- a qubit is physically realized as a quantum state of a two state / two levels quantum system

one qubit can be written as:

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathbb{C}$ — this superposition is similar to the <u>interference of waves</u>

$|0\rangle ; |1\rangle$ => vectors, "kets" representation (Dirac representation)

they are the 2 orthogonal vectors in the <u>qubit space H</u> forming the <u>computational basis</u>:

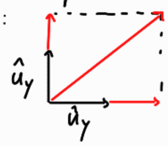
$\{|0\rangle, |1\rangle\}$ two kets — [a ket $|v\rangle$ denotes a vector v in a complex vector space V]

"qubit 1" "qubit 2"

from a mathematical point of view we can describe the qubit as a vector. Indeed, it is a linear superposition

↳ a qubit is mathematically described as <u>a vector</u> (ket) of a 2 dimension complex vectorial space $\mathbb{H}$

a two dimensional complex vectorial space has a <u>base</u> made of 2 elements, similarly to the usual cartesian representation:



any vector belonging to the vectorial space described by the base $\{\hat{u}_x, \hat{u}_y\}$ can be written as a linear superposition of the two elements of the base

complete w.r.t. the norm defined as the scalar product

we need a <u>scalar product</u> to define distances. If you add a scalar product, $\mathbb{H}$ becomes a <u>2-D Hilbert space</u>. Completeness is automatically guaranteed by the finite dimension of the space (it would not be guaranteed in the case of an infinite dimension space)

"every cauchy succession in the space converges in that space"

inner product in Hilbert spaces $|\psi\rangle$ (Dirac notation)

we need to show that $|0\rangle$ and $|1\rangle$ are orthogonal and that their norm is 1

<u>properties of the scalar product between 2 vectors</u> $|\psi_1\rangle$ and $|\psi_2\rangle$ written as:

$\langle\psi_1|\psi_2\rangle$ ← together they form a BRA-KET ($\langle\cdot|$ $|\cdot\rangle$)

$\langle\psi_1|\psi_2\rangle = \underline{\gamma \in \mathbb{C}}$!

1) <u>linearity in the second argument</u>

$\langle\varphi|(\lambda_1|\psi_1\rangle + \lambda_2|\psi_2\rangle)\rangle = \lambda_1\langle\varphi|\psi_1\rangle + \lambda_2\langle\varphi|\psi_2\rangle$ which belongs to the same vector space from which we started

2) <u>conjugate symmetry</u>

$\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^*$ — scalar product inverted and conjugated (if the space was <u>NOT</u> complex but rather it was real then the scalar product is simply commutative)

3) <u>positivity</u>

$\langle\psi|\psi\rangle \geq \emptyset$ (this inequality implies that $\langle\psi|\psi\rangle \in \mathbb{R}$)

and $\langle\psi|\psi\rangle = \emptyset \iff |\psi\rangle = \emptyset$ null <u>vector</u>

(not qubit)

due to this property we can consider $\| |\psi\rangle \|^2 = \langle \psi | \psi \rangle$ square norm of ψ

so the norm is $\| |\psi\rangle \| = \sqrt{\langle \psi | \psi \rangle}$

4) conjugate linearity in the first argument

$|\varphi\rangle = \lambda_1 |\varphi_1\rangle + \lambda_2 |\varphi_2\rangle$ 1^{st} qubit

$\langle \varphi | \psi \rangle = \lambda_1^* \langle \varphi_1 | \psi \rangle + \lambda_2^* \langle \varphi_2 | \psi \rangle$ (derives from ① + ②)

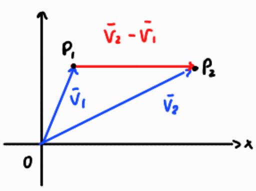
indeed:

$$\langle \lambda_1 \varphi_1 + \lambda_2 \varphi_2 | \psi \rangle \underset{\text{conj. sym.}}{=} \left(\langle \psi | \lambda_1 \varphi_1 + \lambda_2 \varphi_2 \rangle \right)^* \underset{\text{lin. of the second term}}{=} \left(\lambda_1 \langle \psi | \varphi_1 \rangle + \lambda_2 \langle \psi | \varphi_2 \rangle \right)^*$$

$$= \lambda_1^* \langle \psi | \varphi_1 \rangle^* + \lambda_2^* \langle \psi | \varphi_2 \rangle^* = \lambda_1^* \langle \varphi_1 | \psi \rangle + \lambda_2^* \langle \varphi_2 | \psi \rangle$$

distance

Euclidean vector space:

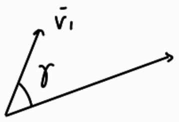


$$d(P_1, P_2) = \overline{P_1 P_2} = \underbrace{|\bar{v}_2 - \bar{v}_1|}_{\text{length of the signal}} = \sqrt{(\bar{v}_2 - \bar{v}_1) \cdot (\bar{v}_2 - v_1)}$$

in the complex Hilbert space:

$$d(|\psi_1\rangle, |\psi_2\rangle) = \sqrt{\langle \psi_2 - \psi_1 | \psi_2 - \psi_1 \rangle} = \| |\psi_2\rangle - |\psi_1\rangle \|$$

Cauchy-Schwarz inequality



$$\bar{v}_1 \cdot \bar{v}_2 = |\bar{v}_1| \cdot |\bar{v}_2| \cos \gamma$$

$$\Rightarrow |\bar{v}_1 \cdot \bar{v}_2| = |\bar{v}_1| \cdot |\bar{v}_2| \cdot \underbrace{|\cos \gamma|}_{\leq 1} \leq |\bar{v}_1| \cdot |\bar{v}_2|$$

and $|\bar{v}_1 \cdot \bar{v}_2| = |\bar{v}_1| \cdot |\bar{v}_2| \iff \underset{|\cos\gamma| = |1| = 1}{\gamma = 0^\circ} \vee \underset{|\cos\gamma| = |-1| = 1}{\gamma = 180^\circ} \Rightarrow$ the 2 vectors are in $\underbrace{\text{parallel}}_{0^\circ}$ or $\underbrace{\text{antiparallel}}_{180^\circ}$

mathematically speaking this means that the two vectors are linearly dependent (one vector is the multiple of the other)

we can extend this consideration to qubits

$$|\langle \psi_1 | \psi_2 \rangle| \leq \underbrace{\| |\psi_1\rangle \|}_{\in \mathbb{C}} \cdot \underbrace{\| |\psi_2\rangle \|}_{\in \mathbb{C}}$$

and $|\langle \psi_1 | \psi_2 \rangle| = \| |\psi_1\rangle \| \cdot \| |\psi_2\rangle \| \iff |\psi_1\rangle$ and $|\psi_2\rangle$ are linearly dependent (extending the concept from the Euclidean space). That is, $|\psi_1\rangle = \alpha |\psi_2\rangle$ and $|\psi_2\rangle = \beta |\psi_1\rangle$ with $\alpha, \beta \in \mathbb{C}$

we can define the <u>angle between the qubits</u>:

from Euclidean space $|\cos\gamma| = \frac{|\bar{v}_1 \cdot \bar{v}_2|}{|\bar{v}_1| \cdot |\bar{v}_2|} \Rightarrow \cos^2\gamma = \frac{(\bar{v}_1 \cdot \bar{v}_2)^2}{|\bar{v}_1|^2 \cdot |\bar{v}_2|^2}$

this can be extended to the Hilbert space

= $\langle \Psi_2 | \Psi_1 \rangle$ (conjugate symmetry)

$$|\cos\gamma| = \frac{|\langle \Psi_1 | \Psi_2 \rangle|}{\|\Psi_1\| \cdot \|\Psi_2\|} \Rightarrow \cos^2\gamma = \frac{|\langle \Psi_1 | \Psi_2 \rangle|^2}{\|\Psi_1\|^2 \cdot \|\Psi_2\|^2} = \frac{\langle \Psi_1 | \Psi_2 \rangle \cdot \langle \Psi_1 | \Psi_2 \rangle^*}{\langle \Psi_1 | \Psi_1 \rangle \cdot \langle \Psi_2 | \Psi_2 \rangle}$$

$|z|^2 = z \cdot z^*$

fidelity between quantum states

=> these properties refer to all quantum states in a Hilbert space of finite or infinite dimension

$$\Rightarrow \boxed{F(|\Psi_1\rangle, |\Psi_2\rangle) = \frac{\langle \Psi_1 | \Psi_2 \rangle \cdot \langle \Psi_2 | \Psi_1 \rangle}{\langle \Psi_1 | \Psi_1 \rangle \cdot \langle \Psi_2 | \Psi_2 \rangle}}$$

<u>degree of similarity between two quantum states</u>

$\cos^2\gamma \le 1$ (Cauchy-Schwarz)

$$\phi \le F(|\Psi_1\rangle, |\Psi_2\rangle) \le 1$$

all quantities are non-negative

<u>note</u>: we should set $|\Psi_1\rangle \neq 0 \wedge |\Psi_2\rangle \neq 0$

↳ <u>the null vector doesn't define any quantum state!</u>

$$F(\psi_1,\psi_2) = \frac{|\langle\psi_1|\psi_2\rangle|^2}{\|\psi_1\|^2\cdot\|\psi_2\|^2} = \frac{\langle\psi_1|\psi_2\rangle\cdot\langle\psi_2|\psi_1\rangle}{\langle\psi_1|\psi_1\rangle\cdot\langle\psi_2|\psi_2\rangle}$$

generic vector in the Hilbert space

$$0 \le F(\psi_1,\psi_2) \le 1$$

normalization of a non-null vector:

$\boxed{\psi' = \frac{\psi}{\|\psi\|}}$ normalized state $(\psi \neq 0)$

=> in Dirac notation => $|\psi'\rangle = \frac{|\psi\rangle}{\sqrt{\langle\psi|\psi\rangle}}$

this is a scalar number

note: if $\|\psi\| \to +\infty$ this normalization process would not be possible as it would lead to a null vector which describes a meaningless quantum state

$$\|\,|\psi'\rangle\|^2 = \langle\psi'|\psi'\rangle = \left\langle \frac{\psi}{\sqrt{\langle\psi|\psi\rangle}}, \frac{\psi}{\sqrt{\langle\psi|\psi\rangle}} \right\rangle = \frac{1}{\sqrt{\langle\psi|\psi\rangle}}\cdot\frac{1}{\sqrt{\langle\psi|\psi\rangle}}\cdot\langle\psi|\psi\rangle = \frac{\langle\psi|\psi\rangle}{\langle\psi|\psi\rangle} = 1$$

=> so the norm of the normalized vector is always $= 1$

$$\Rightarrow F(\psi_1',\psi_2') = \frac{|\langle\psi_1',\psi_2'\rangle|}{\underbrace{\|\psi_1'\|^2}_{1}\cdot\underbrace{\|\psi_2'\|^2}_{1}} = |\langle\psi_1',\psi_2'\rangle|$$

case fidelity $= 0$ (0%)

=> $F(\psi_1,\psi_2) = \emptyset \iff \langle\psi_1,\psi_2\rangle = 0 \iff \psi_1$ and ψ_2 are orthogonal

↳ just like in Euclidean geo. $\bar{v}_1\cdot\bar{v}_2 = \emptyset$ when $\bar{v}_1 \perp \bar{v}_2$

=> the two states are maximally different

case fidelity $= 1$ (100%)

$F(\psi_1,\psi_2) = 1$ when ψ_1,ψ_2 are linearly dependent => $(\underbrace{\psi_1 = \alpha'\psi_2}$ or $\underbrace{\psi_2 = \beta'\psi_1})$

the double condition is needed when $\psi_1 \vee \psi_2$ could be $= 0$. However in our case since $\psi_1,\psi_2 \neq 0$ one of the two conditions is suff.

this derives from the Cauchy-Schwarz inequality:

$$\frac{|\langle\psi_1|\psi_2\rangle|^2}{\|\psi_1\|^2\cdot\|\psi_2\|^2} \le \frac{\|\psi_1\|^2\cdot\|\psi_2\|^2}{\|\psi_1\|^2\cdot\|\psi_2\|^2} = 1$$

$$|\langle\psi_1|\psi_2\rangle| \le \|\psi_1\|^2\|\psi_2\|^2$$

fidelity is $= 1$ when the equality holds, which is when they are lin. dependent

=> 100% fidelity, the two states are essentially identical

$|\psi_1\rangle$ and $\alpha|\psi_1\rangle$ represent the same quantum state

complex scalar coeff.

=> we can identify a quantum state by a normalized vector (apart from a phase factor that is a complex coeff. w/ modulus 1)

if $|\alpha| = 1$ => $\alpha = |\alpha|\cdot e^{j\alpha}$ => $\alpha = e^{j\alpha}$ is just a phase factor

$\| |\varphi_1\rangle \|^2 = 1$ ← φ_1 normalized

$\| \alpha |\varphi_1\rangle \|^2 = \langle \alpha\varphi_1 | \alpha\varphi_1 \rangle = \alpha \langle \alpha\varphi_1 | \varphi_1 \rangle = \underbrace{\alpha\cdot\alpha^*}_{|\alpha|^2} \cdot \langle \varphi_1 | \varphi_1 \rangle = |\alpha|^2 \underbrace{\|\varphi_1\|^2}_{=1}$

so: $\| \alpha |\varphi_1\rangle \|^2 = \| |\varphi_1\rangle \|^2$ so it remains normalized

properties of fidelity

1) $0 \le F(\varphi_1, \varphi_2) \le 1$

2) $F(\varphi_1, \varphi_2) = \emptyset \iff \varphi_1$ orthogonal φ_2 => max. different quantum states

3) $F(\varphi_1, \varphi_2) = 1 \iff \varphi_1, \varphi_2$ lin. dep. => identical quantum states

4) symmetry: $F(\varphi_1, \varphi_2) = F(\varphi_2, \varphi_1)$: it is a property between not just vectors but more precisely quantum states

indeed:

$$F(\varphi_2, \varphi_1) = \frac{|\langle \varphi_2 | \varphi_1 \rangle|^2}{\|\varphi_2\|^2 \cdot \|\varphi_1\|^2} \underset{\text{conjugate symmetry}}{=} \frac{|\langle \varphi_1, \varphi_2 \rangle^*|^2}{\|\varphi_2\|^2 \cdot \|\varphi_1\|^2} \underset{\text{due to abs. val.}}{=} \frac{|\langle \varphi_1, \varphi_2 \rangle|^2}{\|\varphi_2\|^2 \cdot \|\varphi_1\|^2} = F(\varphi_1, \varphi_2)$$

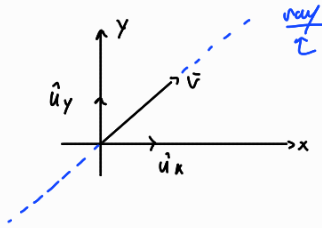
5) $F(\alpha\varphi_1, \beta\varphi_2) = F(\varphi_1, \varphi_2)$

indeed:

$$F(\alpha\varphi_1, \beta\varphi_2) = \frac{|\langle \alpha\varphi_1, \beta\varphi_2 \rangle|^2}{\|\alpha\varphi_1\|^2 \cdot \|\beta\varphi_2\|^2} = \frac{\|\alpha^*\cdot\beta \langle \varphi_1 | \varphi_2 \rangle\|^2}{|\alpha|^2 \cdot \|\varphi_1\|^2 \cdot |\beta|^2 \cdot \|\varphi_2\|^2} = \frac{\cancel{|\alpha|^2} \cdot \cancel{|\beta|^2} \cdot |\langle \varphi_1 | \varphi_2 \rangle|^2}{\cancel{|\alpha|^2} \cdot \cancel{|\beta|^2} \cdot \|\varphi_1\|^2 \cdot \|\varphi_2\|^2} = F(\varphi_1, \varphi_2)$$

a quantum state (defined in a quantum system) is identified by a $\underbrace{\text{ray}}$ of the considered Hilbert space

a linear subspace of dimension 1



ray in Euclidean space
↳ non oriented direction

defines a 1D subspace $\{\bar{v}\}$ base of the subspace

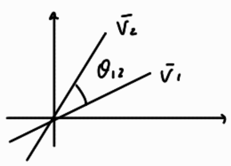
extending the concept to any complex coeff. vectorial space of finite or infinite space

describes all vectors on the $\underbrace{\text{ray}}$ => $\varphi = \alpha\tilde{\varphi}$ w/ any $\alpha \in \mathbb{C}$ and a given $\tilde{\varphi}$ non null vector

quantum state

1 : 1 correspondance between the quantum state and the elements of the ray (excluding the $\emptyset$ vector of the ray, that is, the origin)

$F(\varphi_2, \varphi_1) = \cos^2\theta_{12} = \dfrac{|\langle \varphi_1, \varphi_2 \rangle|^2}{\|\varphi_1\|^2 \cdot \|\varphi_2\|^2}$



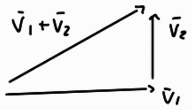
it is a "fictitous" angle. It's just an extension of the concept of angle in Euclidean geom.

when we are in the same ray: $\theta_{12} = \underbrace{0 \vee \pi}$ => $F = 1$

0 or π is irrelevant; rays are not oriented

if φ_1 orthogonal to φ_2 : $\theta_{12} = \pm \pi/2$ => $F = 0$

Pythagorean theorem



$$|\bar{v}_1 + \bar{v}_2|^2 = |\bar{v}_1|^2 + |\bar{v}_2|^2$$

w/ $\bar{v}_1 \perp \bar{v}_2$

in our Hilbert space:

$$\|\psi_1 + \psi_2\|^2 = \langle \psi_1 + \psi_2 | \psi_1 + \psi_2 \rangle = \langle \psi_1|\psi_1\rangle + \langle \psi_2|\psi_2\rangle + \underbrace{\langle \psi_1|\psi_2\rangle + \overbrace{\langle \psi_2|\psi_1\rangle}^{= \langle \psi_1|\psi_2\rangle^*}} = \|\psi_1\|^2 + \|\psi_2\|^2 + 2\mathrm{Re}[\langle \psi_1|\psi_2\rangle]$$

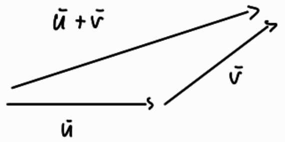
$\alpha = x + Jy$

$\alpha^* = x - Jy$ $\Rightarrow$ $\alpha + \alpha^* = 2x = 2\mathrm{Re}[\alpha]$

$\Rightarrow$ $\|\psi_1 + \psi_2\|^2 = \|\psi_1\|^2 + \|\psi_2\|^2$ if $\langle \psi_1|\psi_2\rangle = 0$

that is, if ψ_1 orthogonal to ψ_2 $\Rightarrow$ we obtain the "same" result as the Eucledean geom.

triangle inequality



$$|\bar{u} + \bar{v}| \le |\bar{u}| + |\bar{v}|$$

[the equality holds when $\bar{u}$ and $\bar{v}$ are aligned

in Hilbert space:

$$\|\psi_1 + \psi_2\| \le \|\psi_1\| + \|\psi_2\|$$

indeed, starting from the result of the previous theo.:

$$\|\psi_1 + \psi_2\|^2 = \|\psi_1\|^2 + \|\psi_2\|^2 + 2\mathrm{Re}[\langle \psi_1|\psi_2\rangle]$$

interference term $\Rightarrow$ similar to interference when considering the intensity of waves

$$\left[\begin{array}{ll} \alpha = x + Jy & \\ \mathrm{Re}[\alpha] = x \le |\alpha| & (x \le \sqrt{x^2+y^2} = |\alpha|) \end{array}\right]$$

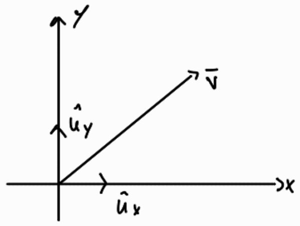
$$\|\psi_1 + \psi_2\|^2 = \|\psi_1\|^2 + \|\psi_2\|^2 + 2\mathrm{Re}[\langle \psi_1|\psi_2\rangle] \le \|\psi_1\|^2 + \|\psi_2\|^2 + 2|\langle \psi_1|\psi_2\rangle| \le \|\psi_1\|^2 + \|\psi_2\|^2 + 2\|\psi_1\|\cdot\|\psi_2\| = (\|\psi_1\| + \|\psi_2\|)^2$$

cauchy - schwarz:

$$|\langle \psi_1|\psi_2\rangle| \le \|\psi_1\|\cdot\|\psi_2\|$$

$\Rightarrow$ $\|\psi_1 + \psi_2\|^2 \le (\|\psi_1\| + \|\psi_2\|)^2$ $\Rightarrow$ $\|\psi_1 + \psi_2\| \le \|\psi_1\| + \|\psi_2\|$

Euclidean geometry (2D)



for each axis we will associate 2 particular vectors: $\hat{u}_x$, $\hat{u}_y$

$\underbrace{\|\hat{u}_x\| = \|\hat{u}_y\| = 1}$ and $\underbrace{\hat{u}_x \perp \hat{u}_y}$

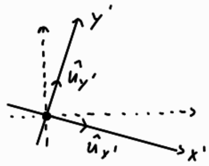
$|\hat{u}_x|^2 = |\hat{u}_y|^2 = 1$ $\quad\Rightarrow \hat{u}_x \cdot \hat{u}_y = 0$

$\Rightarrow \hat{u}_x \cdot \hat{u}_x = \hat{u}_y \cdot \hat{u}_y = 1$ $\quad (\|\vec{x}\| = \sqrt{\vec{x} \cdot \vec{x}} = |x|)$

