trace preserving

$$\Rightarrow \sigma_{AB} = \hat{X}(\mathcal{E}) \in \mathcal{J} \quad \forall \mathcal{E} \in \mathcal{C}.$$

Proof of (iv): $\lim \hat{Y}/\rho \in \mathcal{C}$.

Let $\sigma_{AB} \in \mathcal{S}$. Write $\sigma_{AB} = \sum_k |\tilde{\psi}_k\rangle\langle\tilde{\psi}_k|$ (un-normalized!)
can be any decomposition
- e.g. eigenvalue dec.

$$\text{Expand } |\tilde{\psi}_k\rangle = \sum_j \frac{1}{\sqrt{d}} u_k^{j^*} |j\rangle|i\rangle$$

$$= \frac{1}{\sqrt{d}} \sum_i \pi_k |i\rangle\langle i|$$

$$= (\pi_k \otimes I) |\mathcal{R}\rangle\langle\mathcal{R}|,$$

where π_k has entries $(\pi_k)_{j^*i^*} = u_k^{j^*i^*}$.

$$\begin{aligned} \text{Then, } \sigma_{AB} &= \sum_k (\pi_k \otimes I) |\mathcal{R}\rangle\langle\mathcal{R}| (\pi_k \otimes I)^{\dagger} \\ &= (E \otimes I) (|\mathcal{R}\rangle\langle\mathcal{R}|) = \hat{X}(E) \end{aligned}$$

with $E(\rho) = \sum \pi_k \rho \pi_k^{\dagger}$, and thus

$$\hat{Y}(\sigma_{AB}) = \hat{Y}(\hat{X}(E)) = E \text{ is completely positive.}$$

(Of course, $\hat{Y}(\sigma_{AB}) = \sum \pi_k \circ \pi_k^{\dagger}$ can also be found by explicitly using the definition of \hat{Y} .)

(Note: $E(\rho) = \sum \pi_k \rho \pi_k^\dagger$ removes the ambiguity¹⁹¹ of the ensemble decomposition \otimes : same ambiguity!)

Moreover, $\frac{1}{d} I = \text{tr}_A \sigma_{AB}$

$$= \text{tr}_A \left[\sum_k (\pi_k \otimes I) |\chi\rangle\langle\chi| (\pi_k \otimes I)^\dagger \right]$$

$$= \sum_k \text{tr}_A \left[(\pi_k^\dagger \pi_k \otimes I) |\chi\rangle\langle\chi| \right]$$

$$= \frac{1}{d} \sum_{ijk} \underbrace{\text{tr}(\pi_k^\dagger \pi_k |i\rangle\langle j|)}_{= \langle j | \pi_k^\dagger \pi_k | i \rangle} |i\rangle\langle j|$$

$$\Rightarrow \sum_k \langle j | \pi_k^\dagger \pi_k | i \rangle = \delta_{ij}$$

$$\Rightarrow \sum_k \pi_k^\dagger \pi_k = I.$$

Thus, $\hat{Y}(\sigma_{AB})(\rho) = \sum \pi_k^\dagger \rho \pi_k$ w/ $\sum \pi_k^\dagger \pi_k = I$,

i.e., $\hat{Y}(\sigma_{AB})$ has a Kraus representation

and is thus a CPTP map, $\hat{Y}(\sigma_{AB}) \in \mathcal{C}_B$



Note: The isomorphism still holds if we drop trace preserving from \mathcal{C} and $\text{tr}_A \sigma_{AB} = \frac{1}{d} I$ from \mathcal{S} , respectively.

Corollary (from the proof of (iv)):

All CPTP maps are of Kraus form, and can thus be realized with a three step process (i.e., add ancilla + unitary + tracing).

Moreover, the Kraus operators Π_k can be obtained from the Choi state σ_{AB} by writing

$$\sigma_{AB} = \sum |\tilde{\psi}_k\rangle\langle\tilde{\psi}_k|, \text{ and } |\tilde{\psi}_k\rangle = (\Pi_k \otimes I)|\chi\rangle.$$

6. Axioms of quantum theory ("mixed version") ^{I/93}

- States are linear operators ρ with

$$\rho \geq 0$$

$$\text{tr}(\rho) = 1.$$

- Evolution is completely positive trace preserving (CPTP) maps

$$\mathcal{E}(\rho) = \sum \Pi_n \rho \Pi_n^\dagger, \quad \sum \Pi_n^\dagger \Pi_n = \mathbb{I}.$$

- Measurements act as

$$\rho \mapsto \rho_n = \frac{\Pi_n \rho \Pi_n^\dagger}{\text{tr}(\Pi_n \rho \Pi_n^\dagger)},$$

with probability $p_n = \text{tr}(\Pi_n^\dagger \Pi_n \rho)$,

where $\sum \Pi_n^\dagger \Pi_n = \mathbb{I}$.