II. The formalism: States, measurements, and evolution

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

$$|0\rangle, |1\rangle, \ldots, |d-1\rangle, \text{ i.e.}$$

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

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 $(|v\rangle)^\dagger$ ← transpose conjugate of the matrix/vector

is

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

We write

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

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

$\mathcal{H}$ is a vector space; we write <u>linear combinations</u> 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 give by

$$(|w\rangle)^\dagger \cdot (|v\rangle) = \sum \overline{w_i} v_i =: \underbrace{\langle w|v\rangle}_{\text{"bra-ket"}}$$

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

Canonical basis is orthonormal basis (ONB):

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

$\Rightarrow$ for $|v\rangle = \sum v_i |i\rangle$, $|w\rangle = \sum w_j |j\rangle$,

$$\langle w|v\rangle = \sum \overline{w_j} v_i \underbrace{\langle j|i\rangle}_{\delta_{ij}} = \sum \overline{w_i} v_i .$$

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

Linear maps:

$M : \mathcal{H} \to \mathcal{H}$ is a linear map:

– with $M|v\rangle := M(|v\rangle)$ –

$$M(|v\rangle + \lambda|w\rangle) = M|v\rangle + \lambda M|w\rangle.$$

The map $I = \sum |i\rangle\langle i|$ satisfies ~~that~~

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

$$I|v\rangle = \Big(\sum_i |i\rangle\langle i|\Big)\Big(\sum_j v_j |j\rangle\Big)$$

$$= \sum_{ij} v_j \, |i\rangle \underbrace{\langle i|j\rangle}_{\delta_{ij}} = \sum v_j |j\rangle$$

$\Longrightarrow$ I is the identity map.

This can also be seen in matrix form:

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

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

$$M = I \cdot M \cdot I$$

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

$$= \sum_{ij} \Pi_{ij} \underbrace{|i\rangle\langle j|}_{=\ \begin{array}{cc} & \begin{array}{cccc} & & j & \end{array} \\ i & \begin{pmatrix} 0 & \cdots & \downarrow & 0 \\ \vdots & \rightarrow & 1 & \vdots \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix} \end{array}}$$

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

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

The map $\Pi^\dagger$ is the map with entries $\overline{\Pi_{ji}}$ (where $\Pi_{ij} = \langle i|\Pi|j\rangle$). It holds that

$$\left(\Pi|\omega\rangle\right)^\dagger = \langle\omega|\Pi^\dagger, \text{ and } (AB)^\dagger = B^\dagger A^\dagger.$$

<u>Unitary maps:</u>

A map $\mathcal{U} : \mathcal{H} \rightarrow \mathcal{H}$ is <u>unitary</u> iff

$$\mathcal{U}^\dagger \mathcal{U} = I,$$

or equivalently:

- $\mathcal{U}\mathcal{U}^\dagger = I$
- $(\mathcal{U}|w\rangle)^\dagger (\mathcal{U}|v\rangle) = \langle w|\mathcal{U}^\dagger\mathcal{U}|v\rangle = \langle w|v\rangle$

  ($\mathcal{U}$ preserves angles)

- $\| \mathcal{U}|w\rangle \|_2 = \| |w\rangle \|_2$

  ($\mathcal{U}$ preserves norms)

In matrix notation:

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

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

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

We call $\mathcal{U} = (\mathcal{U}_{ij})_{ij}$ a <u>unitary matrix</u> or just a <u>unitary</u>.

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 $\{|i\rangle_A\}_{i=0}^{d_A-1}$, $\{|j\rangle_B\}_{j=0}^{d_B-1}$

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

we can define the <u>tensor product</u>

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

by <u>defining</u> $\mathcal{H}_A \otimes \mathcal{H}_B$ 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

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

s.th. $\left(\langle i|_A \otimes \langle j|_B\right)\left(|k\rangle_A \otimes |l\rangle_B\right)$

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

and defining $|v\rangle_A \otimes |w\rangle_B$ through linearity

$$|v\rangle_A \otimes |w\rangle_B = \left(\sum v_i |i\rangle_A\right) \otimes \left(\sum w_j |j\rangle_B\right)$$

$$= \left(\sum v_i w_j \, |i\rangle_A \otimes |j\rangle_B\right) = \sum v_i w_j |ij\rangle$$

$$= \begin{array}{c} \begin{pmatrix} v_0 w_0 \\ v_0 w_1 \\ \vdots \\ v_0 w_{d_B-1} \\ v_1 w_0 \\ v_1 w_1 \\ \vdots \end{pmatrix} \end{array} \begin{array}{l} \leftarrow 00 \\ \leftarrow 01 \\ \vdots \\ \\ \leftarrow 10 \\ \\ \\ \end{array}$$

standard convention (but just a conv.!)