$\hat{u}_x, \hat{u}_y$ form an orthonormal basis of our 2D Euclidean space

basis: complete set of linearly independent vectors
↳ any vector of the space can be expanded as a linear superposition of basis vectors

obs. there is an ∞ n° of possible basis': just rotate the axis



cardinality: n° of vectors in the basis $\Leftrightarrow$ dim. of the space

conditions on the elements of the orthonormal basis
- orthogonality: $\hat{u}_x \cdot \hat{u}_y = 0$
- normalization: $\begin{cases} \hat{u}_x \cdot \hat{u}_x = 1 \\ \hat{u} \cdot \hat{u}_y = 1 \end{cases}$

N-dimension Euclidean space

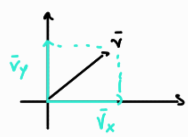
basis: $\{\hat{u}_n : n = 0, 1, \ldots, D-1\}$ where D is the dimension of the space

orthonormality condition $\Rightarrow$ $\hat{u}_n \cdot \hat{u}_y = \delta_{mn}$ — kronecker delta (descrete version of the Dirac δ)

δ_{mn}
- 0 for $m \neq n$
- 1 for $m = n$

note: completeness is guaranteed in the case of a finite dim. space (in the case of an ∞ dim. Hilbert space, this will require a completeness theo.)

orthonormal projection (2D):



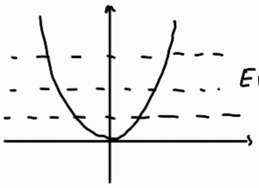
$\vec{v} = \vec{v}_x + \vec{v}_y = v_x \cdot \hat{u}_x + v_y \hat{u}_y$

scalar $\Rightarrow$ NOT the modulus, since v_x, v_y may be negative

$\hat{u}_x \cdot \vec{v} = \underbrace{\hat{u}_x \cdot v_x \hat{u}_x}_{1} + \underbrace{\hat{u}_x \cdot v_y \hat{u}_y}_{0} = v_x$

likewise: $\hat{u}_y \cdot \vec{v} = v_y$

now considering quantum systems (Hilbert spaces)



$E_n = (n+\frac{1}{2})h\nu \quad n = 0, 1, 2, \dots,$

quantum system $\longleftrightarrow$ Hilbert space w/ dimension either finite or infinite

countable / not countable

=> we will consider either finite or infinite countable spaces

"all Cauchy series in the space converge in the same space"

from the completeness theo. of Hilbert spaces

$\Downarrow \qquad \cancel{\Uparrow}$

existence of a (orthonormal) basis

considering finite dim. D Hilbert space or finite countable:

any vector ψ can be expanded as: $\psi = \sum_{n=0}^{D-1} \lambda_n \psi_n$

scalar complex coeff. of the expansion of ψ in the orthonormal basis $\{\psi_n : n = 0, 1, 2, \dots, \}$

orthonormality condition for the basis of the Hilbert space:

=> $\langle \psi_m | \psi_n \rangle = \delta_{mn}$ (there are ∞ orthonormal basis but all w/ the same n° of elements = D)

D = 2 (QUBIT)

D = 3 (QUTRIT)

D = finite integer (QUDIT)

(notation: $\sum_n \lambda_n \psi_n \iff \sum_{n=0}^{D-1} \lambda_n \psi_n$ or $\lim_{N\to\infty} \sum_{n=0}^{N-1} \lambda_n \psi_n$)

the convergence of the series is guaranteed by the completeness theo.

$\lim_{N\to\infty} d(\psi, \sum_{n=0}^{N} \lambda_n \psi_n) = 0 \Rightarrow \lim_{N\to\infty} \| \psi - \sum_{n=0}^{N} \lambda_n \psi_n \| = 0$

$\langle \psi_n | \psi \rangle = \langle \psi_n | \sum_{n=0}^{\infty} \lambda_m \psi_m \rangle = \sum_{m=0}^{D-1} \lambda_m \langle \psi_n | \psi_m \rangle = \sum_{m=0}^{D-1} \lambda_m \cdot \underbrace{\delta_{mn}}_{\neq 0 \text{ for } m=n} = \lambda_m = \lambda_n$

orthonormality

$m = n$

this is the generalization of the orthonormal projection

[linearity of the second term:
$\langle \psi_n | \alpha_1 \varphi_1 + \alpha_2 \varphi_2 \rangle = \alpha_1 \langle \psi_n | \varphi_1 \rangle + \alpha_2 \langle \psi_n | \varphi_2 \rangle$]

from the Cauchy-Schwarz inequality we can derive

$\Downarrow$

continuity of the scalar product (in both arguments)

↳ (we can move the lim. inside or outside the scalar prod.) $\Rightarrow \lim_{n,m\to\infty} \langle \psi_m | \varphi_n \rangle = \langle \lim_{m\to\infty} \psi_m , \lim_{n\to\infty} \varphi_n \rangle$

any quantum state is described by a non-null vector : $\psi \in \mathbb{H}$ $(\psi \neq 0)$

normalized vector: $\tilde{\psi} = \frac{\psi}{\|\psi\|} = \frac{\psi}{\sqrt{\langle\psi|\psi\rangle}}$ $\tilde{\psi}$ and ψ represent the same quantum state

quantum state : $\psi = \alpha \tilde{\psi}$ $\alpha \in \mathbb{C} \neq 0$

normalizability is guaranteed by the fact that $\psi \neq 0$ and that $0 \leq \|\psi\| < +\infty$

$\mathbb{H}^*$ dual space: space formed by continuous linear functionals on $\mathbb{H}$ $G: \mathbb{H} \longrightarrow \mathbb{C}$

lin. : $G(\alpha\psi + \beta\varphi) = \alpha G(\psi) + \beta G(\varphi)$

cont. : $G(\lim_{N\to\infty} \psi_N) = \lim_{N\to\infty} G(\psi_N)$

the functionals of the space $\mathbb{H}^*$ must be:

- linear: $G(\alpha\psi+\beta\varphi)=\alpha G(\psi)+\beta G(\varphi)$
- continuous: $G\left(\lim_{N\to\infty}\psi_N\right)=\lim_{N\to\infty}G(\psi_N)$

note on projections:

in a Euclidean space $\Rightarrow$ $\bar{v}=v_x\hat{u}_x+v_y\hat{u}_y$ where $\begin{cases} v_x=\bar{v}\cdot\hat{u}_x \\ v_y=\bar{v}\cdot\hat{u}_y \end{cases}$

$\therefore$ $|\bar{v}|$ may be computed using Pythagoras' theo: $|\bar{v}|=\sqrt{v_x^2+v_y^2}$

this concept can also be extended to a Hilbert space:

1) finite dimension D: $\|\psi\|^2=\sum_{n=0}^{D-1}|\overbrace{\langle\psi_n|\psi\rangle}^{\lambda_n}|^2=\sum_{n=0}^{D-1}|\lambda_n|^2$ [orthogonal projection along the n-th dimension: λ_n]

where $\{\psi_n\}_{n=0}^{D-1}$ is an orthonormal basis and $\psi=\sum_{n=0}^{D-1}\lambda_n\psi_n$

coeff. that describe ψ as a linear superposition of the elements of the basis

2) infinite countable: $\|\psi\|^2=\sum_{n=0}^{\infty}|\langle\psi_n|\psi\rangle|^2=\sum_{n=0}^{\infty}|\lambda_n|^2$

where $\{\psi_n\}_{n=0}^{\infty}$ is an infinite countable orthonormal bases and the infinite dim. has to be intended in terms of convergence in the norm (we know that if $\psi\in\mathbb{H}$ we will have $\|\psi\|<+\infty$ by def., $\therefore$ the infinite sum will converge)

$\hookrightarrow$ this identity derived for ∞ countable dimension Hilbert spaces is also known as Parseval's theo. (generalization of Pythagoras' theo. in ∞ dimensions)

dim.

[$\langle\lambda\psi|\varphi\rangle=\lambda^*\langle\psi|\varphi\rangle$ conj. lin. of the 1st term]

[lin. of the 2nd term]

$$\|\psi\|^2=\langle\psi|\psi\rangle=\left\langle\sum_n\lambda_n\psi_n\,\Big|\,\sum_m\lambda_m\psi_m\right\rangle=\sum_n\lambda_n^*\langle\psi_n|\sum_m\psi_m\rangle=\sum_n\sum_m\lambda_n^*\cdot\lambda_m\langle\psi_n|\psi_m\rangle$$

elements of the orthonormal bases

note: we are able to move the ∞ sum $\sum_n$ outside the scalar product thanks to the linearity of the scalar prod.

$$=\sum_n\sum_m\lambda_n^*\lambda_m\cdot\delta_{nm}=\sum_n\lambda_n^*\cdot\lambda_n=\sum_n|\lambda_n|^2$$

δ_{nm}: 0 if $n\neq m$, 1 if $n=m$

orthonormality condition

$\hookrightarrow$ this identity (Parseval's theo.) holds both for finite and infinite countable dimension Hilbert spaces

representation theorem (foundation of the Dirac notation)

we want to highlight the connection between the Hilbert space whose elements describe our quantum states and the dual space H^* whose elements are the continuous linear functionals on H (functional $\Leftrightarrow$ operator/function that maps an element of the Hilbert space which is a vector to a complex scalar number)

in the finite case, the continuity of functionals is guaranteed, but not in the ∞ dim. case. However we need both continuity and linearity for the Riesz representation theo.

Riesz representation theo.

there is a mapping between $\mathbb{H}$ and $\mathbb{H}^*$ w/ the following properties:

1) bijective mapping between $\mathbb{H}$ and $\mathbb{H}^*$ (one-to-one correspondance between a vectorial element of $\mathbb{H}$ and a corresponding functional of $\mathbb{H}^*$)
2) conjugate linear mapping
3) isometric mapping (the norm is conserved)
4) H^* is an Hilbert space
5) the mapping is reflexive : $(\mathbb{H}^*)^* = \mathbb{H}$

this mapping is def. by the scalar product

$$\varphi \in \mathbb{H} \xrightarrow[\text{MAP}]{\text{DUALITY}} G\varphi \in \mathbb{H}^*$$

linear and continuous functional associated to φ

in particular: $G_\varphi(\psi) = \langle \varphi | \psi \rangle \quad \forall \psi \in \mathbb{H}$

the functional $G_\varphi(\cdot) = \langle \varphi | \cdot \rangle$ is both linear and continous

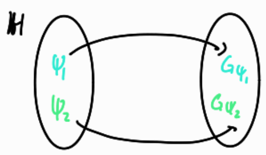
linearity: $G_\varphi(\alpha\psi_1 + \beta\psi_2) = \langle \varphi | \alpha\psi_1 + \beta\psi_2 \rangle \underset{\text{lin. of the second term}}{=} \alpha\langle \varphi|\psi_1\rangle + \beta\langle\varphi|\psi_2\rangle = \alpha G_\varphi(\psi_1) + \beta G_\varphi(\psi_2)$

continuity: this is given by the continuity of the scalar prod. for both finite and ∞ contable dim.

so $\Rightarrow$ $\underline{G_\varphi : \mathbb{H} \longrightarrow \mathbb{C} \quad \in \mathbb{H}^*}$

we have to show that this mapping is bijective, which means it is both injective and surjective

1) injective dual mapping



if $\varphi_1 \neq \varphi_2 \Rightarrow G_{\varphi_1} \neq G_{\varphi_2}$, which means that for any element of $\mathbb{H}^*$ there will be at max. one element in $\mathbb{H}$ (a zero or one in the mapping)

$\hookrightarrow$ no ambiguity in the mapping

equivalently: if $G_{\varphi_1} = G_{\varphi_2} \Rightarrow \varphi_1 = \varphi_2$

dim.

starting from $G_{\psi_1} = G_{\psi_2} \Rightarrow \langle \psi_1 | \cdot \rangle = \langle \psi_2 | \cdot \rangle \Rightarrow \langle \psi_1 | \varphi \rangle = \langle \psi_2 | \varphi \rangle \quad \forall \varphi \in \mathbb{H}$

$\Rightarrow \langle \psi_1 | \varphi \rangle - \langle \psi_2 | \varphi \rangle = 0 \Rightarrow \langle \psi_1 - \psi_2 | \varphi \rangle = \emptyset \quad \forall \varphi \in \mathbb{H}$

[conj. lin. of the first term]

(no conj since coeff. is 1)

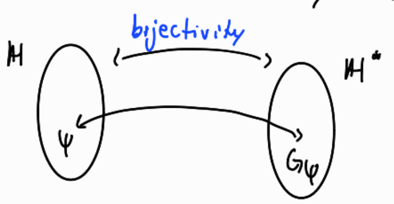
↳ so we may choose $\varphi = \psi_1 - \psi_2$

$\Rightarrow \langle \psi_1 - \psi_2 | \psi_1 - \psi_2 \rangle = \| \psi_1 - \psi_2 \|^2 = \emptyset \iff \psi_1 - \psi_2 = 0$ by def. of norm

so: $\psi_1 = \psi_2$

2) subjective dual mapping (Riesz theo.)

any continuous linear functional $G \in \mathbb{H}^*$ is the image (or the transformed element by the duality mapping defined by the scalar prod.) of one vector of $\mathbb{H}$ (at least one, but due to the injectivity we know that it will be only one)



$\Rightarrow$ quantum state ψ can be represented by $G_\psi = \langle \psi | \cdot \rangle$

BRA (c) KET notation

for the Riesz theo. each quantum state which is an element of an Hilbert space H can be univocally represented by $G_\psi = \langle \psi | \cdot \rangle \in \mathbb{H}^*$ which is the scalar prod. between ψ and any other element of $\mathbb{H}$

the idea is to shorten the notation of $G_\psi = \langle \psi | \cdot \rangle$ to $\langle \psi |$ which is the so-called BRA

↳ Riesz' theo. $\Rightarrow$ this represents exactly the quantum state ψ

we can identify $\mathbb{H}_{BRA} = \mathbb{H}^*$ while for duality we can rewrite the vectors of $\mathbb{H}$ as KETS $\Rightarrow$ $\psi \iff |\psi\rangle$ (it's just a change of notation). So, $\mathbb{H}_{KET} = \mathbb{H}$. All the properties of the vectors remain the same

$$\alpha_1 \psi_1 + \alpha_2 \psi_2 \longrightarrow |\alpha_1 \psi_1 + \alpha_2 \psi_2 \rangle = \alpha_1 |\psi_1\rangle + \alpha_2 |\psi_2\rangle$$

completely identical ways to represent a quantum system

according to Riesz' theorem we can also have another representation

$$\text{QUANTUM SYSTEM} \xrightarrow[\text{"}\dagger\text{"}]{\text{Riesz}} \mathbb{H}_{BRA} = \mathbb{H}^*$$

dagger symbol $\Rightarrow$ identifies duality mapping

note: the element of $\mathbb{H}_{BRA}$ are not vectors but rather functionals. Nonetheless, they describe the $\mathbb{H}$ space for bijective mapping

$\Rightarrow$ we can say that: $\langle \psi | = |\psi\rangle^\dagger$ (the BRA is the dual of the KET for the same quantum state)

obs. due to the duality mapping, we have conjugate linearity

$$\Rightarrow \langle \alpha_1\psi_1 + \alpha_2\psi_2| = |\alpha_1\psi_1 + \alpha_2\psi_2\rangle^\dagger = \alpha_1^* \cdot |\psi_1\rangle^\dagger + \alpha_2^*|\psi_2\rangle^\dagger = \alpha_1^*\langle\psi_1| + \alpha_2^*\langle\psi_2|$$

note the difference:

$$\alpha_1\psi_2 + \alpha_2\psi_2 = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle = \alpha_1^*\langle\psi_1| + \alpha_2^*\langle\psi_2|$$

"BRA" notation "KET" notation

the main diff. is the conjugation of coeff.

dim. (conjugate lin. of the mapping)

the BRA $\langle\psi|$ corresponds to $\langle\psi|\cdot\rangle$ continuous linear functional given by the scalar product

$\psi = \alpha_1\psi_1 + \alpha_2\psi_2 \in \mathbb{H}$ and $\mathbb{H}$'s corresponding BRA $\Rightarrow \langle\psi| = \langle\alpha_1\psi_1 + \alpha_2\psi_2|$ which can be written as:

$$\langle\psi|\cdot\rangle = \langle\alpha_1\psi_1 + \alpha_2\psi_2|\cdot\rangle \underset{\substack{\text{scalar prod.}\\ \text{conjugate lin.}}}{=} \alpha_1^*\langle\psi_1|\cdot\rangle + \alpha_2^*\langle\psi_2|\cdot\rangle = \alpha_1^*\langle\psi_1| + \alpha_2^*\langle\psi_2| \quad \forall\psi\in\mathbb{H}$$

so we get:

$$\langle\psi| = \alpha_1^*\langle\psi_1| + \alpha_2^*\langle\psi_2| \quad \text{if } \psi = \alpha_1\psi_1 + \alpha_2\psi_2$$

we can also demonstrate that $\mathbb{H}^*$ is an Hilbert space w/ the scalar product between $G_{\psi_1} + G_{\psi_2} \in \mathbb{H}^*$ is given by $\langle G_{\psi_1}|G_{\psi_2}\rangle = \langle\psi_1|\psi_2\rangle^* = \langle\psi_2|\psi_1\rangle$ $\forall G_{\psi_1}, G_{\psi_2} \in \mathbb{H}^*$ and $\psi_1,\psi_2 \in \mathbb{H}$

this also implies that the mapping is isometric

$\langle G_{\psi_1}|G_{\psi_2}\rangle = \langle\psi_1|\psi_1\rangle$ the mapping preserves the norm $\Rightarrow \|G_{\psi_1}\|^2 = \|\psi_1\|^2$

we can also say that: $\|\langle\psi_1|\|^2 = \|G_{\psi_1}\|^2 = \langle G_{\psi_1}|G_{\psi_1}\rangle = \langle\psi_1|\psi_1\rangle = \|\psi_1\|^2 = \||\psi_1\rangle\|^2$

the norm of the BRA is the same as the norm of the KET

also the mapping is reflexive $\Rightarrow (\mathbb{H}^*)^* = \mathbb{H}$ which means that: $(|\psi\rangle^\dagger)^\dagger = \langle\psi|^\dagger = |\psi\rangle$

↳ BRA and KETS are dual

we can also define that for a scalar $\alpha \in \mathbb{C}$ $\alpha^\dagger = \alpha^*$. This is a force of notation, however it is useful

finally we can say: $\langle\psi_1|\psi_2\rangle^\dagger = \langle\psi_1|\psi_2\rangle^* = \langle\psi_2|\psi_1\rangle$

let's write the scalar product in terms of expansion of coeff.

$$\psi' = \sum_m \lambda_m' \varphi_m$$
$$\psi'' = \sum_n \lambda_n'' \varphi_n \qquad \text{w/ } \{\varphi_n\} \text{ orthonormal basis of } \mathbb{H}$$

with $n = 0, 1, 2, \dots$, or n countable ∞

$$\psi', \psi'' \in \mathbb{H}$$

the scalar product is: $\langle \psi' | \psi'' \rangle = \langle \sum_m \lambda_m \varphi_m | \sum_n \lambda_n \varphi_n \rangle = \sum_m (\lambda_m')^* \langle \varphi_m | \sum_n \lambda_n'' \varphi_n \rangle = \sum_{m,n} (\lambda_m')^* \cdot \lambda_n'' \cdot \underbrace{\langle \varphi_m | \varphi_n \rangle}_{\delta_{mn}}$

this can be done both in the finite and ∞ countable case thanks to the continuity of the scalar product

δ_{mn} : $\varphi_m, \varphi_n \in$ orthonormal bases

$\neq 0$ only for $m = n$

$\Rightarrow$ $\langle \psi' | \psi'' \rangle = \sum_m \lambda_m'^* \cdot \lambda_m''$ v. important!

if we move to the BRA-KET notation:

$$|\psi'\rangle = \sum_m \lambda_m' |\varphi_m\rangle$$
$$|\psi''\rangle = \sum_n \lambda_n'' |\varphi_n\rangle$$

we have previously shown that $\begin{cases} \lambda_m' = \langle \varphi_m | \psi' \rangle \\ \lambda_n'' = \langle \varphi_n | \psi'' \rangle \end{cases}$ generalization of the orthonormal projection in an Hilbert space

we have also just seen: $\langle \psi' | \psi'' \rangle = \sum_m (\lambda_m')^* \cdot \lambda_m''$

so we can write it in a matrix form

$$|\psi''\rangle \xrightarrow[\text{orthonormal basis } \{|\varphi_m\rangle\}]{\text{for a given}} \begin{bmatrix} \lambda_0'' = \langle \varphi_0 | \psi'' \rangle \\ \lambda_1'' = \langle \varphi_1 | \psi'' \rangle \\ \vdots \\ \lambda_m'' = \langle \varphi_m | \psi'' \rangle \end{bmatrix}$$

column of expansion coeff.

every KET in a given orthonormal basis is represented by the column vector formed by the exp. coeff. (you can reconstruct $|\psi'\rangle = \sum \lambda_m' \varphi_m$)