A general vector $|\gamma\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is of the form

$|\gamma\rangle = \sum \gamma_{ij} |i\rangle|j\rangle$, and not necessarily of the form $|v\rangle \otimes |w\rangle$.

Similarly, two maps $M_A : \mathcal{H}_A \to \mathcal{H}_A$ and $N_B : \mathcal{H}_B \to \mathcal{H}_B$

always linear!

induce a map

$(M_A \otimes N_B) : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A \otimes \mathcal{H}_B$ by virtue of

$$\left(M_A \otimes N_B\right)\left(|v\rangle \otimes |w\rangle\right) := \left(M_A|v\rangle\right) \otimes \left(N_B|w\rangle\right)$$

(and extended linearly to the full space).

In matrix notation,

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

$$= \sum \langle i,j|\, M_A \otimes N_B \,|k,l\rangle \quad |i,j\rangle\langle k,l|$$

$$= \sum \langle i|M_A|k\rangle \langle j|N_B|l\rangle \quad |i,j\rangle\langle k,l|$$

$$= \sum \underbrace{\left(M_A\right)_{ik}\left(N_B\right)_{jl}}_{=\left(M_A \otimes N_B\right)_{(ij),(kl)}} \quad |i,j\rangle\langle k,l|$$

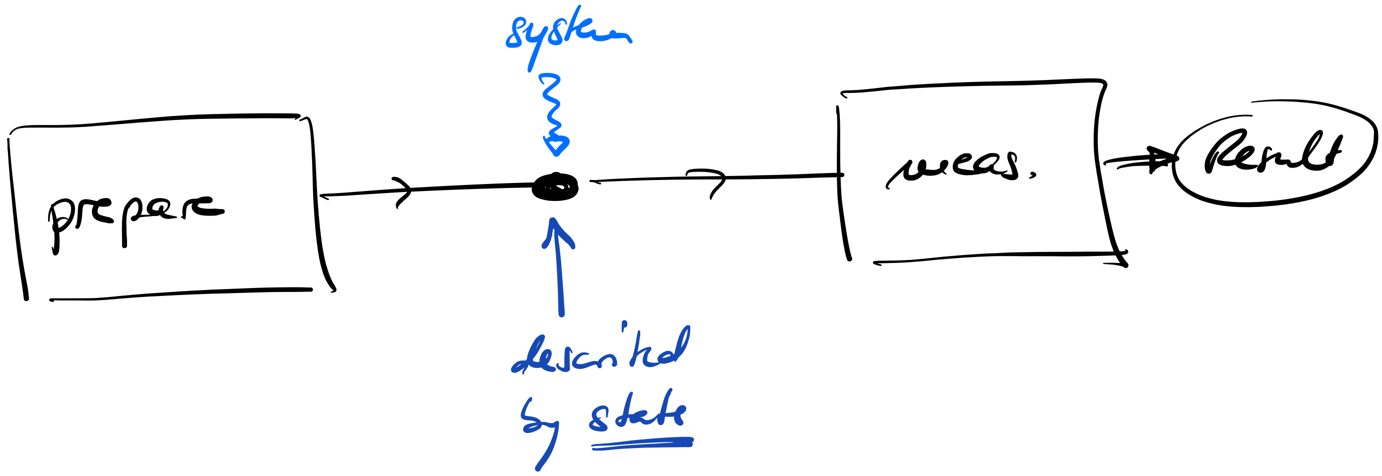
$$\Pi_A \otimes N_B = \begin{pmatrix} \Pi_{00} N_{00} & \Pi_{00} N_{01} & \cdots \\ \Pi_{00} N_{10} & \ddots & \\ \vdots & & \\ \Pi_{10} N_{00} & \Pi_{10} N_{01} & \cdots \\ \Pi_{10} N_{01} & & \ddots \end{pmatrix}$$

$$= \left(\begin{array}{c|c|c} \Pi_{00} \cdot N & \Pi_{01} \cdot N & \cdots \\ \hline \Pi_{10} \cdot N & \Pi_{11} \cdot N & \\ \hline \vdots & & \ddots \end{array}\right)$$

b) 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.