$\langle \psi' | = |\psi'\rangle^\dagger$ (linear functional obtained by the dual mapping described by the scalar product)

since we can apply the dagger notation to the expansion we obtain:

$$\langle \psi' | = |\psi'\rangle^\dagger = \left(\sum_n \lambda_n' |\varphi_n\rangle\right)^\dagger = \sum_n (\lambda_n')^* |\varphi_n\rangle^\dagger = \sum_n (\lambda_n')^* \langle \varphi_n |$$

[dagger is continuous and conjugated linear]

so $\langle \psi' | = \sum_n (\lambda_n')^* \langle \varphi_n |$ and we can associate to the BRA a row vector in the same basis but described in the dual space of the BRA

row of conj. expansion coeff.

$$\langle \psi' | \xrightarrow[\text{orthonormal basis } \{\langle \varphi_n |\}]{\text{for a given}} \begin{bmatrix} (\lambda_0')^* & (\lambda_1')^* & \dots \end{bmatrix}$$

where $(\lambda_m')^* = (\langle \varphi_m | \psi' \rangle)^* = (\langle \psi' | \varphi_m \rangle^*)^* = \langle \psi' | \varphi_m \rangle$

the fundamental aspects for the BRA representation are the conjugate and the fact that the expansion is written in terms of a row vector obs. In BRA-KET notation it is natural to close the BRA (c) KET. Indeed, for the KET expansion we write the expansion coeff. of $|\psi''\rangle$ as $\lambda_m'' = \langle \psi_m | \psi'' \rangle$, so, using a BRA. On the other hand, the expansion coeff. of $\langle \psi' |$ is written as $(\lambda_m')^* = \langle \psi' | \psi_m \rangle$, so, using a KET.

so we can write:

$$\boxed{|\psi'\rangle} = \sum_m \lambda_m' |\psi_m\rangle = \overbrace{\sum_m |\psi_m\rangle \langle \psi_m|}^{\hat{I}_{KET}} \underbrace{|\psi'\rangle}$$

exp. coeff. for KET

$$\boxed{\langle \psi'' |} = \sum_n (\lambda_n'')^* \langle \psi_n'' | = \underbrace{\sum_n \langle \psi_n | \langle \psi''|}_{\hat{I}_{BRA}} \underbrace{|\psi_n\rangle}$$

exp. coeff. for BRA

we have written the KET expansion as a coloumn and the BRA expansion as a row so that we can write the scalar product as a matricial product:

$$\boxed{\langle \psi' | \psi'' \rangle} = \sum_n (\lambda_n')^* \lambda_m = [(\lambda_0')^* \ (\lambda_1')^* \ \dots \ (\lambda_n')^*] \cdot \begin{bmatrix} \lambda_0'' \\ \lambda_1'' \\ \vdots \\ \lambda_m'' \end{bmatrix}$$

=> we move to simple matricial algebra

note that in matrix algebra the dagger notation becomes the conjugated transposition

$$\Rightarrow |\psi\rangle^\dagger = \langle \psi | \Rightarrow \begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \end{bmatrix}^\dagger = \underbrace{[\lambda_0^* \ \lambda_1^* \ \dots]}_{\text{transposed and conjugated}}$$

in this way we reduced the scalar product to a matrix product. By "forcing" a notation we can write that:

$$\boxed{\alpha^\dagger = \alpha^*} \quad \alpha \in \mathbb{C} \text{ complex scalar}$$

"conj. transposition"

It is a forced notation since † is a dual mapping between vectors not scalars

this can be useful to write: $|\alpha\psi\rangle^\dagger = \alpha^* \langle\psi|$ which can also be seen in terms of matrix algebra:

$$\left(\alpha \begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \end{bmatrix}\right)^\dagger = \begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \end{bmatrix}^\dagger \alpha^\dagger = \alpha^* [\lambda_0^* \ \lambda_1^* \ \dots]$$

[in matrix algebra "†" is antidistributive w.r.t. the product by a scalar and vector]

$$\begin{bmatrix} \alpha\lambda_0 \\ \alpha\lambda_1 \\ \vdots \end{bmatrix} = [\alpha^* \lambda_0^* \ \ \alpha \lambda_1^* \ \dots]$$

scalar product between 2 quantum states described by vectors ψ_1 and ψ_2 in $\mathbb{H}$:

using KET representation: $\mathbb{H}_{KET} = \mathbb{H}$; $\langle \psi_1 | \psi_2 \rangle$

$\Updownarrow$ duality map

using BRA representation: $\mathbb{H}_{BRA} = \mathbb{H}^*$; $\langle \psi_2 | \psi_1 \rangle$

rule of thumb: to write the scalar prod. in the BRA space reverse the 1st term to a KET

bijective and reflexive : $|\psi\rangle^\dagger = \langle\psi|$; $\langle\psi|^\dagger = |\psi\rangle \Rightarrow \langle\psi| \rightleftharpoons |\psi\rangle$

$$\langle\varphi_1|\varphi_2\rangle \underset{\dagger}{\overset{\dagger^{-1}=\dagger}{\rightleftharpoons}} \langle\varphi_2|\varphi_1\rangle = \langle\varphi_1|\varphi_2\rangle^*$$ ← another motivation to consider $\alpha^\dagger = \alpha^*$

$$\langle\varphi'|\varphi''\rangle = [\lambda_0'^* \ \lambda_1'^* \dots] \begin{bmatrix}\lambda_0'' \\ \lambda_1'' \\ \vdots\end{bmatrix} = (\lambda_0')^*\lambda_0'' + (\lambda_1')^*\lambda_1'' + \dots$$

antidistributive

$$\Rightarrow (\langle\varphi'|\varphi''\rangle)^\dagger = |\varphi''\rangle^\dagger\langle\varphi'|^\dagger = \langle\varphi''|\varphi'\rangle = \langle\varphi'|\varphi''\rangle^* = \left([\lambda_0'^* \ \lambda_1'^* \dots]\cdot\begin{bmatrix}\lambda_0'' \\ \lambda_1'' \\ \vdots\end{bmatrix}\right)^\dagger = \begin{bmatrix}\lambda_0'' \\ \lambda_1'' \\ \vdots\end{bmatrix}^\dagger [\lambda_0'^* \ \lambda_1'^* \dots]^\dagger$$

$$= [\lambda_0''^* \ \lambda_1''^* \dots] \begin{bmatrix}\lambda_0' \\ \lambda_1' \\ \vdots\end{bmatrix}$$ which is the conjugated of the initial matrix prod.

let's now consider a continuous linear operator $\hat{A}$ acting on $\mathbb{H}$

$\hat{A} : \mathbb{H} \longrightarrow \mathbb{H}$ $\quad \forall \psi \in \mathbb{H}$ there exists its image (a transformed vector through $\hat{A} \Rightarrow \psi'' = \hat{A}\psi'$

by using an operator we can transform an initial quantum state in a new quantum state in the same Hilbert space

for the majority of quantum computing applications we are interested in linearity

$$\hat{A}(\underbrace{\alpha_1\psi_1' + \alpha_2\psi_2'}_{\text{input: 1 © 2 elements of the superposition}}) = \alpha_1\hat{A}(\psi_1') + \alpha_2\hat{A}(\psi_2') = \underbrace{\alpha_1\psi_1'' + \alpha_2\psi_2''}_{\text{output}}$$

$$\underset{\text{input quantum state}}{\psi'} \longrightarrow \underset{\text{physical operator}}{\boxed{\hat{A}}} \longrightarrow \underset{\text{output quantum state}}{\psi''}$$

continuity is redundant (guaranteed by linearity) in finite dimensions while it is not guaranteed in ∞ dimensions

in general a continuous operator is defined as $\underbrace{\hat{A}(\psi_n)}_{\substack{\text{always intended in terms of norm} \\ \lim_{n\to\infty} \|\hat{A}(\psi_n) - \hat{A}(\psi)\| \to \emptyset}} \longrightarrow A(\psi)$ for $n \to \infty$ $\quad$ where $\psi_n \to \psi \Leftrightarrow \lim_{n\to\infty} \psi_n = \psi \Leftrightarrow \lim_{n\to\infty} \|\psi_n - \psi\| = \emptyset$

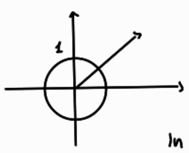
in practice the continuity allows us to move to move the limit inside the operator

$$\Rightarrow \lim_{n\to\infty} \hat{A}(\psi_n) = \hat{A}(\psi) = \hat{A}\left(\lim_{n\to\infty}\psi_n\right)$$

another property is that in an Hilbert space : <u>continuous linear operator on $\mathbb{H}$</u> $\Leftrightarrow$ <u>bounded linear operator</u>

a lin. op. is <u>bounded</u> if the image of all the normalized vectors is bounded in norm

in Euclidean geometry:



the set of all the vectors obtained by transforming a normalized vector must have a limited norm

In formal mathematical terms:

$\|\hat{A}\psi\|$: for any $\psi \in \mathbb{H}$ such that $\|\psi\| = 1 \Rightarrow \|\hat{A}\psi\| < M, \ M \in \mathbb{R}$

in case of finite dimension $\mathcal{H}$ any linear operator is also continuous and <u>bounded</u> and moreover it is represented in a given orthonormal basis $\{\psi_n\}_{n=0,1,\dots,D-1}$ by a $D \times D$ square matrix A of coeff. which are scalar complex that we name $A_{\underset{\text{row}}{m}\underset{\text{column}}{n}}$

<u>obs.</u> In case of a QUBIT A will be a 2×2 matrix

$$A = \begin{bmatrix} & \vdots & \\ \cdots & A_{mn} & \cdots \\ & \vdots & \end{bmatrix} = \begin{bmatrix} A_{00} & A_{01} & \cdots & A_{0\,D-1} \\ A_{10} & \ddots & & \vdots \\ \vdots & & \ddots & \\ A_{D-1\,0} & & \cdots & A_{D-1\,D-1} \end{bmatrix}$$

in BRA-KET notation: $A_{mn} = \langle \psi_m | \hat{A} \psi_n \rangle = \langle \psi_m | \hat{A} | \psi_n \rangle$

continuous and linear operator $\hat{A}$

$\psi' \longrightarrow \boxed{\hat{A}} \longrightarrow \psi''$ $\qquad \hat{A}: \mathbb{H} \longrightarrow \mathbb{H}$ (we assume $\mathbb{H} \equiv \mathbb{H}_{KET}$ so $\hat{A} = \hat{A}_{KET}$)

an operator on a quantum state can be represented both in KET and BRA space

when not specified we will assume that $\hat{A}$ operates on KET

↳ note that it is different: the operator acts "from the left" on the KET $\Rightarrow |\psi'\rangle \longrightarrow |\psi''\rangle = \hat{A}|\psi'\rangle$

we can represent it as a function of the orthonormal basis of $\mathbb{H}_{KET}$ $\{|\psi_n\rangle\}_{n=0,1,\dots,D-1}$ (finite dim.)
$n \in \mathbb{N}$ (∞ countable)

for any $|\psi'\rangle \in \mathbb{H}_{KET}$ we have $|\psi''\rangle = \hat{A}|\psi'\rangle \in \mathbb{H}_{KET}$

using the completeness of the $\mathbb{H}$ spaces we can expand: $|\psi'\rangle = \sum_n \lambda_n |\psi_n\rangle$ where $\underbrace{\lambda_n = \langle\psi_n|\psi'\rangle}$

(orthonormal projection)

$\Rightarrow \quad |\psi'\rangle = \sum_n |\psi_n\rangle\langle\psi_n|\psi'\rangle = \hat{I}_{KET}|\psi'\rangle \Rightarrow |\psi'\rangle = \hat{I}_{KET} \cdot |\psi'\rangle$

identity operator: operator that leaves the KET unchanged (like multiplying by 1)

$\hat{I}_{KET}|\cdot\rangle = \sum_n |\psi_n\rangle\langle\psi_n|\cdot\rangle = |\cdot\rangle$ closure property of identity resolution $\Rightarrow$ the identity is written as a sum of expansion terms

generic KET

all terms must be considered otherwise we get a projection and not an identity

important: we can completely characterize the operator once we know the result of the application of the operator to all the elements of the basis

so if we have: $\hat{A}|\psi'\rangle = \hat{A}\sum_n |\psi_n\rangle\overbrace{\langle\psi_n|\psi'\rangle}^{\lambda_n} = \sum_n \hat{A}|\psi_n\rangle\langle\psi_n|\psi'\rangle = |\psi''\rangle \; (= \hat{A}|\psi'\rangle)$

linearity/continuity

transformation of the element belonging to the orthonormal basis: $|\varphi_n\rangle = \hat{A}|\psi_n\rangle$

so, since the operator is completely characterized by the elements $|\varphi_n\rangle$ we can write the matrix A that completely describes the operator $\hat{A}$:

$$A = [\,|\varphi_0\rangle \;\; |\varphi_1\rangle \;\; \dots \;\; |\varphi_n\rangle\,]$$

however these elements are KETS and can $\therefore$ be represented as column vectors:

$$|\varphi_n\rangle \longrightarrow \begin{bmatrix} \langle\psi_0|\varphi_n\rangle \\ \langle\psi_1|\varphi_n\rangle \\ \vdots \\ \langle\psi_n|\varphi_n\rangle \end{bmatrix}$$

in general:

$$A = \begin{bmatrix} & \vdots & \\ \cdots & A_{mn} & \cdots \\ & \vdots & \end{bmatrix} \qquad A_{mn} = \langle\psi_m|\varphi_n\rangle = \langle\psi_m|A|\psi_n\rangle$$

transformation through $\hat{A}$ of the ψ_n basis state

m row: related to the basis element

n column: related to the output of the operator application on the basis vector: $\hat{A}|\psi_n\rangle = \varphi_n$

where $A_{mn} = \langle\psi_m|\varphi_n\rangle = \langle\psi_m|A|\psi_n\rangle$

expansion coefficients of $|\varphi''\rangle = \hat{A}|\varphi'\rangle$

$\lambda_m'' = \langle \varphi_m | \varphi'' \rangle$

since $|\varphi''\rangle = \sum_m |\varphi_m\rangle \underbrace{\langle \varphi_m | \varphi''\rangle}_{\lambda_m}$ and $|\varphi''\rangle = A|\varphi'\rangle$

$\hat{A}|\varphi'\rangle = \hat{A} \sum_n |\varphi_n\rangle\langle \varphi_n|\varphi'\rangle = \sum_n \hat{A}|\varphi_n\rangle\langle\varphi_n|\varphi'\rangle = |\varphi''\rangle$

$\Rightarrow \lambda_m'' = \langle \varphi_m | \varphi''\rangle = \langle \varphi_m | \sum_n \hat{A}|\varphi_n\rangle\langle \varphi_n|\varphi'\rangle = \sum_n \underbrace{\langle \varphi_m|\hat{A}|\varphi_n\rangle}_{A_{mn}} \underbrace{\langle \varphi_n|\varphi'\rangle}_{\lambda_n' \text{ orthonormal proj.}}$

$\Rightarrow \lambda_m'' = \sum_n A_{mn} \cdot \lambda_n'$

row by coulomn matrix multiplication

$$\Rightarrow \begin{bmatrix} \vdots \\ \lambda_m'' \\ \vdots \end{bmatrix} = \begin{bmatrix} & \vdots & \\ \cdots & A_{mn} & \cdots \\ & \vdots & \end{bmatrix} \cdot \begin{bmatrix} \vdots \\ \lambda_n \\ \vdots \end{bmatrix}$$

we can also describe the same situation in the BRA domain

$\varphi' \longrightarrow \hat{A} \longrightarrow \varphi''$ physically it's just a linear transformation of quantum states

$\mathbb{H} = \mathbb{H}_{KET}$: $\hat{A}_{KET} = \hat{A}$

$\mathbb{H} = \mathbb{H}_{BRA}$: $\hat{A}_{BRA} = \hat{A}^{+}_{KET} = \hat{A}^{+} \Rightarrow$ dual operator ($\hat{A}$ linear and continuous | $\hat{A}^+$ linear and continuous)

↳ $\hat{A}|\cdot\rangle \longrightarrow |\varphi''\rangle = \hat{A}|\varphi'\rangle$

↳ this operator will act on BRA on the right: $\langle\cdot|\hat{A}^{+} \longrightarrow \langle\varphi''| = \langle\varphi'|\hat{A}^{+}$

it is possible to move from one representation to the other w/ the dagger

$|\varphi''\rangle = \hat{A}|\varphi'\rangle \longleftrightarrow \langle\varphi''| = \langle\varphi'|\hat{A}^{+}$

$(|\varphi''\rangle)^{+} = (\hat{A}|\varphi'\rangle)^{+} = |\varphi'\rangle^{+}\hat{A}^{+} = \langle\varphi'|\hat{A}^{+}$

[anti-distributive]

in the BRA domain we have a matrix representation:

$\langle\varphi''| = \langle\varphi'|\hat{A}^{+} \Rightarrow$ in a given basis $\{\langle\varphi_n|\}$

$\Rightarrow$ matrix of coeff. $\hat{A}^{+} \Rightarrow (A^{+})_{mn} = A^{*}_{nm}$

[A^{+} is the conjugate transposed matrix of A]

KET vs. **BRA**

$$\begin{bmatrix} & \vdots & \\ \cdots & A_{mn} & \cdots \\ & \vdots & \end{bmatrix} \begin{bmatrix} \vdots \\ \lambda_n' \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ \lambda_m'' \\ \vdots \end{bmatrix}$$

$$\begin{bmatrix} \cdots & (\lambda_n')^* & \cdots \end{bmatrix} \cdot \begin{bmatrix} & \vdots & \\ \cdots & (A^\dagger)_{mn} & \cdots \\ & \vdots & \end{bmatrix} = \begin{bmatrix} \cdots & (\lambda_m'')^* & \cdots \end{bmatrix}$$

note: $(\lambda_n')^* = \langle \varphi' | \psi_n \rangle = \langle \psi_n | \varphi' \rangle^* = \lambda_n'^*$

so:

$$\langle \varphi'' | = \langle \varphi' | \hat{A}^\dagger$$
$$\updownarrow$$
$$| \varphi'' \rangle = \hat{A} | \varphi' \rangle$$

dim.

$$\langle \varphi'' | \psi_m \rangle = \langle \varphi' | \hat{A}^\dagger | \psi_m \rangle = \left(\sum_n \langle \varphi' | \psi_n \rangle \langle \psi_n | \right) | \hat{A}^\dagger | \psi_m \rangle$$

$$= \sum_n \langle \varphi' | \psi_n \rangle \langle \psi_n | \hat{A}^\dagger | \psi_m \rangle \Rightarrow (\lambda_m'')^* = \langle \varphi' | \psi_n \rangle \langle \psi_n | \hat{A}^\dagger | \psi_m \rangle$$

$$= (\lambda_n')^* \hat{A}^\dagger_{mn}$$

[$\hat{A}$ lin. and cont. $\Leftrightarrow$ $\hat{A}^\dagger$ lin. and cont.]

before we obtained $\langle \psi_m | \varphi'' \rangle = \sum \langle \psi_m | \varphi' \rangle \langle \psi_m | A | \psi_n \rangle$

$$(\lambda_m'') = (\lambda_n') \hat{A}_{mn}$$

since $(\lambda_m'')^* = (\lambda_n')^* A^\dagger_{mn}$ and $(\lambda_m'') = A_{mn} (\lambda_n')$

conjugating

$$\langle \psi_m | \hat{A} | \psi_n \rangle^* = \langle \psi_m | \hat{A}^\dagger | \psi_n \rangle$$

$$(A^\dagger)_{nm} = \left(\langle \psi_n | \hat{A}^\dagger | \psi_m \rangle^\dagger \right)^\dagger = \left(| \psi_m \rangle^\dagger (\hat{A}^\dagger)^\dagger \langle \psi_n |^\dagger \right)^\dagger = \Big(\underbrace{\langle \psi_m | \hat{A} | \psi_n \rangle}_{\text{scalar}} \Big)^\dagger = \left(\langle \psi_m | \hat{A} \psi_n \rangle \right)^* = A_{mn}^*$$

[anti-distributive]

$\varphi' \longrightarrow A \longrightarrow \varphi''$ $\quad\quad$ $\hat{A} : \hat{\mathbb{H}} \longrightarrow \mathbb{H}$

$\hat{A} \equiv \hat{A}_{KET} : \mathbb{H}_{KET} \longrightarrow \mathbb{H}_{KET}$

$\hat{A}_{KET} |\varphi'\rangle = |\varphi''\rangle$ $\quad\quad$ $(\mathbb{H}_{KET} = \mathbb{H} \, ; \, \hat{A}_{KET} = \hat{A})$

$\underbrace{\langle\varphi'| \hat{A}_{BRA}}_{\langle\varphi'|\hat{A}^+} = \langle\varphi''|$ $\quad\quad$ $(\mathbb{H}_{BRA} = \mathbb{H} \, ; \, (\hat{A}_{KET})^+ = \hat{A}^+)$

def. of dual operator

we consider a generic quantum state ψ and then close the bracket

$\Rightarrow \langle\psi| \hat{A}_{KET} |\varphi'\rangle = \underline{\langle\psi|\varphi''\rangle}$

$\Rightarrow \langle\varphi'| \underbrace{\hat{A}_{BRA}}_{\hat{A}^+} |\psi\rangle = \underline{\langle\varphi''|\psi\rangle}$

one is the complex conj. of the other

dim.

$\underline{\langle\psi| \hat{A}_{KET} |\varphi'\rangle^*} = \langle\psi|\varphi''\rangle^* = \langle\varphi''|\psi\rangle = \underline{\langle\varphi'|A^+|\psi\rangle}$

$\Rightarrow \langle\psi|\hat{A}_{KET}|\varphi'\rangle^* = \langle\varphi'|A^+|\psi\rangle$

if $\hat{A} : \mathbb{H} \longrightarrow \mathbb{H}$ is a lin. and cont. op.

$\Downarrow$ Riesz' theo.

there exists and is unique an operator $\underline{\hat{A}^{(dual)} \equiv \hat{A}^+ : \mathbb{H}^* \longrightarrow \mathbb{H}^*}$
defined/characterized by:

$\langle\psi|\hat{A}_{KET}|\varphi'\rangle^* = \langle\varphi'|A^+|\psi\rangle \Rightarrow \langle\varphi'| \underbrace{\hat{A}^{(dual)}}_{\hat{A}^{(dual)} \text{ is acting on the BRA}} |\psi\rangle = \langle\psi|\hat{A}|\varphi'\rangle$

note: the (dual) operator acts in the BRA space and sends in the BRA space

in the case of discrete orthonormal basis $\{|u_n\rangle\}$ for $\mathbb{H}$ (either finite dimension or ∞ countable):

$$\hat{A} \xrightarrow[\text{in the } \{u_n\}]{\text{discrete representation}} A = \begin{bmatrix} & \vdots & \\ \cdots & A_{mn} & \cdots \\ & \vdots & \end{bmatrix}$$

DxD square matrix

where $A_{mn} = \langle u_m|\hat{A}|u_n\rangle$

$$\Rightarrow \hat{A}|\cdot\rangle \longrightarrow \begin{bmatrix} & \vdots & \\ \cdots & A_{mn} & \cdots \\ & \vdots & \end{bmatrix} \cdot \underbrace{\begin{bmatrix} \cdot \end{bmatrix}}_{\text{column vector of exp. coeff. of } |\cdot\rangle}$$

now considering the dual matrix:

$$A^{+} = \begin{bmatrix} & \vdots & \\ \cdots & (A)^{+}_{mn} & \cdots \\ & \vdots & \end{bmatrix} \quad \text{where} \quad (A^{+})_{mn} = \langle \psi_m | \hat{A}^{+} | \psi_n \rangle \overset{\text{apply dagger twice}}{=} \left(\langle \psi_m | \hat{A}^{+} | \psi_n \rangle^{+} \right)^{+} \overset{\text{anti-distributive}}{=} \left(|\psi_n\rangle^{+} \hat{A}^{+^{+}} \langle \psi_m |^{+} \right)^{+}$$

$$= \Big(\underbrace{\langle \psi_n | \hat{A} | \psi_m \rangle}_{\text{scalar} \Rightarrow \alpha^{+} = \alpha^{*}} \Big)^{+} = \langle \psi_n | \hat{A} | \psi_m \rangle^{*} \quad \text{transposed and conjugated}$$

$$\Rightarrow \langle \cdot | A^{+} \longrightarrow [\,\cdot\,] \cdot \begin{bmatrix} & \vdots & \\ \cdots & (A^{+})_{mn} & \cdots \\ & \vdots & \end{bmatrix}$$

so "$+$" $\equiv$ conjugation and transposition
(reflexive and antidistributive)

$$+^{-1} = +$$
$$+^{+} = (+^{+})^{-1} \quad \text{def. of identity}$$

once again considering $\hat{A} : \mathbb{H} \longrightarrow \mathbb{H}$ lin. and cont. op.

$$\xrightarrow{\varphi'} \boxed{\hat{A}} \xrightarrow{\varphi''}$$

we can define the (adjoint) operator $\hat{A}^{(adj)}$ such that $\hat{A}^{(adj)} : \mathbb{H} \longrightarrow \mathbb{H}$

$$\xrightarrow{\varphi'} \boxed{\hat{A}} \xrightarrow{\tilde{\varphi}''}$$

obs. in general $\varphi'' \neq \tilde{\varphi}''$

it is possible to demonstrate that $\forall \hat{A}$ lin. and cont. also $\hat{A}^{(adj)}$ will be lin. and cont. in the same space where

$\hat{A}^{(adj)} : \mathbb{H} \longrightarrow \mathbb{H}$ is characterized/defined by: $\langle \psi | \underbrace{\hat{A}^{(adj)} | \varphi \rangle} = \langle \varphi | \hat{A} | \psi \rangle^{*}$

$\hat{A}^{(adj)}$ is acting on the KET

note: the (adj) operator acts on the KET space and sends in the KET space

$$A^{+} \begin{cases} \hat{A}^{(adj)} |\cdot\rangle \equiv \hat{A}^{+} |\cdot\rangle \\ \langle \cdot | \hat{A}^{(dual)} \equiv \langle \cdot | A^{+} \end{cases}$$

$\langle \psi | \hat{A}^{+} | \varphi \rangle = \langle \varphi | \hat{A} | \psi \rangle^{*}$

$\hat{A}^{+}$ can be interpreted as acting on KET or BRA

the conj. transposed matrix: $(A^{+})_{mn} = A_{nm}^{*}$

$$\begin{cases} [\,\cdot\,] \cdot A^{(dual)}_{mn} & \text{row vector of exp. coeff. of the BRA} \\ A^{(adj)}_{mn} \cdot [\,\cdot\,] & \text{column vector of exp. coeff. of the KET} \end{cases}$$

$$\langle \varphi' | A^{+} | \varphi'' \rangle = \langle \varphi'' | \hat{A} | \varphi' \rangle^{*}$$

discrete representation

scalar prod. as closure of $\langle \varphi' | \hat{A}^{(dual)}$ and $|\varphi''\rangle$ that is, the scalar prod. in $\mathbb{H}$ between $\hat{A}\varphi'$ and φ'

$$\left[\dots (\lambda_m')^{*} \dots \right] \cdot \left[\begin{matrix} & \vdots & \\ \dots & (A^{+})_{mn} & \dots \\ & \vdots & \end{matrix} \right] \cdot \left[\begin{matrix} \vdots \\ \lambda_n'' \\ \vdots \end{matrix} \right]$$

$(\lambda_m')^{*} = \langle \varphi' | \psi_m \rangle$

$(A^{+})_{mn} = \langle \psi_m | \hat{A}^{+} | \psi_n \rangle$

elements of orthonormal basis

$\langle \psi_n | \varphi'' \rangle$

scalar product as closure of $\langle \varphi' |$ and $\hat{A}^{(adj)} | \varphi'' \rangle$ that is, the scalar prod. in $\mathbb{H}$ between φ' and $\hat{A}^{(adj)}\varphi''$

$$\langle \varphi' | \hat{A} | \varphi'' \rangle = \langle \varphi' | (\hat{A}^{+})^{+} | \varphi'' \rangle$$

dual acts on BRA

closure between $\langle \varphi' |$ and $\hat{A}^{(adj)} | \varphi'' \rangle$

closure between $\langle \varphi' | \left[\hat{A}^{(adj)} \right]^{(dual)}$ and $|\varphi''\rangle$

$\hat{A}$ acts on KET

a linear and continuous op. $\hat{A} : \mathbb{H} \to \mathbb{H}$ is Hermitian (or self adjoint) when

$\hat{A}^{(adj)} = \hat{A}$ $\quad (\Rightarrow \hat{A}^{+} | \cdot \rangle = \hat{A}^{(dual)} | \cdot \rangle = \hat{A} | \cdot \rangle) \Rightarrow \langle \varphi | \hat{A} | \psi \rangle = \langle \psi | \hat{A} | \varphi \rangle^{*}$

some properties:

I) all eigenvalues of a Hermitian op. are real

II) the eigenvectors of a Hermitian op. corresponding to diff. eigenvalues are orthogonal

def. a cmplx. num. γ is an eigenvalue of a lin. op. $\hat{A}$ when the characteristic eq. (or eigenvalue eq.) is satisfied:

$\hat{A}\varphi = \gamma\varphi$ where φ (eigenvector) $\neq 0$

in case of lin. and cont. op. $\hat{A} : \mathbb{H} \to \mathbb{H}$ any lin. comb. of eigenvectors w/ same eigen is still an eigenvector (w/ the same eigenvalue)

indeed:

$$\begin{cases} \hat{A}\varphi_1 = \gamma\varphi_1 \\ \hat{A}\varphi_2 = \gamma\varphi_2 \end{cases} \qquad \varphi = \alpha_1\varphi_1 + \alpha_2\varphi_2$$

$$\Rightarrow \hat{A}\varphi = \alpha_1 \underbrace{\hat{A}\varphi_1}_{\gamma\varphi_1} + \alpha_2 \underbrace{\hat{A}\varphi_2}_{\gamma\varphi_2} = \gamma(\alpha_1\varphi_1 + \alpha_2\varphi_2) = \gamma\varphi$$

so φ is an eigenvector w/ the same eigenvalue

in case of lin. and cont. $\hat{A} : \mathbb{H} \to \mathbb{H}$ all the eigenvectors of $\hat{A}$ w/ the same eigenvalue λ together w/ the null vector will form a vectorial subspace of dim. f_λ (named eigenspace of $\hat{A}$ for the eigenvalue λ)

multiplicity of the eigenvalue: max. n° of orthonormal eigenvectors w/ eigenvalue λ

$1 \leq f_\lambda \leq D$ (for finite dim.)

$1 \leq f_\lambda$ (for ∞ countable) if $d_\lambda = 1$ all eigenvectors are lin. independant

[non degenerate eigenvalue λ] => eigenspace corresponds to a single vector (identifying a single quantum state as eigenstate)

$\hat{A}(\alpha\varphi) = \alpha\hat{A}\varphi = \alpha\lambda\varphi = \lambda(\alpha\varphi)$

Hermitian operator

theo. **1)** all the eigenvalues of an Hermitian operator $\hat{A}: \mathbb{H} \to \mathbb{H}$ are real numbers

dim.

Hp. $\hat{A}^{+} = \hat{A}^{(adj)} = \hat{A}$ (def. of Hermitian)

Hp. $\hat{A}|\varphi\rangle = \gamma|\varphi\rangle$ w/ $|\varphi\rangle \neq 0$ (eigenvalue)

$\hat{A}|\varphi\rangle = \gamma|\varphi\rangle \Rightarrow$ close the bracket $\Rightarrow \langle\varphi|\hat{A}|\varphi\rangle = \gamma\langle\varphi|\varphi\rangle \Rightarrow \gamma = \dfrac{\langle\varphi|\hat{A}|\varphi\rangle}{\langle\varphi|\varphi\rangle}$

where $\|\varphi\|^2 = \langle\varphi|\varphi\rangle \geq 0$ and $\|\varphi\|^2 = 0 \Leftrightarrow |\varphi\rangle = 0$ but $|\varphi\rangle \neq 0$ (Hp.) so $\Rightarrow \langle\varphi|\varphi\rangle > 0$

$\Rightarrow \quad \gamma = \dfrac{\langle\varphi|\hat{A}|\varphi\rangle}{\underbrace{\|\varphi\|^2}_{\text{real \& positive}}}$ so we have to show that $\langle\varphi|\hat{A}|\varphi\rangle$ is real

$\Rightarrow \langle\varphi|\hat{A}|\varphi\rangle \underset{[\hat{A} = \hat{A}^{+} \text{ Hp. Hermitian op.}]}{=} \langle\varphi|\hat{A}^{+}|\varphi\rangle = \langle\varphi|\underbrace{\hat{A}^{+}}_{=\hat{A}}|\varphi\rangle^{*} \Rightarrow \langle\varphi|\hat{A}|\varphi\rangle = \langle\varphi|\hat{A}|\varphi\rangle^{*}$

$\alpha = \alpha^{*} \Leftrightarrow \alpha$ real $\Rightarrow \langle\varphi|\hat{A}|\varphi\rangle$ is real $\Rightarrow \gamma = \dfrac{\langle\varphi|\hat{A}|\varphi\rangle}{\langle\varphi|\varphi\rangle}$ is real

alternatively:

$$\gamma^{*} = \frac{\langle\varphi|\hat{A}|\varphi\rangle^{*}}{\|\varphi\|^2} \underset{[\alpha^{*} = \alpha^{+}]}{=} \frac{\langle\varphi|\hat{A}|\varphi\rangle^{+}}{\|\varphi\|^2} = \frac{\langle\varphi|\hat{A}^{+}|\varphi\rangle}{\|\varphi\|^2} = \frac{\langle\varphi|\hat{A}|\varphi\rangle}{\|\varphi\|^2} = \gamma \Rightarrow \gamma^{*} = \gamma \Rightarrow \gamma \text{ real}$$

theo. **2)** the eigenvectors of a Hermitian op. $\mathbb{H} \to \mathbb{H}$ corresponding to diff. eigenvalues are orthogonal

dim. $\hat{A}^{+} = \hat{A}$, $\gamma_1 \neq \gamma_2$

$\hat{A}|\varphi_1\rangle = \gamma_1|\varphi_1\rangle$; $\hat{A}|\varphi_2\rangle = \gamma_2|\varphi_2\rangle$

$\Rightarrow$ closing the bracket $\Rightarrow \begin{cases} \langle\varphi_2|\hat{A}|\varphi_1\rangle = \gamma_1\langle\varphi_2|\varphi_1\rangle \\ \langle\varphi_1|\hat{A}|\varphi_2\rangle = \gamma_2\langle\varphi_1|\varphi_2\rangle \end{cases}$

$\Rightarrow \langle\varphi_2|\hat{A}|\varphi_1\rangle = (\langle\varphi_2|\hat{A}|\varphi_1\rangle^{+})^{+} = (\langle\varphi_1|\hat{A}^{+}|\varphi_2\rangle)^{+} = \overbrace{\langle\varphi_1|\hat{A}|\varphi_2\rangle^{+}} = \gamma_2^{*}\cdot\langle\varphi_1|\varphi_2\rangle^{*}$

and also $\langle\varphi_2|\hat{A}|\varphi_1\rangle = \gamma_1\langle\varphi_2|\varphi_1\rangle \Rightarrow \gamma_1\langle\varphi_2|\varphi_1\rangle = \gamma_2^{*}\cdot\underbrace{\langle\varphi_1|\varphi_2\rangle^{*}}_{\langle\varphi_2|\varphi_1\rangle}$

$\Rightarrow \gamma_1, \gamma_2$ are real (theo. 1) $\Rightarrow \gamma_1\langle\varphi_2|\varphi_1\rangle = \gamma_2\langle\varphi_2|\varphi_1\rangle$

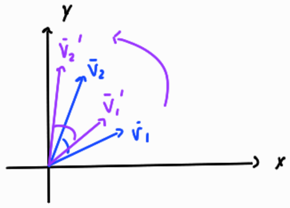
$\Rightarrow (\gamma_1 - \gamma_2)\langle\varphi_2|\varphi_1\rangle = \emptyset$ but since $\gamma_1 \neq \gamma_2 \Rightarrow \gamma_1 - \gamma_2 \neq 0 \Rightarrow \langle\varphi_2|\varphi_1\rangle = \emptyset$ def. of orthogonality unitary operator

a linear and continuous operator $\hat{U}: \mathbb{H} \longrightarrow \mathbb{H}$ is unitary when: $\hat{U} \cdot \hat{U}^+ = \hat{U}^+ \cdot \hat{U} = \hat{I}$

that is, $\hat{U}^{-1} = \hat{U}^+$ (def. of inverse: $\hat{U}\hat{U}^{-1} = \hat{U}^{-1}\hat{U} = \hat{I}$)

theo. 1) a unitary operator $\hat{U}$ preserves the scalar prod. between vectors (and hence the norms of the vectors)

in Euclidean space:



e.g. rotations and reflections in Euclidean space don't change the norm (angle between vectors)

the unitary op. is an extension of this concept to $\mathbb{H}$

dim.

$\varphi_1' \xrightarrow{\hat{U}} \varphi_1''$

$\varphi_2' \xrightarrow{\hat{U}} \varphi_2''$

$|\varphi_1''\rangle = \hat{U}|\varphi'\rangle \xrightarrow{+} |\varphi_1''\rangle^+ = (\hat{U}|\varphi_1'\rangle)^+ = \langle\varphi_1''| = \underline{\langle\varphi_1'|\hat{U}^+}$

$\hat{U}^+$ to be intended as a dual, since it is acting on a BRA

likewise we obtain $|\varphi_2''\rangle = \underline{\hat{U}}|\varphi_2'\rangle$

here $\hat{U} = \hat{U}^+$ is to be intended as adjoint

closing the bracket $\Rightarrow \langle\varphi_1''|\varphi_2''\rangle = \langle\varphi_1'|\hat{U}^+\hat{U}|\varphi_2'\rangle \underset{[\hat{U} \text{ unitary}]}{=} \langle\varphi_1'|\hat{I}|\varphi_2'\rangle = \langle\varphi_1'|\varphi_2'\rangle$

$\Rightarrow \langle\varphi_1''|\varphi_2''\rangle = \langle\varphi_1'|\varphi_2'\rangle$ so scalar prod. is preserved

$\underbrace{\| |\varphi''\rangle \|^2}_{\langle\varphi''|\varphi''\rangle} = \| \hat{U}|\varphi'\rangle \|^2$

$\langle\varphi''|\varphi''\rangle = \langle\varphi'|\underbrace{\hat{U}^+\hat{U}}_{\hat{I}}|\varphi'\rangle = \langle\varphi'|\varphi'\rangle = \| |\varphi'\rangle \|^2$

$\Rightarrow \| |\varphi''\rangle \|^2 = \| |\varphi'\rangle \|^2$ norm is preserved

theo. 2) a unitary op. $\hat{U}$ has unitary eigenvalues (i.e. w/ modulus = 1)

dim.

$\hat{U}|\varphi\rangle = \gamma|\varphi\rangle \xrightarrow{+} (\hat{U}|\varphi\rangle)^+ = (\gamma|\varphi\rangle)^+ = \langle\varphi|\gamma^*$

but also $(\hat{U}|\varphi\rangle)^+ = \langle\varphi|\hat{U}^+ \Rightarrow \langle\varphi|\hat{U}^+ = \langle\varphi|\gamma^* = \gamma^*\langle\varphi|$

($\hat{U}^+$ intended as dual acting on BRA)

closing the bracket $\Rightarrow \langle\varphi|\underbrace{\hat{U}^+}_{\hat{I}}\hat{U}|\varphi\rangle = \gamma^*\langle\varphi|\underbrace{\hat{U}|\varphi\rangle}_{\gamma|\varphi\rangle} = \gamma^*\gamma\langle\varphi|\varphi\rangle$

(interpreting $\hat{U}^+$ as adjoint acting on KET)

$\Rightarrow \langle\varphi|\cancel{\varphi\rangle} = |\gamma|^2\langle\varphi|\cancel{\varphi\rangle}$ ($\langle\varphi|\varphi\rangle > 0$ since φ is an eigenvector)

$\Rightarrow |\gamma| = 1$

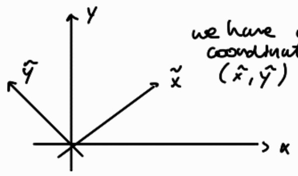
unitary op. in finite dim. (or ∞ countable)

$\Rightarrow$ we have a discrete orthonormal basis $\{|\varphi_n\rangle\}$ and $\hat{U}$ is represented by a unitary matrix

a unitary op. (in this discrete case) gives a bijective mapping (i.e. one-to-one correspondance) between orthonormal (discrete) basis

$$\{|\varphi_n\rangle\} \underset{\substack{\hat{U}^+ (=U^{-1}) \\ \text{adjoint}}}{\overset{\hat{U}}{\rightleftarrows}} \{|\tilde{\varphi}_n\rangle = \hat{U}|\varphi_n\rangle\}$$

In Euclidean geo. :



we have a new coordinate system $(\tilde{x}, \tilde{y})$

dim.