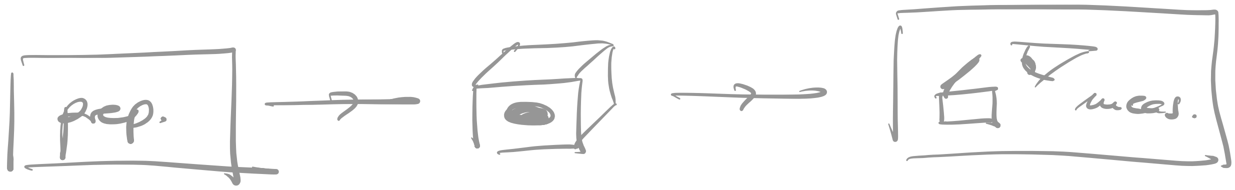
Measurement: Determine some property of phys. system.

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: $\vec{p} = \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$, or $\vec{p} = \begin{pmatrix} p_1 \\ \vdots \\ p_6 \end{pmatrix}$ is state of coin/dice.

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

Measurement: Outcome i w/ prob.

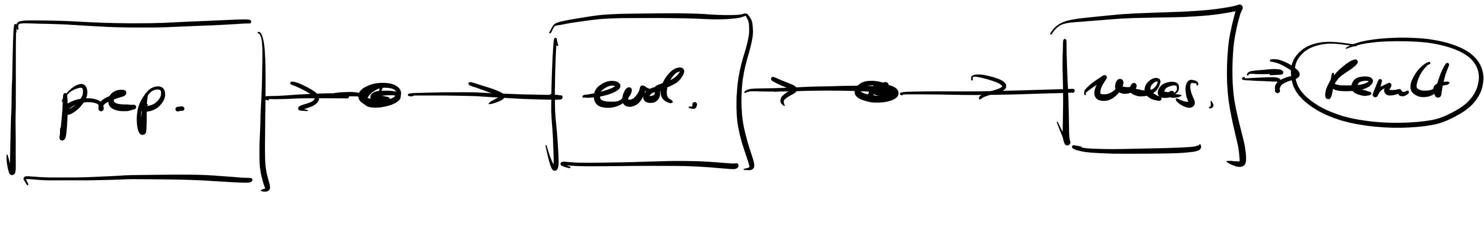
$$p_i = |\vec{e_i} \cdot \vec{p}|$$

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

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

Note: The state describes our knowledge about the system.

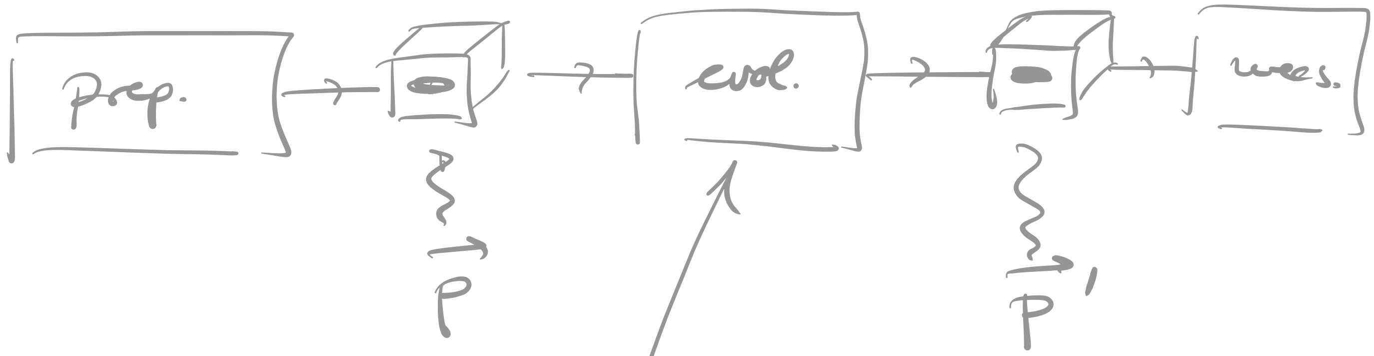
Evolution: In addition, we can "do things" with the system btw. preparation & measurement, i.e. evolve it:



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

∘ evolution can consist of a sequence of individual evolutions

Ex:



e.g.: ∘ shake box (→ add randomness)

∘ put coin heads up

∘ flip coin / permute dice values

∘ do one of the above w/ certain probability

Most general evolution:

1) Check value of coin/dice/... : i

2) Output j with prob. E_{ji}.