$\{|\varphi_n\rangle\}$ orthonormal set of vectors $\Leftrightarrow \langle\varphi_m|\varphi_n\rangle = \delta_{mn}$

$$\langle\tilde{\varphi}_m|\tilde{\varphi}_n\rangle = \langle\varphi_m|\underbrace{\hat{U}^+U}_{\mathbb{I}}|\varphi_n\rangle = \langle\varphi_m|\varphi_n\rangle = \delta_{mn}$$ so we once again have orthonormality

$$\left[\begin{array}{l} |\tilde{\varphi}_m\rangle = \hat{U}|\varphi_m\rangle \Rightarrow |\tilde{\varphi}_m\rangle^+ = (\hat{U}|\varphi_m\rangle)^+ \Rightarrow \langle\tilde{\varphi}_m| = \langle\varphi_m|\hat{U}^+ \\ |\tilde{\varphi}_n\rangle = \hat{U}|\varphi_n\rangle \end{array}\right]$$

in case of $\mathcal{H}$ w/ discrete orthonormal basis $\{|\varphi_n\rangle\}$

$\hat{U}$ is a unitary op. $\Leftrightarrow$ the representing matrix $U = \begin{bmatrix} & \vdots & \\ \cdots & U_{mn} & \cdots \\ & \vdots & \end{bmatrix}$ is a unitary matrix

matrix w/ orthonormal columns and equivalently rows (and viceversa)

i.e. if the columns are orthonormal then it is unitary and $\therefore$ the rows are orthonormal (and viceversa)

w/ $U_{mn} = \langle\varphi_m|\hat{U}|\varphi_n\rangle$

$$\begin{bmatrix} & a & e & \\ \vdots & b & f & \vdots \\ & c & g & \\ & d & h & \end{bmatrix} \Rightarrow [a^* \; b^* \; c^* \; d^*] \cdot \begin{bmatrix} e \\ f \\ g \\ h \end{bmatrix}$$

$a^* \cdot e + b^* \cdot f + \dots = 0$

and the scalar prod. of a column w/ itself is $= 0$

$U_{00} = \langle\varphi_0|\tilde{\varphi}_0\rangle = \langle\varphi_0|\hat{U}|\varphi_0\rangle$

$$\begin{bmatrix} \langle\varphi_0|\tilde{\varphi}_0\rangle & \hat{U}|\varphi_1\rangle & \hat{U}|\varphi_2\rangle & \dots \\ \langle\varphi_1|\tilde{\varphi}_0\rangle & & & \\ \langle\varphi_2|\tilde{\varphi}_0\rangle & & & \\ \vdots & & & \end{bmatrix}$$

columns are the expansion coeff. of the vector $|\tilde{\varphi}_n\rangle = \hat{U}|\varphi_n\rangle$ (KET)

the rows are orthonormal : $\hat{U}$ unitary $\Rightarrow \hat{U}^{-1} = U^+$ is also unitary

the inverse matrix of $\hat{U}$, $\hat{U}^{-1} = U^+$ will be the conj. and transposed matrix of $\hat{U}$

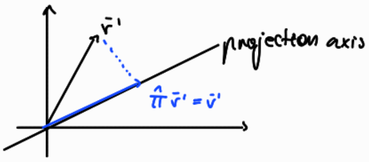
$\hookrightarrow$ the columns of $\hat{U}$ become the rows of the inverse (aside from the conj.). However since the inverse is also unitary, the columns of $\hat{U}^{-1} = U^+$ (which are the rows of $\hat{U}$) are also orthonormal

$\hat{U}$ is unitary : $\hat{U}^{-1} = \hat{U}^{+} \Rightarrow (\hat{U}^{-1})(\hat{U}^{-1})^{+} = \underbrace{\hat{U}^{+} \cdot (\hat{U}^{+})^{+}}_{\hat{U}^{+}U = \hat{I}}$

so also U^{-1} is unitary

orthogonal projector

In Euclidean geometry:



$\hat{\pi}(\hat{\pi}\vec{v}') = \hat{\pi}^2\vec{v}' = \hat{\pi}\vec{v}'$

$\hat{\pi}\vec{v}'' = \hat{\pi}\hat{\pi}\vec{v}' = \hat{\pi}\vec{v}' = \vec{v}''$ idempotence property

1) $\hat{\pi}$ is Hermitian ($\hat{\pi}^{+} = \hat{\pi}$) $\Rightarrow$ eigenvalues are real

2) $\hat{\pi}$ is idempotent $\Rightarrow \hat{\pi}^2 = \hat{\pi}$ or $\hat{\pi}^n = \hat{\pi}$ for $n = 1, 2, \dots$

$\Rightarrow$ the only possible eigenvalues of $\hat{\pi}$ are either 0 or 1

dim.

$\hat{\pi}|e\rangle = \gamma|e\rangle$ w/ $|e\rangle \neq 0$ def. of eigenvector

$\hat{\pi}\hat{\pi}|e\rangle = \hat{\pi}\gamma|e\rangle = \gamma\hat{\pi}|e\rangle = \gamma^2|e\rangle$

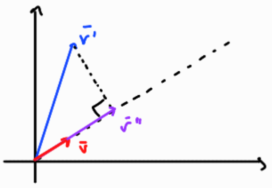
but also $\hat{\pi}^2|e\rangle = \hat{\pi}|e\rangle = \gamma|e\rangle$

$\Rightarrow \gamma^2\cancel{|e\rangle} = \gamma\cancel{|e\rangle} \Rightarrow \gamma^2 = \gamma \Rightarrow \gamma(\gamma - 1) = 0 \begin{cases} \gamma = 0 \\ \gamma = 1 \end{cases}$

so idempotence forces the eigenvalues to be 0 or 1, by also adding the Hermiticity we get orthogonality aswell

orthogonal projector

- Hermitian and idempotent operator



$\boxed{\hat{\pi}_{\vec{v}}\, \vec{v}' = \vec{v}''}$ orthogonal projector on the oriented direction (i.e. ray) identified by a vector $\vec{v}$

it can be written in terms of scalar product: $\vec{v}'' = \underbrace{\frac{\vec{v}}{|\vec{v}|}}_{\text{direction/versor of the projected vector}} \underbrace{\left(\vec{v}' \cdot \frac{\vec{v}}{|\vec{v}|}\right)}_{\text{modulus of the projected vector}}$ versor of the projection where $\vec{v}' \cdot \frac{\vec{v}}{|\vec{v}|} = |\vec{v}'| \cdot \cos\theta$

so:

$$\vec{v}'' = \frac{\vec{v}}{|\vec{v}|} \cdot \left(\frac{\vec{v}}{|\vec{v}|} \cdot \vec{v}'\right) = \frac{\vec{v} \cdot \vec{v}'}{|\vec{v}|^2}\, \vec{v}$$

in an Hilbert space the projection is intended in terms of quantum states (ray)

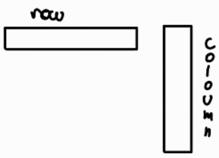
the orthogonal projection on the quantum state ψ described by a non null vector $\propto |\psi\rangle$ is:

$$\boxed{\hat{\pi}_\psi |\cdot\rangle = \underbrace{\langle\psi|\cdot\rangle}_{\text{scalar prod. that gives us the "modulus"}} \underbrace{|\psi\rangle}_{\text{"direction" (ray)}} = |\psi\rangle\langle\psi|\cdot\rangle}$$

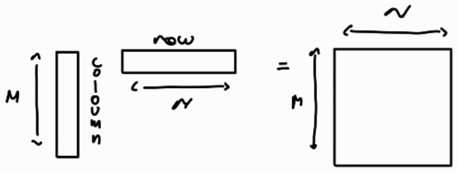
where $\underbrace{|\psi\rangle\langle\psi|}_{\text{outer product}}\cdot\rangle$

outer product ← different from the inner product $\langle\psi|\varphi\rangle$ which is a complex scalar

<u>inner product</u>: $\langle\psi|\varphi\rangle \Rightarrow$



<u>outer product</u>: $|\psi\rangle\langle\varphi| \Rightarrow$



$M \times N$ matrix

for a non-normalized ψ:

$$\hat{\pi}_\psi |\cdot\rangle = \frac{|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle} |\cdot\rangle \Rightarrow \boxed{\hat{\pi}_\psi = \frac{|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle}}$$

this def. is an extension of the one given for a Euclidean space. Due to the "symmetry" of the two spaces we expect this def. to actually give us an orthogonal projection

we now have to verify:

1) <u>Hermiticity</u>

$$\langle\varphi'|\hat{\pi}_\psi|\varphi''\rangle = \langle\varphi''|\hat{\pi}_\psi^\dagger|\varphi'\rangle^* \quad \text{(double dagger)}$$

hence the Hermitian condition is:

$$\langle\varphi'|\hat{\pi}_\psi|\varphi''\rangle = \langle\varphi''|\hat{\pi}_\psi|\varphi'\rangle^* \quad (\text{so } \hat{\pi} = \hat{\pi}^\dagger)$$

$$\Rightarrow \quad \frac{\langle \varphi' | \psi \rangle \langle \psi | \varphi'' \rangle}{\langle \psi | \psi \rangle} = \left(\frac{\langle \varphi'' | \psi \rangle \langle \psi | \varphi' \rangle}{\langle \psi | \psi \rangle} \right)^*$$

$(\hat{\pi}_\psi)$ closes both the brackets

removing the conjugate and reversing the order of the second term:

$$\frac{\langle \varphi' | \psi \rangle \langle \psi | \varphi'' \rangle}{\langle \psi | \psi \rangle} = \frac{\langle \psi | \varphi'' \rangle \langle \varphi' | \psi \rangle}{\langle \psi | \psi \rangle} = \frac{\langle \varphi' | \psi \rangle \langle \psi | \varphi'' \rangle}{\langle \psi | \psi \rangle}$$ so the two terms are equal

intuitively:

$$\hat{H}_\psi^+ = \left(\frac{|\psi\rangle\langle\psi|}{\|\psi\|^2} \right)^+ = \frac{\langle\psi|^+ |\psi\rangle^+}{\|\psi\|^2} = \frac{|\psi\rangle\langle\psi|}{\|\psi\|^2} = \hat{H}_\psi$$

let's take a look @ the dual operator (acts on BRA)

$$\boxed{\langle \cdot | \hat{H}_\psi^+} = \left(\frac{|\psi\rangle\langle\psi|\cdot\rangle}{\langle\psi|\psi\rangle} \right)^+ = \frac{(\langle\psi|\cdot\rangle)^+ \langle\psi|}{\langle\psi|\psi\rangle} = \boxed{\frac{\langle\cdot|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle}}$$

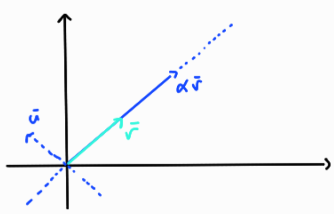
same expression for the dual, as we have seen for Hermitian operators

2) Idempotence

$$\hat{\pi}_\psi^2 = \hat{\pi}_\psi \hat{\pi}_\psi = \frac{|\psi\rangle\cancel{\langle\psi|\,|\psi\rangle}\langle\psi|}{\cancel{\langle\psi|\psi\rangle}\,\langle\psi|\psi\rangle} = \frac{|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle} = \hat{\pi}_\psi$$

↳ so we have shown it is Hermitian ⊕ idempotent $\Rightarrow$ $\hat{\pi}_\psi$ is a valid expression for the orthogonal projector

eigenvectors of $\hat{\pi}_\psi$



if the direction of the projection is $\bar{v}$, a vector $\alpha\bar{v}$ is an eigenvector w/ $\lambda = 1$ $\Rightarrow$

$\underline{\hat{\pi}_{\bar{v}}(\alpha\bar{v}) = \lambda\cdot(\alpha\bar{v})}$ true for $\lambda = 1$ (projection of a multiple of the base)

the multiplicity is 1 (the eigenspace is of dimension 1)

for an orthogonal vector $\bar{u}$ we get: $\hat{\pi}_{\bar{v}}(\bar{u}) = \emptyset$ and again the multiplicity is 1 $(D - 1 = 1)$

dim. of the $\bar{v}$ subspace

dim. of the Euclidean space

note: in the 3D space the multiplicity of the eigenspace of the "parallel" space is still one, while the multiplicity of the eigenspace of $\emptyset$ eigenvalues is $3-1=2$ $\Rightarrow$ the other 2 directions are orthogonal) in the Hilbert space:

$\hat{\Pi}_\psi |\alpha\psi\rangle$ w/ $\alpha \neq 0$ $\Rightarrow$ $\hat{\Pi}_\psi |\alpha\psi\rangle = \frac{|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle} |\alpha\psi\rangle = \alpha \frac{|\psi\rangle \cancel{\langle\psi|\psi\rangle}}{\cancel{\langle\psi|\psi\rangle}} = \alpha|\psi\rangle$

$\Rightarrow$ $\hat{\Pi}_\psi |\alpha\psi\rangle = \alpha|\psi\rangle$ so this is the one eigenvalue

since the multiplicity is the dimension of the eigenspace $E_{\lambda=1}$ i.e. the max. n° of normalized orthogonal eigenvectors w/ $\lambda=1$ eigenvalue, so it is obvious that the multiplicity is 1 (all the orthogonal vectors to $\alpha|\psi\rangle$ are in the $\lambda=\emptyset$ eigenspace)

in fact if $|\varphi\rangle$ (non null) is orthogonal to $|\psi\rangle$ then $\hat{\Pi}_\psi|\varphi\rangle = \frac{|\psi\rangle\langle\psi|\varphi\rangle}{\langle\psi|\psi\rangle} = \emptyset$

$\Rightarrow$ $\hat{\Pi}_\psi|\varphi\rangle = \emptyset \cdot |\varphi\rangle$ every non null vector orthogonal to $|\psi\rangle$ is an eigenvector w/ $\lambda=\emptyset$

so $g_1 = 1$ (dim. of the eigenspace)

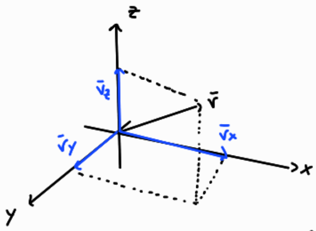
the multiplicity of the zero eigenspace ($\lambda=\emptyset$) being that orthogonal to the $\lambda=1$ eigenspace will be:

$g_{\lambda=\emptyset} = D-1$ in the finite $\mathcal{H}$ (∞ in the infinite countable $\mathcal{H}$)

for the orthogonal projector the multiplicity of ($\lambda=1$) is the rank of the linear operator

dimension of the image subspace $\Rightarrow$ the "output" of the projector are all eigenvectors w/ $\lambda=1$

orthogonal projector of rank $r \geq 1$



$$\bar{v} = \bar{v}_x + \bar{v}_y + \bar{v}_z$$

$$= \underbrace{\hat{\pi}_x \bar{v}}_{} + \hat{\pi}_y \bar{v} + \hat{\pi}_z \bar{v} = \underbrace{(\hat{\pi}_x + \hat{\pi}_y + \hat{\pi}_z)}_{\hat{I}} \bar{v}$$

orthogonal projection of $\bar{v}$ over the direction x

we can also see it as: $\bar{v} = \bar{v}_x + \underbrace{(\bar{v}_y + \bar{v}_z)}_{}$

new vector that belongs to the z-y plane $\Rightarrow \tilde{v}$

$\Rightarrow \tilde{v} = \hat{\pi}_{(y,z)} \bar{v}$ where $\hat{\pi}_{(y,z)} = \hat{\pi}_y + \hat{\pi}_z$

orthogonal projector of rank 2

set of all the results of transformations through the operator of all possible input vectors

[$\overbrace{\text{image}}$ dimension = 2 (rank)]

we can extend this concept to $\mathbb{H}$:

$$\hat{\pi}_{\{|\varphi_n\rangle\}} = \sum_{n=0}^{r-1} \hat{\pi}_{\varphi_n} = \sum_{n=0}^{r-1} \frac{|\varphi_n\rangle\langle\varphi_n|}{\langle\varphi_n|\varphi_n\rangle} \quad = 1 \text{ (orthonormal)}$$

set of orthonormal vectors (orthonormality simplifies the expressions)

sum of orthogonal projectors of rank = 1

in case of finite dim. D of $\mathbb{H}$: $1 \leq r \leq D$

when $r = D$: $\hat{\pi}_{\{|\varphi_n\rangle\}_{n=0,1,\dots,D-1}}$ is the identity $\hat{I}$ $\Rightarrow \sum_{n=0}^{D-1} \hat{\pi}_{\varphi_n} = \hat{I}$

in the case of countable ∞ dim. of $\mathbb{H}$ $\Rightarrow \sum_{n=0}^{\infty} \hat{\pi}_{\varphi_n} = \hat{I}$

indeed:

expansion of $|\varphi\rangle$

$$\left(\sum_{n=0}^{\infty} |\varphi_n\rangle\langle\varphi_n|\right)|\varphi\rangle = \sum_{n=0}^{\infty} |\varphi_n\rangle \underbrace{\langle\varphi_n|\varphi\rangle}_{} = \overbrace{\sum_{n=0}^{\infty} \lambda_n |\varphi_n\rangle} = |\varphi\rangle$$

linearity w.r.t. the second argument + continuity

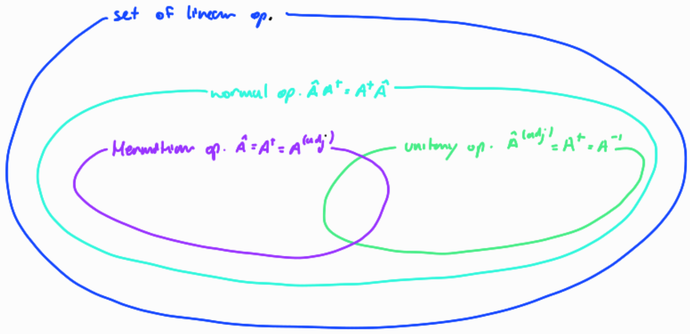
expansion coeff. λ_n of $|\varphi\rangle$

so $\sum_{n=0}^{\infty} |\varphi_n\rangle\langle\varphi_n|$ is $\hat{I}$ also in the ∞ countable case

normal operator

a linear and continuous (bounded) operator $\hat{A}: \mathbb{H} \longrightarrow \mathbb{H}$ is said a normal operator when it commutes w/ its adjoint operator $\hat{A}^{+}: \mathbb{H} \longrightarrow \mathbb{H}$ => $\hat{A} \cdot \hat{A}^{+} = \hat{A}^{+}\hat{A}$

(KET space so $A^{+} = A^{(adj)}$)



Hermiticity $\xrightarrow{\quad}$ normality ; normality $\not\Rightarrow$ Hermiticity

dim.

$\hat{A}^{+}\hat{A}$ but because $\hat{A}$ is Hermitian => $\hat{A}^{+}\hat{A} = \hat{A}^{2}$

$\hat{A}^{+} = \hat{A}$

but also $\hat{A}\hat{A}^{+} = \hat{A}^{2}$ => $\hat{A}\hat{A}^{+} = \hat{A}^{+}\hat{A}$ so if $\hat{A}$ is Hermitian it is also normal

unitary $\xrightarrow{\quad}$ normal ; normal $\not\Rightarrow$ unitary

dim.

$$\hat{U}^{-1}\hat{U} = \hat{U}\hat{U}^{-1} \quad (= \hat{I})$$

but $\hat{U}^{-1} = \hat{U}^{+}$ => $\hat{U}^{+}\hat{U} = \hat{U}\hat{U}^{+}$ which is the normal condition

if $\hat{A}$ is a norm. op. then the eigenvectors corresponding to diff. eigenvalues are orthogonal (just like Hermitian operators)

the Hermitian op. is a more specific case since Hermitian op. also require that the eigenvalues are real (alt. def. of Hermitian op. : a normal op. w/ real eigenvalues)

Likewise, an alt. def. of unitary op. : a normal op. w/ eigenvalues w/ modulus = 1

spectral decomposition

in any case of finite dim. $\mathbb{H}$ any normal operator admits a spectral decomposition over an orthonormal basis $\{|\psi_n\rangle\}_{n=0,1,\dots,D-1}$. That is, $\hat{A}$ can be written as the sum:

$$\hat{A} = \sum_{n=0}^{D-1} \alpha_n \hat{\pi}_{\psi_n} = \sum_{n=0}^{D-1} \alpha_n |\psi_n\rangle\langle\psi_n|$$

eigenvalue corresponding to the eigenvector ψ_n

(characteristic prop. of normal op.)

moreover $\{|\psi_n\rangle\}$ is an orthonormal basis formed by eigenvectors of $\hat{A}$ and the scalar coeff. α_n of the spectral decomposition are the respective eigenvalues

=> it is the orthonormal diagonalization of the operator

$$\hat{A}|\psi_m\rangle = \Big(\sum_n \alpha_n |\psi_n\rangle\langle\psi_n|\Big)|\psi_m\rangle \underset{\text{linearity}}{=} \sum_n \alpha_n |\psi_n\rangle \underbrace{\langle\psi_n|\psi_m\rangle}_{\substack{\delta_{nm} \\ (\text{Hp. of orthonormality})}} \overset{(n=m)}{=} \alpha_n|\psi_m\rangle$$

element of the basis

$\Rightarrow \hat{A}|\psi_m\rangle = \alpha_m|\psi_m\rangle$ so α_m is an eigenvalue of $\hat{A}$

matrix representing $\hat{A}$:

$$A = \begin{bmatrix} & \vdots & \\ \cdots & A_{mn} & \cdots \\ & \vdots & \end{bmatrix} \quad \text{where } A_{mn} = \langle\psi_m|\hat{A}|\psi_n\rangle$$

we want to verify it is diagonal

$$\hat{A} = \sum_r a_r |\psi_r\rangle\langle\psi_r|$$

$$\langle\psi_m|\hat{A}|\psi_n\rangle = \langle\psi_m|\Big(\sum_r |\psi_r\rangle\langle\psi_r|\Big)|\psi_n\rangle \underset{\text{linearity}}{=} \langle\psi_n|\sum_r \alpha_r |\psi_r\rangle\langle\psi_r|\psi_n\rangle$$

$$= \sum_r \alpha_r \underbrace{\langle\psi_m|\psi_r\rangle}_{\delta_{mr}} \underbrace{\langle\psi_r|\psi_n\rangle}_{\delta_{rn}} \begin{cases} \emptyset & (m \neq n) \\ \sum_r \alpha_r \delta_{nr} = \alpha_n & (m = n) \end{cases}$$

conjugate linearity
(however the BRA has no coeff. so it's just like normal linearity)

in finite dim. $\mathbb{H}$:

$\hat{A}$ is a normal linear operator $\Leftrightarrow$ $\hat{A}$ is represented in a suitable (formed by eigenvectors of $\hat{A}$) orthonormal basis by a diagonal matrix (w/ diagonal elements given by the eigenvalues of $\hat{A}$) $\Leftrightarrow$ $\hat{A}$ is represented in any orthonormal basis by a normal matrix, that is, $A^\dagger A = AA^\dagger$

unitary matrix: matrix representation of a unitary operator

normal matrix: $A^\dagger A = AA^\dagger$ $\Leftrightarrow$ unitary diagonalizable matrix: $U^\dagger A U = \text{diag}\{\alpha_n\}$