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

i.e. E is a <u>stochastic matrix</u>.

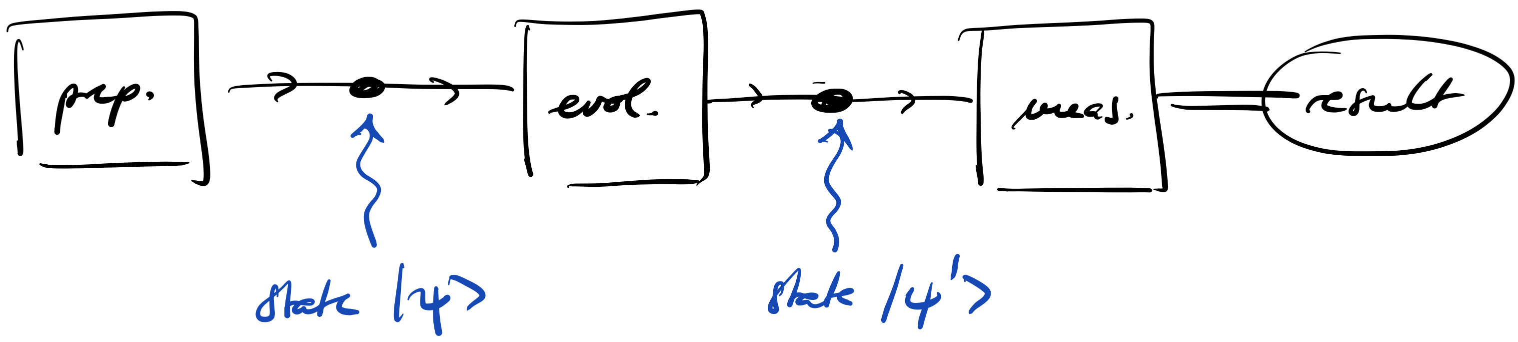
$\Rightarrow$ Evolution maps

$$\vec{p} \longmapsto \vec{p}\,' = E \cdot \vec{p}$$

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

the <u>only</u> property we care about – irrespective of physical realization.

... such that $\underbrace{\| |\psi\rangle \|_2}_{\text{often just write } \| |\psi\rangle \|} = 1$

and where $|\psi\rangle$ and $e^{i\phi}|\psi\rangle$ represent (ϕ real)

the same state.

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

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

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

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

$$\boxed{p_i = |\langle b_i|\psi\rangle|^2}$$

Note that

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

$$= \sum \langle\psi|b_i\rangle\langle b_i|\psi\rangle$$

$$= \langle\psi| \underbrace{\left(\sum |b_i\rangle\langle b_i|\right)}_{= I} |\psi\rangle$$

$$= \langle\psi|\psi\rangle$$

$$= \| |\psi\rangle \|_2^2 = 1.$$

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:

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

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 a 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:

$$|\psi\rangle \longmapsto U|\psi\rangle$$

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.

$\Longrightarrow$ U is unitary, $UU^\dagger = U^\dagger U = I$.

And: Any unitary U is an allowed evolution.

$$\boxed{\text{Evolution: } |\psi\rangle \longmapsto U|\psi\rangle, \quad UU^\dagger = U^\dagger U = I}$$

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
system $\longrightarrow$ •	•
described by Hilbert space $\mathcal{H}_A$	described by H. sp. $\mathcal{H}_B$
state $\lvert\psi_A\rangle$	state $\lvert\psi_B\rangle$

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

$\rightarrow$ Joint state of A & B described by

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

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

$$|\psi_{AB}\rangle \longmapsto (X_A \otimes I_B)\,|\psi_{AB}\rangle.$$

Why is this a good (correct) choice?

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

evolve →

add Bob ↓

$$\begin{tikzcd}
|\psi_A\rangle \arrow[r] \arrow[d] \arrow[dr, phantom, "\circlearrowleft"] & U_A|\psi_A\rangle \arrow[d] \\
|\psi_A\rangle \otimes |\psi_B\rangle \arrow[r] & (U_A|\psi_A\rangle) \otimes |\psi_B\rangle
\end{tikzcd}$$

• **or**: measure $\{E_i^A\}$. **Prob.**:

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

$$= (\langle\psi_A| \otimes \langle\psi_B|)\,(\underset{\uparrow \atop E_i^2 = E_i}{E_i^A} \otimes I)\, |\psi_A\rangle \otimes |\psi_B\rangle$$

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

Note: If both A & B act with X_A & Y_B, the total action is $(\mathbb{I}\otimes Y_B)(X_A\otimes\mathbb{I}) = X_A\otimes Y_B$.

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 $\{E_i^A\} \equiv \{E_i^A\otimes\mathbb{I}_B\}$ is

$$|\psi_i\rangle \propto (E_i^A\otimes\mathbb{I}_B)|\psi\rangle.$$

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

Analogy - probability:

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

$\Longrightarrow$ total prob. distr. has 4 possibilities

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 $X \otimes I = \left(\begin{array}{cc|cc} & & 1 & \\ & & & 1 \\ \hline 1 & & & \\ & 1 & & \end{array}\right)$.

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 (pure state version):

- Systems are described by Hilbert spaces $\mathcal{H} \cong \mathbb{C}^d$.
- States are normalized vectors
  $$|\psi\rangle \in \mathcal{H}, \quad \| |\psi\rangle \| = 1, \quad |\psi\rangle \sim e^{i\phi}|\psi\rangle$$
- 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. $p_i = \| |\tilde{\psi}_i\rangle \|_2^2 = \langle \tilde{\psi}_i | \tilde{\psi}_i \rangle$

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

- 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" $= I$).

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

If we write O in its spectral decomposition,

$$O = \sum \lambda_i E_i$$ 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 <u>the average value</u> (und <u>weaker</u> notion 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:

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

$$\rightarrow \text{prob. } p_0 = \| \alpha|0\rangle \|^2 = |\alpha|^2$$

$$= \langle\psi|E_0|\psi\rangle = |\alpha|^2$$

$$= |\langle 0|\psi\rangle|^2 = |\alpha|^2$$

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

<u>Outcome 1</u>: $|\tilde{\psi}_1\rangle = E_1|\psi\rangle = \beta|1\rangle$

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

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

<u>Measurement "in X basis"</u>, i.e. of observable

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

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

$$|\tilde{\psi}_\pm\rangle = |\pm X\pm|\psi\rangle = |\pm\rangle\left(\frac{1}{\sqrt{2}}(\langle 0| \pm \langle 1|)(\alpha|0\rangle + \beta|1\rangle)\right)$$

$$= |\pm\rangle\left(\frac{1}{\sqrt{2}}(\alpha \pm \beta)\right)$$

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

$$|\psi_\pm\rangle = |\pm\rangle \quad \longleftarrow \text{post-meas. state}$$

<u>Note</u>: 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: $YZ = iX$, $ZX = iY$
- diff. Paulis anti-comm.: $XY = -YX$ etc.
- in addition $X^2 = Y^2 = Z^2 = I$
- summarized as $\sigma_\alpha \sigma_\beta = i \epsilon_{\alpha\beta\gamma} \sigma_\gamma + \delta_{\alpha\beta} I$

fully anti-symmetric tensor.

The Pauli matrices are <u>hermitian</u> <u>and</u> unitary, i.e. can describe <u>both</u> measurements and evolution!

Evolution:

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

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

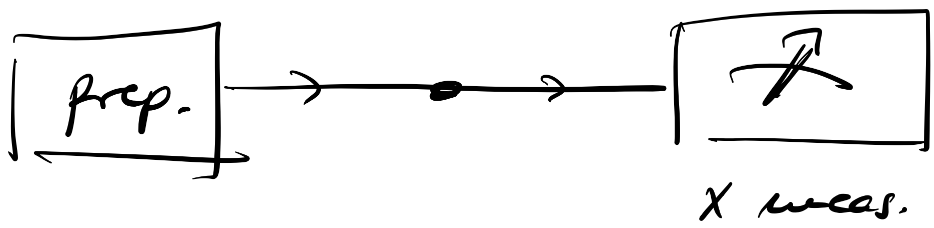
$$= \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