$\Rightarrow$ one to one correspondance between orthonormal basis
- formed by eigenvectors $\{|\psi_n\rangle\}$
- used to obtain the matrix A $\{|e_n\rangle\}$

<u>in finite dim. $\mathbb{H}$</u>

$\hat{A}$ is a normal lin. op $\Leftrightarrow$ there exists an orthonormal basis formed by eigenvectors of $\hat{A}$

$\hat{A}$ is a Hermitian lin. op. $\Leftrightarrow$ there exists an orthonormal basis formed by eigenvectors of $\hat{A}$ and all eigenvalues are real

$\hat{A}$ is a unitary lin. op. $\Leftrightarrow$ there exists an orthonormal basis formed by eigenvectors of $\hat{A}$ and all eigenvalues have modulus $= 1$

In both finite and ∞ countable dim. $\mathbb{H}$:

we ask it is continuous: the condition on continuity (boundedness) has been removed !!

if a linear op. $\hat{A}$ admits a spectral decomposition over an orthonormal basis (formed by eigenvectors of $\hat{A}$) then $\hat{A}$ is a normal op. (that is, $\hat{A}^\dagger \hat{A} = \hat{A}\hat{A}^\dagger$ where $\hat{A}, \hat{A}^\dagger$ are defined since by removing boundedness the op. may not be def. over the whole of $\mathbb{H}$) w/ coeff. α_n given by eigenvalues)

$$\Rightarrow \hat{A} = \sum_n \alpha_n |\varphi_n\rangle\langle\varphi_n|$$

eigenvectors

eigenvalues

$\therefore$ defined over the whole of $\mathbb{H}$

$\hat{A}$ is bounded (continuous) if and only if $\sup\{|\alpha_n|\} < +\infty$ (finite upper bound)

note: in the finite dim. case, the boundedness is always valid consider a finite/countable ∞ dimension Hilbert space $\mathbb{H}$

if a lin. op. $\hat{A}: \mathbb{H} \to \mathbb{H}$ admits a spectral decomposition (this is the case for quantum physics) over an orthonormal (in this case also discrete since $\mathbb{H}$ is finite/∞ countable) basis $\{|\psi_n\rangle\}$ then it is a normal operator

$$\Rightarrow \hat{A} = \sum_n \alpha_n \hat{\pi}_n = \sum_n \alpha_n |\psi_n\rangle\langle\psi_n| \qquad |\psi_n\rangle \text{ is eigenvector of } \hat{A} \text{ w/ eigenvalue } \alpha_n$$

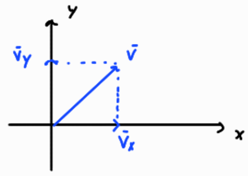
dim.

$$\hat{A}^\dagger = \Big(\sum_n \alpha_n |\psi_n\rangle\langle\psi_n|\Big)^\dagger \underset{\text{conj. lin.}}{\overset{\text{(adj) since we remain in } \mathbb{H}}{=}} \sum_n \alpha_n^* \hat{\pi}_n^\dagger \underset{\text{orthogonal projector is Hermitian}}{=} \sum_n \alpha_n^* \hat{\pi}_n$$

$\hat{A}$ and $\hat{A}^\dagger$ have the same eigenvectors (since $\hat{\pi}_n = \hat{\pi}^\dagger$) and conjugated complex eigenvalues

$$\hat{A}^\dagger \hat{A} = \Big(\sum_m \alpha_m^* \hat{\pi}_m\Big)\Big(\sum_n \alpha_n \hat{\pi}_n\right) \underset{\text{linearity}}{=} \sum_m \sum_n \alpha_m^* \alpha_n \hat{\pi}_m \hat{\pi}_n$$

$\hat{\pi}_m \hat{\pi}_n$: $=0$ $m \neq n$; $\hat{\pi}_m = \hat{\pi}_n$ $m = n$



$\Rightarrow \hat{\pi}_x \hat{\pi}_y \bar{v} = \hat{\pi}_x \bar{v}_y = \emptyset$

indeed: $\hat{\pi}_m \hat{\pi}_n = |\psi_m\rangle\underbrace{\langle\psi_m|\psi_n\rangle}_{\delta_{mn}}\langle\psi_n|$ (ψ_n, ψ_m elements of an orthonormal basis)

$=0$ $m \neq n$

$|\psi_m\rangle\langle\psi_n|$ $m=n \Rightarrow |\psi_m\rangle\langle\psi_m| = |\psi_n\rangle\langle\psi_n| = \hat{\pi}_m = \hat{\pi}_n$

$$= \sum_m \sum_n \alpha_m^* \alpha_n \delta_{mn} \hat{\pi}_n$$

$$= \sum_m \alpha_m^* \alpha_m \hat{\pi}_m = \sum_m |\alpha_m|^2 \hat{\pi}_m$$

$\Rightarrow \hat{A}^\dagger \hat{A} = \sum_m |\alpha_m|^2 \hat{\pi}_m$ $\qquad$ $\hat{A}^\dagger\hat{A}$ has the same eigenvectors of $\hat{A}, \hat{A}^\dagger$ w/ eigenvalues $|\alpha_m|^2$

if we reverse the order: $\hat{A}\hat{A}^\dagger$ we get the same result

$\Rightarrow \hat{A}^\dagger \hat{A} = \hat{A}\hat{A}^\dagger$ this is valid also for ∞ countable dim. $\mathbb{H}$

- in a finite / countable ∞ dim. $\mathbb{H}$, a linear $\hat{A}$ is normal $\Leftrightarrow$ there exists a (discrete) orthonormal basis of $\mathbb{H}$ formed by eigenvectors of $\hat{A}$ (dim. is omitted)

(if and only if condition)

$$\Rightarrow \hat{A} = \sum_n \alpha_n \hat{\pi}_n = \sum_n \underset{\text{eigenvalues}}{\alpha_n} \underset{\text{eigenvectors}}{|\psi_n\rangle\langle\psi_n|}$$

in the case of ∞ countable: $\longrightarrow$ (only if) $\quad \cancel{\longleftarrow}$

in the finite dim. case every op. is bounded (eq. to continuity). From the continuity:
$\Rightarrow \hat{A}$ is def. for any $|\psi_n\rangle \in \mathbb{H}$

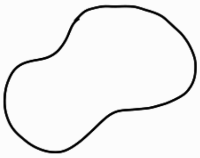
(in the ∞ case $\hat{A}$ (normal op.) is bounded $\Leftrightarrow \sup\{|\alpha_n|\} < +\infty$ otherwise $\hat{A}$ is unbounded and $\therefore$ not continuous $\Rightarrow$ the domain $\text{Dom}(\hat{A}) \subseteq \mathbb{H}$)

$\hookrightarrow$ an unbounded op. $\hat{A}$ is not defined everywhere in $\mathbb{H}$

- in the finite dim. $\mathcal{H}$ a lin. op. $\hat{A}$ is Hermitian (subclass of normal) $\Longleftrightarrow$ there exists an orthonormal basis formed by eigenvectors w/ real eigenvalues

(or equivalently $\hat{A}$ admits a spectral decomp. over a suitable orth. basis w/ real coeff.)

in the ∞ countable case: $\cancel{\longrightarrow}$ $\longleftarrow$ (only if)



2-state quantum system
(max. 2 orthogonal states)

$\mathcal{H}$ w/ dim. $D=2$ (generated by the lin. comb. of 2 orthogonal states) $\Rightarrow$ any $|\psi\rangle$ (quantum state) $\in \mathcal{H}$ can be expanded into a 2-dim. orthonormal basis $\{|\psi_0\rangle, |\psi_1\rangle\}$

QUBIT

$\hookrightarrow |\psi\rangle = \lambda_0|\psi_0\rangle + \lambda_1|\psi_1\rangle$

$\lambda_0 = \langle\psi_0|\psi\rangle \qquad \lambda_1 = \langle\psi_1|\psi\rangle$

in agreement w/ the closure property (or identity resolution)

$$\hat{I} = \hat{\pi}_0 + \hat{\pi}_1 = |\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|$$

$$\Rightarrow |\psi\rangle = \hat{I}|\psi\rangle = (\hat{\pi}_0 + \hat{\pi}_1)|\psi\rangle = \hat{\pi}_0|\psi\rangle + \hat{\pi}_1|\psi\rangle = |\psi_0\rangle\underbrace{\langle\psi_0|\psi\rangle}_{\lambda_0} + |\psi_1\rangle\underbrace{\langle\psi_1|\psi\rangle}_{\lambda_1}$$

$$\Rightarrow |\psi\rangle = \lambda_0|\psi_0\rangle + \lambda_1|\psi_1\rangle$$

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

$|\psi_1\rangle$ "1 KET"

$|\psi_0\rangle$ "0 KET"

$\Rightarrow |\psi\rangle = \lambda_0|0\rangle + \lambda_1|1\rangle$ so we can build ∞ qubits $|\psi\rangle$

$$\Rightarrow \begin{cases} \alpha = \langle 0|\psi\rangle & (\lambda_0) \\ \beta = \langle 1|\psi\rangle & (\lambda_1) \end{cases} \Rightarrow |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\Rightarrow \begin{bmatrix} \langle 0|\psi\rangle \\ \langle 1|\psi\rangle \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$ column vector w/ 2 complex scalar coeff.

column representation of the KET

$$\langle 0|\psi\rangle = \alpha\underbrace{\langle 0|0\rangle}_{1} + \beta\underbrace{\cancel{\langle 0|1\rangle}}_{\text{orthogonality}} = \alpha$$ (likewise $\langle 1|\psi\rangle = \beta$)

$$\|\psi\|^2 = \sum_n |\lambda_n|^2 = |\alpha|^2 + |\beta|^2$$

indeed: $\|\psi\|^2 = \langle\psi|\psi\rangle$ but $\langle\psi| = |\psi\rangle^\dagger = (\alpha|0\rangle + \beta|1\rangle)^\dagger = \alpha^*\langle 0| + \beta^*\langle 1|$

$$\Rightarrow \|\psi\|^2 = (\alpha^*\langle 0| + \beta^*\langle 1|)(\alpha|0\rangle + \beta|1\rangle) = \alpha^*\alpha\underbrace{\langle 0|0\rangle}_{1} + \alpha^*\beta\underbrace{\cancel{\langle 0|1\rangle}}_{0} + \beta^*\alpha\underbrace{\cancel{\langle 1|0\rangle}}_{0} + \beta^*\beta\underbrace{\langle 1|1\rangle}_{1}$$

$= |\alpha|^2 + |\beta|^2 < +\infty$ in the finite dim. case because $\sup\{|\lambda_n|\} < +\infty$

$$\|\psi\|^2 = \langle\psi|\psi\rangle = [\alpha^* \ \beta^*]\begin{bmatrix}\alpha \\ \beta\end{bmatrix} = |\alpha|^2 + |\beta|^2$$ confirming the result w/ matrix algebra

$$\langle\psi| = |\psi\rangle^\dagger \Rightarrow \underbrace{\begin{bmatrix}\alpha \\ \beta\end{bmatrix}}_{|\psi\rangle}^\dagger = [\alpha^* \ \beta^*]$$

$|\psi\rangle$ and $\gamma|\psi\rangle$ represent the same quantum state (the state is characterized by the ray)

so we may consider a <u>normalized</u> qubit: $\|\psi\| = 1 \iff |\alpha|^2 + |\beta|^2 = 1$

single - QUBIT quantum gates

$\psi_{in} \rightsquigarrow \boxed{\text{quantum gate}} \rightsquigarrow \psi_{out}$

rule of transf. of qubit

it is the extension to quantum computing of classical gates (single input)

e.g. NOT classical gate

$b_{in} \rightsquigarrow \boxed{NOT} \rightsquigarrow b_{out} = NOT(b_{in})$

b_{in}	b_{out}
0	1
1	0

$\iff$ they correspond to unitary (linear) operators $\hat{U}$ in the 2-DIM $\mathcal{H}$ of qubits (<u>the norm is preserved</u>) $\Rightarrow$ $\underline{\hat{U}^{-1} = U^{+}}$

(preservation of scalar prod.)

e.g.

$\psi'_{in} \perp \psi''_{in} \Rightarrow \psi'_{out} \perp \psi''_{out}$

$$\langle \psi_{in}' | \psi_{in}'' \rangle = \underbrace{\langle \hat{U}\psi_{in}' | \hat{U}\psi''_{in} \rangle}_{\langle \psi'_{out} | \psi''_{out} \rangle} = \langle \psi_{in}' | \underbrace{\hat{U}^{+}\hat{U}}_{\hat{U}^{-1}\hat{U} = \hat{I}} | \psi''_{in} \rangle = \langle \psi_{in}' | \psi''_{in} \rangle$$

$$\left[\begin{array}{l} (\hat{U}|\psi'_{in}\rangle)^{+} = (|\psi'_{out}\rangle)^{+} \\ \Rightarrow \langle \psi'_{in} | \hat{U}^{+} = \langle \psi'_{out} | \end{array} \right]$$

in a given orthonormal basis the unitary op. $\hat{U}$ is represented by a unitary matrix (2×2) U

$$\Rightarrow U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \quad \text{where } u_{nm} \in \mathbb{C}$$

w/ orthonormal coloumns (and consequently the rows, because U^{+} is also unitary)

$$U^{+} = \begin{bmatrix} u_{00}^{*} & u_{10}^{*} \\ u_{01}^{*} & u_{11}^{*} \end{bmatrix} = U^{-1} \quad \text{(also unitary)}$$

conj. transp.

$$UU^{+} = U^{+}U = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

an equivalent check: orthonormality of coloums (treat each coloumn as a <u>KET</u>)

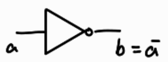
$$\begin{cases} |u_{00}|^2 + |u_{10}|^2 = 1 \\ |u_{01}|^2 + |u_{11}|^2 = 1 \\ u_{00}^{*} u_{01} + u_{10}^{*} u_{11} = 0 \end{cases} \quad \text{orthonormality check}$$

$$u_{mn} = \langle \psi_m | \hat{U} | \psi_n \rangle \Rightarrow U = \begin{bmatrix} \langle 0|\hat{U}|0\rangle & \langle 0|\hat{U}|1\rangle \\ \langle 1|\hat{U}|0\rangle & \langle 1|\hat{U}|1\rangle \end{bmatrix} \quad \text{using the computational basis}$$

elements of orthonormal basis

quantum NOT

classical NOT:



a	b
0	1
1	0

quantum NOT (or more properly "flip gate" : Pauli-X gate)

described by the unitary operator $\hat{X}$ (that we know is completely characterized by its action as an orthonormal basis) defined as:

$$\begin{cases} \hat{X}|0\rangle = |1\rangle \\ \hat{X}|1\rangle = |0\rangle \end{cases}$$

in general, for any $|\psi\rangle \in \mathcal{H}$:

$$\hat{X}|\psi\rangle = \hat{X}(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$$

note: since we know the action of X on the computational basis we know its action on every quantum state

in the matrix representation:

$$X\begin{bmatrix}\alpha \\ \beta\end{bmatrix} = \begin{bmatrix}\beta \\ \alpha\end{bmatrix}$$

in the computational basis it is a matrix that applied to a vector flips it

$$\begin{cases} \hat{X}|0\rangle = 1 \\ \hat{X}|1\rangle = 0 \end{cases} \Rightarrow \begin{cases} X\begin{bmatrix}1 \\ 0\end{bmatrix} = \boxed{\begin{bmatrix}0 \\ 1\end{bmatrix}} \\ X\begin{bmatrix}0 \\ 1\end{bmatrix} = \boxed{\begin{bmatrix}1 \\ 0\end{bmatrix}} \end{cases} \xrightarrow[\text{representation of X in the comp. basis}]{} X = \begin{bmatrix}\langle 0|\hat{X}|0\rangle & \langle 0|\hat{X}|1\rangle \\ \langle 1|\hat{X}|0\rangle & \langle 1|\hat{X}|1\rangle\end{bmatrix}$$

$$\left(A_{mn} = \langle\psi_m|\hat{A}|\psi_n\rangle \Rightarrow A = \begin{bmatrix}A_{00} & A_{01} \\ A_{10} & A_{11}\end{bmatrix}\right)$$

$$= \begin{bmatrix}\langle 0|1\rangle & \langle 0|0\rangle \\ \langle 1|1\rangle & \langle 1|0\rangle\end{bmatrix} = \begin{bmatrix}\boxed{\begin{matrix}0 \\ 1\end{matrix}} & \boxed{\begin{matrix}1 \\ 0\end{matrix}}\end{bmatrix}$$

indeed:

$$\begin{bmatrix}0 & 1 \\ 1 & 0\end{bmatrix}\begin{bmatrix}\alpha \\ \beta\end{bmatrix} = \begin{bmatrix}\beta \\ \alpha\end{bmatrix}$$

$\hat{X}$ is also unitary since we have obtained that:

$X = \begin{bmatrix}0 & 1 \\ 1 & 0\end{bmatrix}$ so its columns are orthonormal and the operator is unitary. This means that an orthonormal basis is mapped by $\hat{X}$ in another orthonormal basis

$$\{|0\rangle, |1\rangle\} \xrightarrow[\hat{X}]{} \{|1\rangle, |0\rangle\}$$

$\hat{X}$ is also a Pauli operator:

a linear operator $\hat{A}$ acting on a qubit is a Pauli operator when A is both unitary AND Hermitian and moreover has the two distinct eigenvalues 1 and -1

so if $\hat{A}$ is a Pauli operator: $\begin{cases} \hat{A}^{\dagger} = \hat{A} & \text{Hermiticity} \\ \hat{A}^{\dagger} = A^{-1} & \text{Unitarity} \end{cases}$

combining the 2 properties:

$\hat{A}^2 = \hat{A}\cdot\hat{A} = \hat{A}\cdot\hat{A}^{\dagger} = \hat{A}\cdot\hat{A}^{-1} = \hat{I}$ so every Pauli operator is an involution: $\hat{A}^2 = \hat{I}$

at the same time since:

$\hat{A}$ Hermitian => real eigenvalues
$\hat{A}$ Unitary => eigenvalues w/ $|\cdot| = 1$
} only possible eigenvalues are +1, -1

the Pauli operator has to have the two distinct eigenvalues +1 and -1. This for example excludes the identity operator

$\hat{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ has +1 w/ multiplicity 2 (diagonal is made up of eigenvalues)
↳ it is NOT a Pauli operator even if it is Hermitian and unitary (it is missing the -1 eigenvalue)

e.g.

check that X is a Pauli operator

$\hat{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ is unitary since $\{|0\rangle, |1\rangle\} \xrightarrow{\hat{X}} \{|1\rangle, |0\rangle\}$ (transforms an orthonormal basis into an orthonormal basis)

$\hat{X}^{+} = \begin{bmatrix} 0^* & 1^* \\ 1^* & 0^* \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \hat{X}$ $\hat{X}^{+} = X$ ∴ it is Hermitian

conj. + transp.

we could also check unitarity knowing Hermiticity

$\hat{X} \cdot \hat{X}^{+} = \hat{X} \cdot \hat{X} = \hat{X}^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \hat{I}$

Hermiticity

so since $\hat{X} \cdot \hat{X}^{+} = \hat{I}$ => $\hat{X}$ is unitary

lastly, we have to check the eigenvalues

we have to remember that the two eigenvectors of $\hat{X}$ are $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ -1 \end{bmatrix}$

=> they are orthogonal: $1 \cdot 1 + 1 \cdot -1 = 1 - 1 = 0$

this is immediate since it is obviously normal being both unitary and Hermitian

so we get that $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \cdot 1 \Rightarrow \lambda = 1$

$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \end{bmatrix} = -1 \cdot \begin{bmatrix} -1 \\ 1 \end{bmatrix} \Rightarrow \lambda = -1$

↳ so $\hat{X}$ is a Pauli operator

since $\hat{X}$ is normal, its eigenvectors form an orthogonal basis which can be normalized

$\dfrac{\begin{bmatrix} 1 \\ 1 \end{bmatrix}}{\left\| \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\|} = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ => orthonormal basis $\left\{ \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$

so we can obtain an orthonormal basis formed by the eigenvalues of the quantum NOT. They are two "known" vectors

=> + QUBIT $|+\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (first eigenvector of the NOT gate) if we think of a qubit as representing the state of polarization of a single photon we can identify:

$|0\rangle = |H\rangle$ horizontal polarization $\leftrightarrow$
$|1\rangle = |V\rangle$ vertical polarization $\updownarrow$

and the + qubit can be represented as $|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ diagonal polarization $\swarrow$ $|Q\rangle$

$\Rightarrow$ - QUBIT $|-\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (second eigenvector of the NOT gate)

it corresponds to the orthogonal polarization $|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) = \searrow$ $|-Q\rangle$

these two qubits are orthogonal

$$\langle + | - \rangle = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix} = \frac{1}{2} - \frac{1}{2} = \emptyset$$

we can also see this w/ the Dirac notation:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \Rightarrow \langle + | = (|+\rangle)^{\dagger} = \underbrace{(1/\sqrt{2})^{*}}_{= 1/\sqrt{2}}(\langle 0| + \langle 1|)$$

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

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

$$= \frac{1}{2}(1 - 1) = \emptyset$$

phase shift gate

$\hat{P}(\delta)$
phase shift

$\hat{P}(\delta)|0\rangle = |0\rangle \Rightarrow |0\rangle$ is an eigenvector w/ eigenvalue $= +1$
$\hat{P}(\delta)|1\rangle = e^{i\delta}|1\rangle \Rightarrow |1\rangle$ is an eigenvector w/ eigenvalue $= e^{i\delta}$

this operator is unitary: the computational basis is mapped to another orthonormal basis (same basis aside from the phase shift on $|1\rangle$)

also we've already found the eigenvectors which are $|0\rangle$ and $|1\rangle$ and so they are orthogonal $\Rightarrow \hat{P}$ is a normal operator. In addition, since the eigenvalues associated to the eigenvectors have $1.1 = 1 \Rightarrow \hat{P}$ is unitary

in the computational basis the matrix representation of $\hat{P}(\delta)$ is:

$$P(\delta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix}$$

(already diagonal since the 2 orthogonal eigenvectors are nothing more than the computational basis $\Rightarrow$ in this basis we have the diagonal matrix of eigenvalues)

in general $\hat{P}(\delta)$ is NOT a Pauli op., we have to verify the conditions:

Hermiticity:

$$\mathbb{P}(\delta)^+ = \begin{bmatrix} 1 & 0 \\ 0 & (e^{j\delta})^* \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{-j\delta} \end{bmatrix} = \mathbb{P}(-\delta) = \mathbb{P}^{-1}(\delta)$$

obviously the inverse op. of phase shifting by δ is shifting by $-\delta$

so $\mathbb{P}(\delta)$ is Hermitian only in 2 cases:

1) $\delta = \emptyset$ (trivial case) $\Rightarrow$ $\mathbb{P}(0) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \hat{I}$ (Hermitian and unitary but NOT a Pauli op.)