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

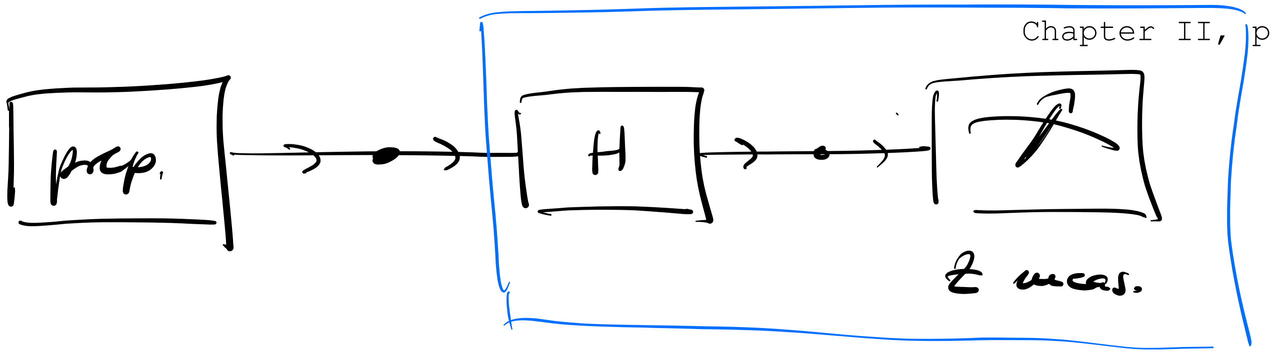
outcome 0 w/ $p_0 = \frac{|\alpha+\beta|^2}{2}$

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.: $HXH = Z$, $HZH = X$ (note $H^2 = I$).

Measurement on a bipartite state:

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

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 $\langle +|0\rangle = \langle +|1\rangle = \langle -|0\rangle = 1/\sqrt{2}, \; \langle -|1\rangle = -1/\sqrt{2}$)

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

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

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

$$|\langle --|\psi\rangle|^2 = \quad \ldots \quad = 0$$

$\Rightarrow$ perfect anti-correlation!

In fact, outcomes anti-correlated for same measurement in <u>any</u> basis! (→ homework)

(But the outcomes of A or B <u>alone</u> are completely random.)

Best: Alice measures X, Bob Z:

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

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

$$|\langle -0|\psi\rangle|^2 = \quad \ldots \quad = \tfrac{1}{4}$$

$$|\langle -1|\psi\rangle|^2 = \quad \ldots \quad = \tfrac{1}{4}$$

Outcomes of A & B are completely independent.

d) The Bloch sphere:

Consider state of one qubit:

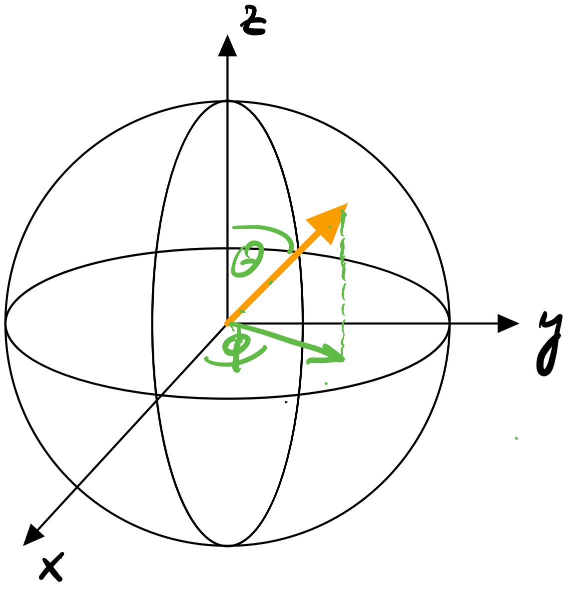
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

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

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

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

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



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

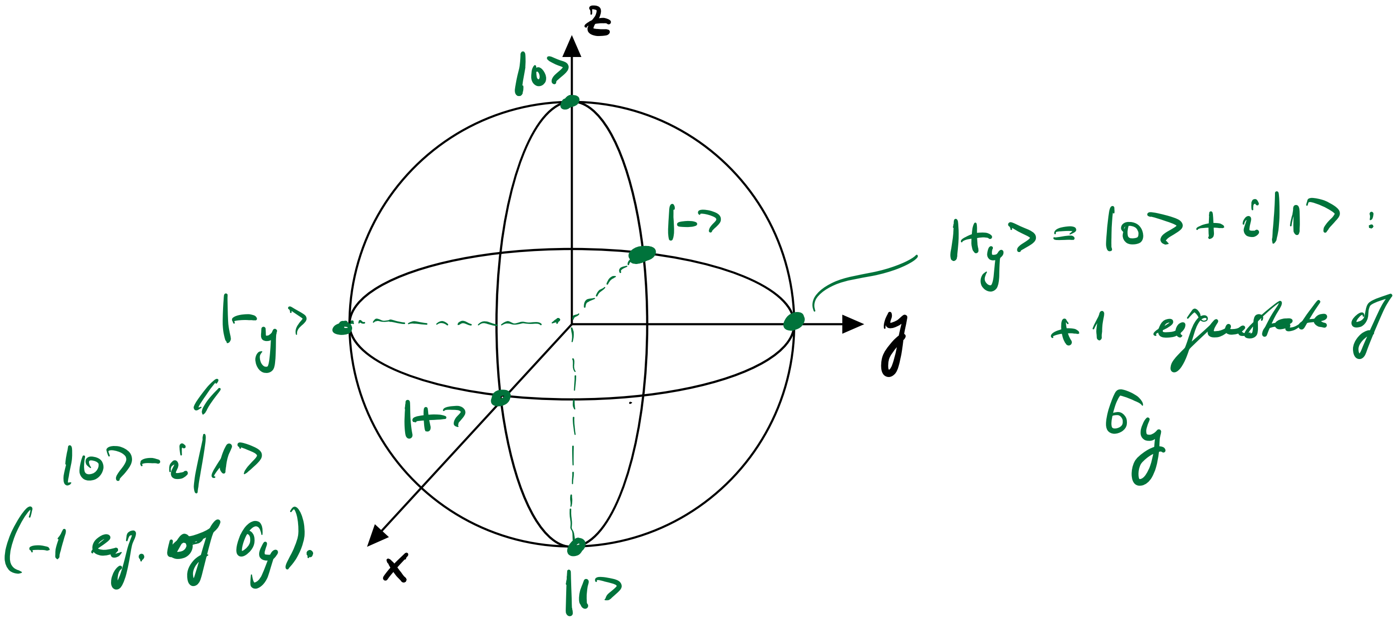
$\boxed{\text{"Bloch sphere"}}$

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 → proof cf. Hwork):

Important states:



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

Denotes $m_1\sigma_1 + m_2\sigma_2 + m_3\sigma_3$

$$\equiv m_x\sigma_x + m_y\sigma_y + m_z\sigma_z .$$

(Reason: $\{I, \sigma_x, \sigma_y, \sigma_z\}$ is a basis of herm. matrices over $\mathbb{R}$, and all mtx. over $\mathbb{C}$ → cf. Hwork.)

$\Rightarrow$ eigenstates ± 1 of M have Bloch vectors $\pm\vec{m}$.

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).

Measurement of qubit:

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

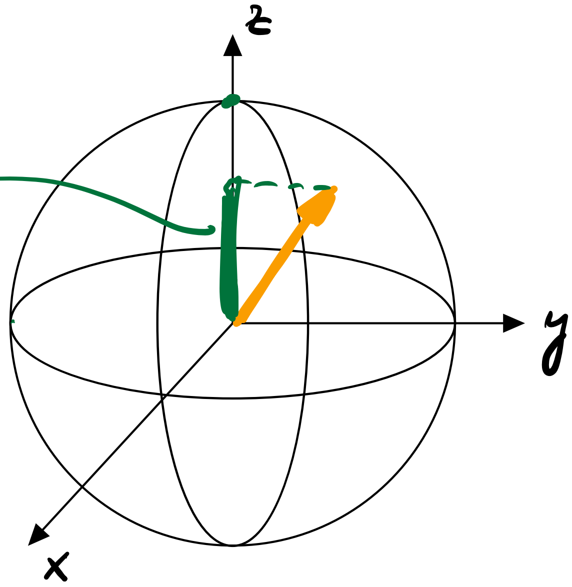
Prob. for outcome ± 1 is then

$$p_{\pm 1} = \langle\psi|\, E_{\pm 1}\,|\psi\rangle = \frac{1 \pm \vec{m}\cdot\vec{r}}{2} .$$

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

E.g. meas in Z basis:

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



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

Probability changes linearly along z axis for 1 to 0, or 0 to 1.