2) $\delta = \pi$ $\Rightarrow$ $\mathbb{P}(\pi) = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}$ which IS a Pauli op. since it has eigenvalues 1 and -1 as well as being Hermitian and unitary

$\hat{\mathbb{P}}(\pi)$ is also def. as $\hat{z}$ $\Rightarrow$ Z-Pauli operator

$$\Rightarrow \begin{cases} \hat{z}|0\rangle = |0\rangle \\ \hat{z}|1\rangle = e^{j\delta}|1\rangle \end{cases}$$

$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ in the computational basis

S-gate

($\pi/4$ phase gate)

$\hat{S} = \hat{\mathbb{P}}(\pi/2)$ phase shift w/ $\delta = \pi/2$ (double $\pi/4$, hence the name)

in the computational basis:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{j\pi/2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & j \end{bmatrix} = e^{j\pi/4}\begin{bmatrix} e^{-j\pi/4} & 0 \\ 0 & e^{j\pi/4} \end{bmatrix}$$

it is clearly not Hermitian $\therefore$ not a Pauli op.

rapid check for Hermiticity of a 2x2 matrix:

$$\begin{cases} A = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} \\ A^+ = \begin{bmatrix} a_{00}^* & a_{10}^* \\ a_{01}^* & a_{11}^* \end{bmatrix} \end{cases} \Rightarrow A \text{ Hermitian} \Leftrightarrow \underbrace{a_{10}^* = a_{01}}\ \text{and}\ \underbrace{a_{01}^* = a_{10}}\ \text{and}\ \underbrace{a_{00}^* = a_{00},\ a_{11}^* = a_{11}}_{\text{diagonal elements must be real}}$$

antidiagonal elements must be cmplx. conj.

quantum gates:

$\hat{X}$, $\hat{\mathbb{P}}(\delta)$, $\hat{Z} = \hat{\mathbb{P}}(\pi)$, $\hat{S} = \hat{\mathbb{P}}(\frac{\pi}{2})$, $\hat{T} = \hat{\mathbb{P}}(\frac{\pi}{4})$

quantum NOT ($\hat{X}$ Pauli gate)

phase shift gate

($\hat{Z}$ Pauli gate)

phase gate ($\pi/4$ gate)

($\pi/8$ gate)

matricial form in the comp. basis:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} ; \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} ; \quad \mathbb{P}(\delta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{j\delta} \end{bmatrix} ; \quad S = \begin{bmatrix} 1 & 0 \\ 0 & j \end{bmatrix} = e^{j\pi/4} \begin{bmatrix} e^{-j\pi/4} & 0 \\ 0 & e^{j\pi/4} \end{bmatrix} ; \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{j\pi/4} \end{bmatrix} = e^{j\pi/8} \begin{bmatrix} e^{-j\pi/8} & 0 \\ 0 & e^{j\pi/8} \end{bmatrix}$$

<u>note</u>: $\hat{\mathbb{P}}(\delta_1) \cdot \hat{\mathbb{P}}(\delta_2) = \hat{\mathbb{P}}(\delta_1 + \delta_2)$ for this quantum gate the commutative property is valid (in general it is not)

indeed:

$$\hat{\mathbb{P}}(\delta_1)\hat{\mathbb{P}}(\delta_2) = \begin{bmatrix} 1 & 0 \\ 0 & e^{j\delta_1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & e^{j\delta_2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{j(\delta_1+\delta_2)} \end{bmatrix}$$

Pauli Y-gate

$\Rightarrow$ $\hat{Y}|0\rangle = j|1\rangle$

$\hat{Y}|1\rangle = -j|0\rangle$

different from the NOT gate due to the phase shift

It is <u>unitary</u> because it maps the comp. basis into the comp. basis, just phase shifted

matrix representation in comp. basis:

$$Y = \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix}$$

<u>obs.</u> if we didn't have the minus sign we wouldn't have a new operator since it would just be $= j \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = j \cdot Z$

another consideration:

$$-|+\rangle \neq |-\rangle \Rightarrow -\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \neq \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

this is just a label

$\hat{Y}$ is also <u>Hermitian</u> because the diagonal elements are real and the antidiagonal elements are complx. conj. $\Rightarrow Y^{+} = Y \Rightarrow$ Hermiticity we want to also check if it is a Pauli operator:

$\hat{Y}|\psi\rangle = \gamma|\psi\rangle$ eigenvalue equation

$$\Rightarrow Y\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \gamma\begin{bmatrix}\alpha\\\beta\end{bmatrix} \Rightarrow \underbrace{(Y-\gamma I)}_{\begin{bmatrix}-\gamma & -J\\ J & -\gamma\end{bmatrix}}\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \begin{bmatrix}0\\0\end{bmatrix} \quad w/ \begin{bmatrix}\alpha\\\beta\end{bmatrix} \neq \begin{bmatrix}0\\0\end{bmatrix}$$

the condition to have non-trivial solutions is: $(Y-\gamma I)$ <u>NOT</u> invertible

if it is invertible, the unique sol. would be the inverse of this matrix applied to the vector $\begin{bmatrix}0\\0\end{bmatrix}$. But if this matrix admits an inverse matrix the multiplication between the inverse matrix and the zero matrix would give $\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \begin{bmatrix}0\\0\end{bmatrix}$ i.e. the trivial solution

$\Rightarrow$ the rank must be $<2 \Rightarrow \det(\underbrace{\gamma I - Y}) = 0$

(we can consider $Y-\gamma I$, it's the same)

$\Rightarrow \gamma^2 + J^2 = \gamma^2 - 1 = 0 \Rightarrow \gamma = \pm 1$ so we have dem. that the 2 eigenvalues are ± 1 so it is a Pauli operators

the corresponding eigenvectors are:

$|J\rangle = (|0\rangle + J|1\rangle)\frac{1}{\sqrt{2}}$ normalized $\Rightarrow \||J\rangle\| = \||-J\rangle\| = 1$

$|-J\rangle = (|0\rangle - J|1\rangle)\frac{1}{\sqrt{2}}$

unitary operators are also normal operators $\Rightarrow$ eigenvectors are $\perp$

$\hookrightarrow \langle J|-J\rangle = \emptyset$

we have generated a new orthonormal basis

considering the physical interpretation as polarization of photons: $|0\rangle = |H\rangle$; $|1\rangle = |V\rangle$

$|J\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm J|V\rangle)$ comb. of an horizontal state + a vertical one, shifted by $\pm\pi/2$, generates the <u>circular state</u> (+ $\Rightarrow$ right polarization, − $\Rightarrow$ left polarization)

$\langle J| = |J\rangle^+$

$|J\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\J\end{bmatrix}$; $|-J\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-J\end{bmatrix} \Rightarrow \langle J|-J\rangle = \frac{1}{\sqrt{2}}[1 \;\; -J]\cdot\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-J\end{bmatrix} = \frac{1}{2}(1+J^2) = \emptyset$

so they are indeed orthogonal

$$\begin{cases}\hat{Y}|J\rangle = 1\cdot|J\rangle\\ \hat{Y}|-J\rangle = -1\cdot|-J\rangle\end{cases} \Rightarrow \begin{cases}\begin{bmatrix}0 & -J\\ J & 0\end{bmatrix}\cdot\frac{1}{\sqrt{2}}\begin{bmatrix}1\\J\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\J\end{bmatrix}\\ \begin{bmatrix}0 & -J\\ J & 0\end{bmatrix}\cdot\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-J\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\J\end{bmatrix} = -\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-J\end{bmatrix}\end{cases}$$

so indeed $|J\rangle$ and $|-J\rangle$ are eigenvectors w/ eigenvalues +1 and −1 respectively

Hadamard gate $\hat{H}$ (superposition gate)

$\hat{H}|0\rangle = |+\rangle$
$\hat{H}|1\rangle = |-\rangle$

$\hat{H}$ is unitary (maps an orthonormal basis into another orthonormal basis)

$$\{|0\rangle, |1\rangle\} \xrightarrow[\hat{H}]{} \{|+\rangle, |-\rangle\}$$

$$H = \begin{bmatrix} \langle 0|\hat{H}|0\rangle & \langle 0|\hat{H}|1\rangle \\ \langle 1|\hat{H}|0\rangle & \langle 1|\hat{H}|1\rangle \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$|+\rangle$ $|-\rangle$

diagonal elements are real, antidiagonal are cmplx. conj. (they are real, so they are the same) => Hermiticity

unitary + Hermitian => $\hat{H}^2 = I$ => eigenvalues are ± 1

it can be shown that:

$$\det(\gamma I - H) = 0 \Leftrightarrow \gamma = \pm 1$$

Bloch sphere

same concept as the Poincaré sphere extended to quantum physics (sphere in 3D Euclidean space w/ unitary radius)

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ normalization: $\|\psi\| = 1 \Rightarrow |\alpha|^2 + |\beta|^2 = 1$

we can also write this normalized qubit as:

$$|\psi\rangle = \underbrace{e^{j\varphi_1} \cdot \cos\left(\tfrac{\theta}{2}\right)}_{\alpha}|0\rangle + \underbrace{e^{j\varphi_2} \cdot \sin\left(\tfrac{\theta}{2}\right)}_{\beta}|1\rangle$$

$$= e^{j\varphi_1} \cdot \left[\cos\left(\tfrac{\theta}{2}\right)|0\rangle + e^{j(\varphi_2 - \varphi_1)} \cdot \sin\left(\tfrac{\theta}{2}\right)|1\rangle\right]$$

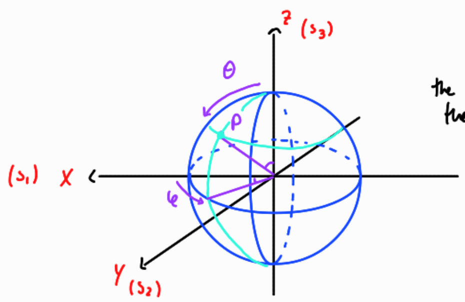
we assume $\varphi_1 = 0 \Rightarrow \varphi_2 - \varphi_1 = \phi$

$$\Rightarrow |\psi\rangle = \cos\left(\tfrac{\theta}{2}\right)|0\rangle + e^{j\phi} \cdot \sin\left(\tfrac{\theta}{2}\right)|1\rangle$$

in comp. basis

$$\begin{bmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{j\phi} \cdot \sin\left(\frac{\theta}{2}\right) \end{bmatrix}$$ 2 degrees of freedom, θ and ϕ

QUBIT $\xrightarrow[\text{correspondence}]{\text{1-to-1}}$ point on a sphere



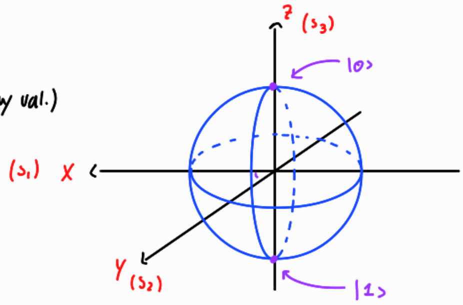
the poin P can be described by the latitude and longitude

$P = (\theta, \phi)$

longitude colatitude

$\left(\begin{matrix} 0 \le \phi < 2\pi \\ 0 \le \theta \le \pi \end{matrix} \right)$

$|0\rangle \to \begin{bmatrix} 1 \\ 0 \end{bmatrix} \Rightarrow \theta = 0$ (φ can be any val.)



it can be shown that orthogonal qubits are represented on the Bloch sphere by diametrically opposite points

indeed: $|1\rangle \to \begin{bmatrix} 0 \\ 1 \end{bmatrix} \Rightarrow \theta = \pi$ (φ " " ")

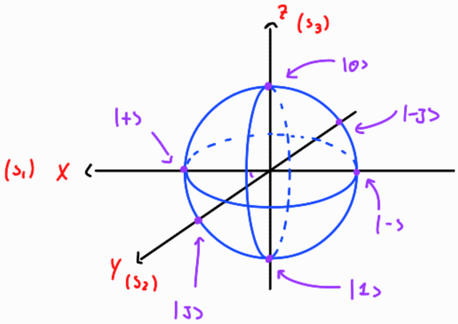
It is interesting to observe that the eigenvectors of $\hat{z}$ Pauli operator are aligned on the z-axis (hence why it has this name)

likewise:

$\hat{x} \Rightarrow$ eigenvectors $\{|+\rangle, |-\rangle\}$ x-basis

$\hat{y} \Rightarrow$ eigenvectors $\{|j\rangle, |-j\rangle\}$ y-basis

$\hat{z} \Rightarrow$ eigenvectors $\{|0\rangle, |1\rangle\}$ a.k.a. z-basis



$|+\rangle$: $\theta = \pi/2$; $\varphi = 0 \Rightarrow \begin{bmatrix} \cos(\pi/4) \\ \sin(\pi/4) \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

$|-\rangle$: $\theta = \pi/2$; $\varphi = \pi \Rightarrow \begin{bmatrix} \cos(\pi/4) \\ \underbrace{e^{j\pi}}_{-1} \cdot \sin(\pi/4) \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$

$|j\rangle$: $\theta = \pi/2$; $\varphi = \pi/2 \Rightarrow \begin{bmatrix} \cos(\pi/4) \\ e^{j\pi/2} \cdot \sin(\pi/4) \end{bmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 \\ j \end{bmatrix}$

$|-j\rangle$: $\theta = \pi/2$; $\varphi = \underbrace{\frac{3}{2}\pi}_{-\pi/2} \Rightarrow \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 \\ -j \end{bmatrix}$

quantum measurement process

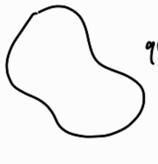
"neutral" observer ⇒ not (appreciably) influencing the result of measurement of some physical quantity

(aside from some error due to precision of instruments) - however there is no intrinsic limit to this precision

classical physical system (macroscopical)

- the physical properties of classical systems are objective and can be measured in a deterministic way

as for a quantum system



quantum physical system in a quantum state Ψ

max. possible info on the system

the observer however is in the classical system. Since the quantum system is very microscopic, the macroscopic observer heavily influences the measurement

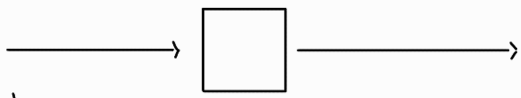
⇒ the quantum measurement process is a random and not reversible process

↳ if you repeat the measurement, we get different results. It random in an intrinsic way

the result of a measurement of a physical quantity (observable) of quantum systems are no more deterministic. They depend on the measurement process basically given by a projective non-destructive quantum measurement

according to the Copenhagen interpretation (1926)

Hp. max. info on the quantum state Ψ immediatly before the measurement



$|\Psi\rangle$

normalized (for simplicity)

measurement process of an observable quantity A

$|\Psi_{PM}\rangle$

post measurement quantum state ⇒ an eigenstate Ψ_n of a Hermitian operator $\hat{A}$ associated to the observable A. It is the random collapse of $|\Psi\rangle$ into Ψ_n, so producing a_n.

A

result of measurement ⇒ the only possible values are the eigenvalues $a_n \in \mathbb{R}$ of $\hat{A}$ corresponding to $|\Psi_n\rangle$

In the case of destructive measurements (e.g. photon absorption) we destroy the system so we don't have $|\Psi_{PM}\rangle$

In the case of qubits any Hermitian operator has 2 different orthogonal eigenstates so there are 2 different possibilities of random collapse

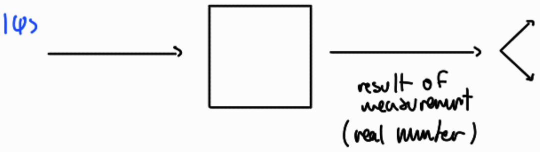
obs. the Copenhagen interpretation does not explain this collapse. It only states the probability

$P(\text{measuring } a_n) = P_n = F(\Psi, \Psi_{PM} = \Psi_n)$ $\quad (\hat{A}|\Psi_n\rangle = a_n|\Psi_n\rangle)$

$$F(\Psi, \Psi_n) = \frac{|\langle\Psi_n|\Psi\rangle|}{\|\Psi_n\|^2\,\|\Psi\|^2} = |\langle\Psi_n|\Psi\rangle|^2 \quad \text{Born rule}$$

we assume observable A w/ discrete ← discrete set of eigenvalues (finite or ∞ countable) ⇒ QUANTIZED (hence the name quantum) as opposed to continuous values (physical fact independent of mathematical interpretation)

and non-degenerate spectrum ← all eigenvalues are different



$\begin{cases} |\psi_0\rangle \\ |\psi_1\rangle \\ \vdots \\ |\psi_n\rangle \\ \vdots \end{cases}$ all with probability $p_0, p_1, \dots, p_n$ respectively

$\begin{cases} a_0 \\ a_1 \\ \vdots \\ a_n \\ \vdots \\ a_{D-1} \end{cases}$ all with probability $p_0, p_1, \dots, p_{D-1}$ respectively

when we measure a_n, if we repeat the measurement you will obtain the same value. In other words, this means that the quantum state will collapse in a precisely defined quantum state $|\psi_n\rangle$. There is a strict relation between the measurement a_n and the post measurement quantum state. This relation is independent on the initial $|\psi\rangle$

⇒ $|\psi'\rangle \rightsquigarrow |\psi_n\rangle$ w/ a_n
$|\psi''\rangle \rightsquigarrow |\psi_n\rangle$ w/ a_n

If we consider $|\psi\rangle \rightsquigarrow |\psi_1\rangle \rightsquigarrow |\psi_1\rangle$ ⇒ $|\psi_0\rangle, |\psi_1\rangle \dots$ are all orthogonal in mathematical terms (describes the physical fact that after the collapse we get the same val.)

if we repeat the measurement we get $|\psi_1\rangle$ w/ $p=1$

so:

any observable A w/ discrete and non degenerate spectrum is described by a Hermitian operator $\hat{A}$ w/ (real) eigenvalues $\{a_n\}$ representing the only possible results of measurements in correspondance of the collapse of the post measurement quantum state $|\psi_{PM}\rangle$ into the eigenstates $\{|\psi_n\rangle\}$ of $\hat{A}$ w/ prob. of collapse

$$\Rightarrow p_n = F(\psi, \psi_n) = |\langle\psi_n|\psi\rangle|^2$$

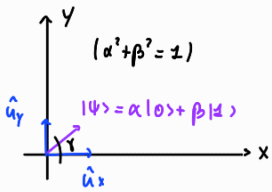
mathematical interpretation of the Copenhagen interpretation

spectral decomp. of $\hat{A}$:

$$\hat{A} = \sum_n a_n \hat{\Pi}_n = \sum_n a_n |\psi_n\rangle\langle\psi_n|$$

the collapse $|\psi_{PM}\rangle$ can be seen as the orthogonal proj. of $|\psi\rangle$ into a new state

In the case of qubits:



$\langle 0|\psi\rangle = \alpha\langle 0|0\rangle + \beta\cancel{\langle 0|1\rangle} = \alpha \ (\lambda_0)$

$$p_0 = F(|\psi\rangle, |0\rangle) = |\langle 0|\psi\rangle|^2 = |\lambda_0|^2 = \underbrace{\cos^2\gamma}_{\text{geometrical interpretation}}$$

(α)

⇒ the closer the initial qubit to the final eigenstate, the higher the prob.