$\Leftrightarrow \quad p = \frac{1 \pm \vec{m} \cdot \vec{r}}{2}$.

Evolution:

Unitaries on qubits are of the form

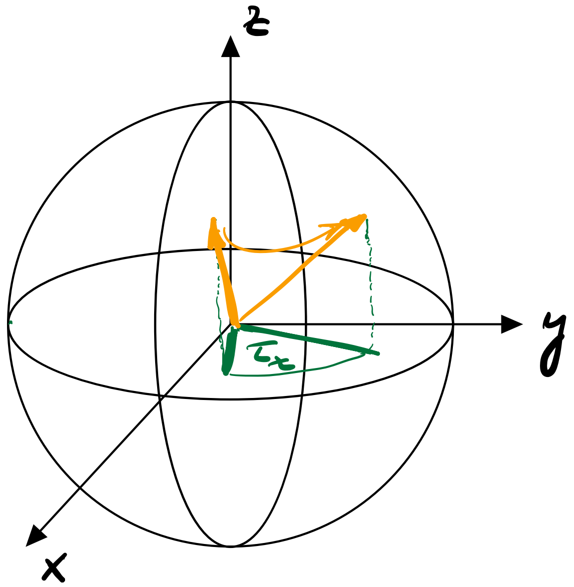
$$U = e^{i\chi} \exp\left[-i \vec{\tau} \cdot \vec{\sigma}/2\right]$$

(Proof idea: Go from U to generator $G = G^\dagger$, $U = e^{-iG}$, and write G as $G = \vec{m} \cdot \vec{\sigma} + c \cdot I$.)

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

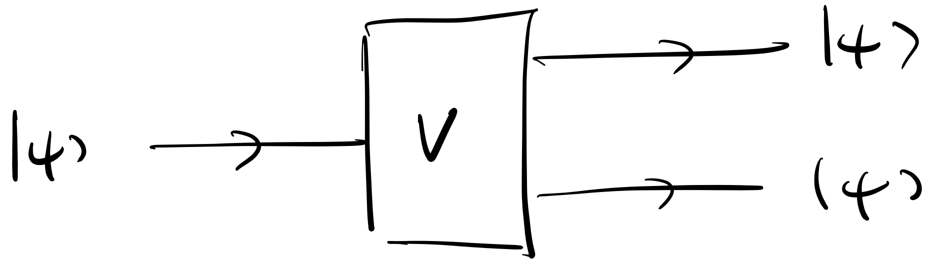
$$SU(2)/\mathbb{Z}_2 \cong SO(3)$$

(The $\cdot/\mathbb{Z}_2$ 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 theorem

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



i.e. a transformation

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

$$|\psi\rangle \longmapsto |\psi\rangle \otimes |\psi\rangle \qquad ?$$

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

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

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

$$|\psi\rangle \otimes |0\rangle \longmapsto |\psi\rangle \otimes |\psi\rangle$$

any suitable fiducial state

Note: $V := \mathcal{U}(I_A \otimes |0\rangle_B)$ is an <u>isometry</u>:

$$V^\dagger V = (\langle 0|_B \otimes I_A)\, \underbrace{\mathcal{U}^\dagger \mathcal{U}}_{I_{AB}}\, (I_A \otimes |0\rangle_B)$$

$$= \langle 0|_B\, I_{AB}\, |0\rangle_B = I_A$$

No-cloning-Theorem:

Quantum information cannot be copied, i.e. a

$$\mathcal{U} : |\psi\rangle \otimes |0\rangle \longmapsto |\psi\rangle \otimes |\psi\rangle \qquad (*)$$

cannot exist.

Proof:

$$\mathcal{U}\,(|0\rangle \otimes |0\rangle) \overset{(*)}{=} |0\rangle \otimes |0\rangle$$

$$\mathcal{U}\,(|1\rangle \otimes |0\rangle) \overset{(*)}{=} |1\rangle \otimes |1\rangle$$

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

But, from $(*)$:

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

$\lightning$

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

$\longrightarrow$ Contradiction!

$\longrightarrow$ U cannot exist (note: we only used linearity!)

$\boxtimes$

Quantum information cannot be copied!

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

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

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

(Proof: Homework)