$$p_1 = F(|\psi\rangle, |1\rangle) = |\langle 1|\psi\rangle|^2 = |\lambda_1|^2$$

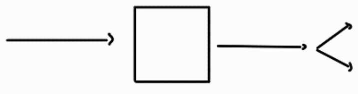
(β)

$$\underbrace{p_0 + p_1}_{\cos^2\gamma + \sin^2\gamma} = 1 \Rightarrow p_1 = 1 - |\alpha|^2 = 1 - \cos^2\gamma = \sin^2\gamma \ \left(= \cos^2\left(\tfrac{\pi}{2} - \gamma\right)\right)$$

formalizing the geometric interp.:

where $\{|\psi_n\rangle\}$ is an orthonormal basis of eigenvectors of A

we normalize for comodity



measurement

$$|\psi_{PM}\rangle = \frac{\hat{\pi}_n |\psi\rangle}{\| \hat{\pi}_n |\psi\rangle \|} \quad a_n \;\; ① \qquad w/ \;\; \hat{\pi}_n = |\psi_n\rangle\langle\psi_n| \quad \text{and prob. } P_n = F(\psi, \psi_n) = \underbrace{\| \hat{\pi}_n |\psi\rangle \|^2}_{} \;\; ②$$

square of the "length" of the projection

this must be demonstrated (① and ②):

① $$|\psi_{PM}\rangle = \frac{\overbrace{|\psi_n\rangle\langle\psi_n}^{\hat{\pi}_n}\overbrace{|\psi\rangle}^{}}{\| |\psi_n\rangle\langle\psi_n|\psi\rangle \|} \quad (\langle\psi_n|\psi\rangle = \lambda_n) \quad = \frac{\lambda_n}{|\lambda_n|}|\psi_n\rangle = e^{J\gamma}\cdot|\psi_n\rangle$$ $\Rightarrow$ the final result is exactly the eigenstate $|\psi_n\rangle$ (aside from a phase term)

② $$\| \hat{\pi}_n |\psi\rangle \|^2 = \langle\psi|\hat{\pi}_n\hat{\pi}_n|\psi\rangle = \langle\psi|\hat{\pi}_n|\psi\rangle = \langle\psi|\psi_n\rangle\langle\psi_n|\psi\rangle = \langle\psi_n|\psi\rangle^*\langle\psi_n|\psi\rangle = |\langle\psi_n|\psi\rangle|^2 = P_n$$

$\left[(\hat{\pi}_n|\psi\rangle)^\dagger = |\psi\rangle^\dagger \hat{\pi}_n^\dagger = \langle\psi|\hat{\pi}_n \right]$

idempotence: also describes the fact that repeating the measurement gives the same result (repeating the orthogonal proj.)

lastly we may show that $\sum_n P_n = 1$:

$$\sum_n P_n = \sum_n F(\psi, \psi_n) = \sum_n |\underbrace{\langle\psi_n|\psi\rangle}_{\lambda_n}|^2 = \sum_n |\lambda_n|^2 = \|\psi\|^2 = 1$$ (we consider ψ normalized (otherwise we have to consider the general expr. of the fidelity))

expectation value of an observable A in a quantum state ψ:

e.g. energy, spin, polarization ecc. (any physical state)

$$\langle A\rangle_\psi = \frac{\langle\psi|\hat{A}|\psi\rangle}{\langle\psi|\psi\rangle}$$

real number since $\hat{A}$ is Hermitian

squared norm, so also positive

($\hat{A}$ is the Hermitian operator describing A)

=> so $\langle A\rangle_\psi$ is a real number

physical interpretation: $\langle A\rangle_\psi$ is the statistical avg. of a random variable that gives the result of the measurement of A

$$|\psi\rangle \rightsquigarrow \boxed{\hat{A}} \rightsquigarrow A = \begin{cases} a_0 \\ a_1 \\ \vdots \end{cases}$$

w/ some prob. $P_0 = (e_0|\psi)$

eigenvalues are corresponding to eigenvectors e_n

discrete real random var.

$\{|e_n\rangle\}_{n=0,1,\dots}$ is an orthonormal basis formed by eigenstates of $\hat{A}$

we can see that the physical interpretation is meaningful:

statistical mean $= \mu_A = \sum_n a_n P_n$ probability

in a normalized quantum state => $\langle A\rangle_\psi = \langle\psi|\hat{A}|\psi\rangle$

closure prop.: $\hat{\mathcal{I}} = \sum_n \hat{\Pi}_n$ orthogonal projector on ψ_n where $\{|\psi_n\rangle\}$ is some orthonormal bases => we chose to expand on the particular bases $\{|e_n\rangle\}$

$$\Rightarrow\ |\psi\rangle = \hat{\mathcal{I}}|\psi\rangle = \sum_n \hat{\Pi}_{e_n}|\psi\rangle = \sum_n |e_n\rangle\langle e_n|\psi\rangle = \sum_n \lambda_n |e_n\rangle \quad \text{and} \quad \langle\psi| = \sum_n \lambda_n^* \langle e_n|$$

$$\hookrightarrow \langle A\rangle_\psi = \sum_m\sum_n \lambda_m^*\lambda_n \langle e_m|\underbrace{\hat{A}|e_n\rangle}_{\hat{A}|e_n\rangle = a_n|e_n\rangle} \Rightarrow \langle A\rangle_\psi = \sum_m\sum_n \lambda_m^*\lambda_n a_n \overbrace{\langle e_m|e_n\rangle}^{\delta_{mn}} = \sum_m |\lambda_m|^2 \cdot a_m$$

(a_n eigenvalues of e_n)

$\lambda_m = \langle e_m|\psi\rangle$

$\Rightarrow \langle A\rangle_\psi = \sum_m a_m P_m$ def. of avg. w/ probabilities $P_m = |\lambda_m|^2$

furthermore, being a random non deterministic measurement it is important to def. the uncertainty

uncertainty of an observable

$(\Delta A)_\psi = \sqrt{(\Delta A)^2_\psi}$ std. deviation σ_A of the results of measurements

(correspondingly $(\Delta A)^2_\psi$ is the variance σ_A^2)

$\sigma_A^2 = E[(A-\bar{A})^2]$ where $\bar{A} = E[A]$ avg. value (μ_A)

(the variance σ_A^2 can also be written as $\sigma_A^2 = E[A^2] - \bar{A}^2$)

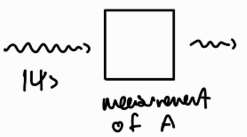
$\mu_A = \sum_m a_m P_m = E[A] = \langle A\rangle_\psi$

$$\Rightarrow (\Delta A)^2_\psi = \langle \underbrace{(A - \langle A\rangle)^2}_{E[(A-\bar{A})^2]} \rangle_\psi = \langle A^2 - 2A\langle A\rangle_\psi + \langle A\rangle^2_\psi\rangle_\psi = \langle A^2\rangle_\psi - 2\langle A\rangle^2_\psi + \langle A\rangle^2_\psi = \langle A^2\rangle_\psi - \langle A\rangle^2_\psi$$

$E[A]$

$$(\Delta A)^2_\psi = \langle A^2\rangle_\psi - \langle A\rangle^2_\psi = \langle\psi|\hat{A}^2|\psi\rangle - \langle\psi|\hat{A}|\psi\rangle^2$$

in quantum physics this uncertainty is intrinsic to the measurement so even w/ perfect precision devices there is still some degree of uncertainty



$\begin{cases} A = a_0 \\ A = a_1 \\ \vdots \end{cases}$ and quantum collapse into $|e_0\rangle$ w/ prob. $|\langle e_0|\psi\rangle|^2$ (fidelity)

particular case where $|\psi\rangle = e^{j\phi}|e\rangle$ (initial state is an eigenvector) ← phase factor

the generic prob. $P_n = |\langle e_n|\psi\rangle|^2 = |\langle e_n|e^{j\phi}|e_m\rangle|^2 = |\langle e_n|e_m\rangle|^2 \begin{cases} 1 & \text{if } e_n = e_m \ (m=n,\ \text{same eigenstate}) \\ 0 & \text{eigenvectors corresponding to diff. eigenvalues are } \perp \end{cases}$

(for a normal op., and $\hat{A}$ is normal since it is Hermitian)

so if we start from an eigenstate the measurement is deterministic

=> $(\mu_A)_{e_m} = a_m$ corresponding eigenvalue

=> $(\sigma_A)_{e_m} = 0$ there is no uncertainty

indeed:

1) $\langle A\rangle_{e_m} = \langle e_m|\hat{A}|e_m\rangle = \langle e_m|a_m|e_m\rangle = a_m\langle e_m|e_m\rangle = a_m$

[$\hat{A}|e_m\rangle = a_m|e_m\rangle$ def. of eigenstate]

2) $(\Delta A)^2_{e_m} = \langle A^2\rangle_{e_m} - \langle A\rangle^2_{e_m}$

$\hat{A} = \sum_n a_n|e_n\rangle\langle e_n|$ spectral decomposition

($f(\hat{A}) = \sum_n f(a_n)|e_n\rangle\langle e_n|$ same eigenstates but diff. eigenvalues)

so:

$$\hat{A}^2|e_m\rangle = \hat{A}(\hat{A}|e_m\rangle) = \hat{A}(a_m|e_m\rangle) = a_m^2|e_m\rangle$$

=> $\langle A^2\rangle_{e_m} = \langle e_m|\hat{A}^2|e_m\rangle = \langle e_m|a_m^2|e_m\rangle = a_m^2\langle e_m|e_m\rangle = a_m^2$

and ∴ $(\Delta A)^2_{e_m} = \langle A^2\rangle_{e_m} - \langle A\rangle^2_{e_m} = a_m^2 - (a_m)^2 = a_m^2 - a_m^2 = \emptyset$

observable in a 2 state quantum system

↳ described by a Hermitian op. $\hat{A}: \mathbb{H} \to \mathbb{H}$ acting on a 2-dim. $\mathbb{H}$

=> $\hat{A} = a_0|e_0\rangle\langle e_0| + a_1|e_1\rangle\langle e_1|$ (spectral decomp. in 2-D)

only 2 possible results $\begin{cases} a_0 \\ a_1 \end{cases}$ ($a_0 = a_1$ trivial case) non-degenerate case $\Leftrightarrow a_0 \neq a_1 \Leftrightarrow$ only one pair of orthogonal states

so only 2 possible results of measurement :
* $a_0 \longrightarrow +1$ (qubit $\emptyset$)
* $a_1 \longrightarrow -1$ (qubit 1)

$$\hat{A} = f(A) \quad w/ \begin{cases} f(a_0) = 1 \\ f(a_1) = -1 \end{cases}$$

qubit measurement

part. case of quantum measurement

$$|\tilde{\psi}\rangle \longrightarrow \boxed{\hat{U}} \longrightarrow |\psi\rangle$$

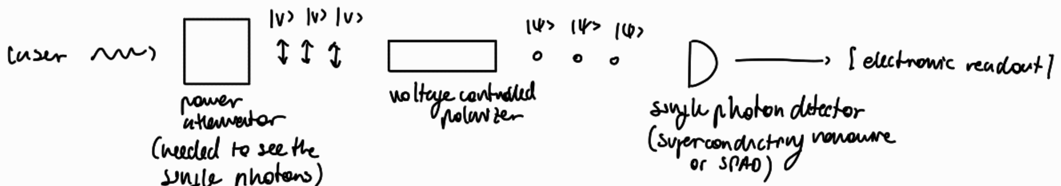
e.g. state of polarization

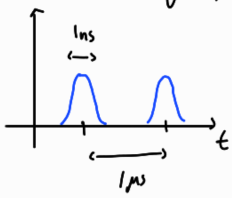
$|0\rangle = |H\rangle$, $|1\rangle = |V\rangle$

$|\tilde{\psi}\rangle = \alpha|H\rangle + \beta|V\rangle$

quantum gate (unitary op.) can be implemented w/ a polarizer filter (voltage controlled)

we can implement a stream of coherent photons w/ a laser





photon rate set by power attenuator

$$\sim\sim\sim\!\!\to \boxed{\hat{A}}$$

→ result of measurement of A ⇒ either a_0 or a_1 (real eigenvalues corresponding to p.m. qubits)

→ quantum collapse ⇒ p.m. qubit $|\varphi_0\rangle$ or $|\varphi_1\rangle$ (orthogonal)

uncertainty principle

$$(\Delta A)_\psi \, (\Delta B)_\psi \geq \frac{1}{2}\left| \frac{\langle [\hat{A},\hat{B}] \rangle}{j} \right| = \frac{1}{2} \left| \langle [\hat{A},\hat{B}] \rangle \right|$$

commutator

uncertainties corresponding to 2 diff. observables related to the same quantum state

in classical physics the lower bound of uncertainty is ∅. However in quantum physics we have a lower limit to the product of uncertainty of the two observables

$[\hat{A},\hat{B}] = \hat{A}\cdot\hat{B} - \hat{B}\cdot\hat{A}$ def. of commutator

$[\hat{A},\hat{B}]$ is <u>anti-Hermitian</u>: i.e. $\underline{\hat{A}^+ = -\hat{A}}$

Indeed:

$$[\hat{A},\hat{B}]^\dagger = (\hat{A}\cdot\hat{B} - \hat{B}\cdot\hat{A})^\dagger = (\hat{A}\hat{B})^\dagger - (\hat{B}\hat{A})^\dagger = \hat{B}^+\hat{A}^+ - \hat{A}^+\hat{B}^+ \overset{\hat{A},\hat{B}\ \text{Hermitian}}{=} BA - AB = -(\hat{A}\hat{B} - \hat{B}\hat{A}) = -[\hat{A},\hat{B}]$$

an antiHermitian op. can be written as the prod. of J and a Hermitian op.

$$\Rightarrow \underset{\text{anti Hermitian}}{\hat{A}} = J \cdot \underset{\text{Hermitian}}{\hat{A}}$$

$\hat{A}, \hat{B}$ Hermitian $\Rightarrow [\hat{A}, \hat{B}]$ anti Hermitian $\Rightarrow \hat{C} = \frac{[\hat{A}, \hat{B}]}{J}$ is Hermitian

indeed:

$$\hat{C}^+ = \left(\frac{[\hat{A}, \hat{B}]}{J}\right)^+ \underset{\underset{[\hat{A},\hat{B}]^+ = -[A,B]}{\uparrow}}{=} \frac{-[\hat{A}, \hat{B}]}{-J} = \frac{[\hat{A}, \hat{B}]}{J} = \hat{C}$$

$$(\Delta A)_\psi (\Delta B)_\psi \geq \frac{1}{2} \left| \langle \frac{[\hat{A}, \hat{B}]}{J} \rangle \right| = \frac{1}{2} \left| \langle \psi | \hat{A}\hat{B} - \hat{B}\hat{A} | \psi \rangle \right|$$

obs. if $[\hat{A}, \hat{B}] = \emptyset \Rightarrow (\Delta A)_\psi (\Delta B)_\psi \geq 0$

two observables are said compatible (or simultaneously measurable) if the corresponding Hermitian operators commute

↳ i.e. A, B compatible $\Leftrightarrow [\hat{A}, \hat{B}] = 0$ ($\hat{A}\hat{B} = \hat{B}\hat{A}$ - in general this is not the case)

A, B compatible observable ($[A,B] = \emptyset$) $\Rightarrow (\Delta A)_\psi (\Delta B)_\psi \geq \emptyset$ for any qubit ψ

theo.

in a finite dim. $\mathbb{H}$ two normal op. $\hat{A} : \mathbb{H} \to \mathbb{H}$, $\hat{B} : \mathbb{H} \to \mathbb{H}$ commute $\Leftrightarrow$ there exists an orthonormal bases formed by simultaneous eigenstates for both op., $\{|e_n\rangle\}_{n=0,1,\dots,D-1}$

$|e_n\rangle = |e_n^{(A,B)}\rangle$ eigenstates of both the operators $\Rightarrow \begin{cases} \hat{A}|e_n\rangle = a_n|e_n\rangle \\ \hat{B}|e_n\rangle = b_n|e_n\rangle \end{cases}$

if $\hat{A}, \hat{B}$ commute the post measurement eigenstate will be the same for both operators

$\Rightarrow A, B$ simultaneously measurable $\Leftrightarrow$ there exists a complete set of common eigenstates $|e_n\rangle = |e_n\rangle^{(A,B)}$ having well defined values (measured w/ absolute certainty)

$[\hat{A},\hat{B}]=0$ $\xrightarrow{\quad}$ / $\overset{\times}{\longleftarrow}$ there exists an orthonormal basis $\{|\varphi_n\rangle\}_{n=0,1,\dots,D-1}$ formed by common eigenstates of $\hat{A}$ and $\hat{B}$

in the ∞ countable case

Hp. A, B are observable (so $\hat{A}, \hat{B}$ Hermitian. Being normal is also suff.) w/ discrete spectrum and $\mathbb{H}$ has a finite or ∞ countable dimension. Moreover, $\{|\varphi_n\rangle^{(A)}\} = \{|\varphi_n\rangle^{(B)}\}$ is an orthonormal basis of $\mathbb{H}$

teo.

$\Rightarrow$ $[\hat{A},\hat{B}]=\emptyset$

dim.

$\hat{A} = \sum_n a_n |\varphi_n\rangle^{(A)}\langle\varphi_n|^{(A)}$ (spectral decomp.)

$\hat{B} = \sum_n b_n |\varphi_n\rangle^{(B)}\langle\varphi_n|^{(B)}$ (")

$$\Rightarrow \hat{A}\cdot\hat{B} = \left(\sum_n a_n|\varphi_n\rangle\langle\varphi_n|\right)\left(\sum_m b_m|\varphi_m\rangle\langle\varphi_m|\right) = \sum_m\sum_n a_n b_m \underbrace{\hat{\pi}_m\hat{\pi}_n}_{=\hat{\pi}_m\delta_{mn}}$$

$m\neq n \Rightarrow = \emptyset$

$m=n \Rightarrow \hat{\pi}_m^2 = \hat{\pi}_n^2 = \hat{\pi}_m = \hat{\pi}_n$ (idempotence)

$= \sum_m a_m b_m \hat{\pi}_m$

and likewise we obtain $\hat{B}\cdot\hat{A} = \sum_m b_m a_m \hat{\pi}_m$

so:

$\hat{A}\cdot\hat{B} = \hat{B}\cdot\hat{A} \Rightarrow [\hat{A},\hat{B}]=\emptyset$

$|\psi\rangle \rightsquigarrow \boxed{}$ $\rightsquigarrow$ p.m. quantum state $\begin{cases}|\varphi_0\rangle\\|\varphi_1\rangle\\ \vdots \\ |\varphi_n\rangle\end{cases}$ w/ corresponding prob. $F(\psi,\varphi_n)$

simultaneous measurement of $\hat{A}$ and $\hat{B}$ $\rightsquigarrow$ $\begin{cases}A=a_n\\B=b_n\end{cases}$ well def. values of observables (eigenvalues corresponding to the p.m. state)

considering a finite dim. $\mathbb{H}$ (dim. = D)

$\hookrightarrow$ 2 observables are said complementary when:

I) A and B are NOT compatible (not sim. measurable) i.e. $\hat{A},\hat{B}$ do not commute $\Leftrightarrow [\hat{A},\hat{B}]\neq 0$

II) the 2 orthonormal basis $\{|\varphi_m\rangle^{(A)}\}$ and $\{|\varphi_n\rangle^{(B)}\}$ formed respectively by eigenstates of $\hat{A}$ and $\hat{B}$ are mutually unbiased i.e. $|\langle\varphi_m^{(A)}|\varphi_n^{(B)}\rangle|^2 =$ independent on the indices m,n $\Rightarrow$ so it is const.

$\Rightarrow F(\varphi_m^{(A)},\varphi_n^{(B)}) = \frac{1}{D}$ const. (all fidelities are the same)

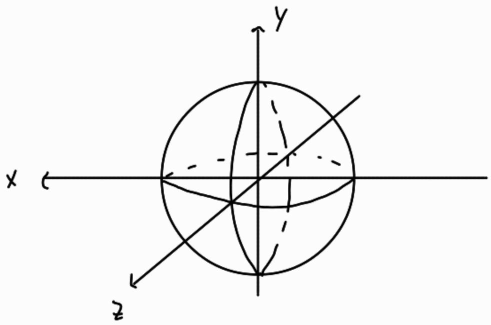
NOT an eigenstate of B $\Rightarrow$ the second measurement will have some uncertainty

$|\psi\rangle \rightsquigarrow \boxed{} \xrightarrow[(A=a_m)]{|\varphi_m^A\rangle} \boxed{} \xrightarrow[(B=b_n)]{|\varphi_n^B\rangle}$

measurement of A — measurement of B

so there are $D\times D$ different situations $\Rightarrow$ $D\times D$ different conditioned probabilities

$$P(B=b_n\,|\,A=a_m) = F(\varphi_n^{(A)},\varphi_m^{(B)}) = \text{const., independent of } m,n = \frac{1}{D}$$ (we have D equiprobable probabilities)



we want to see that $\hat{x}$ and $\hat{z}$ are complementary

we must verify that:

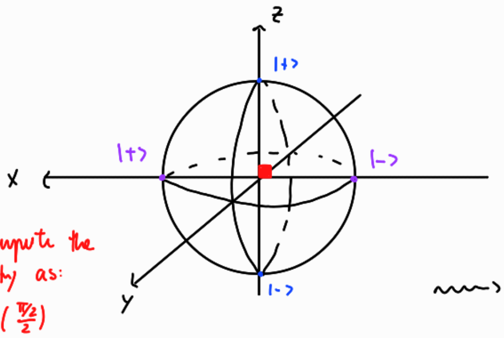
$$[\hat{x},\hat{z}] \longrightarrow [x,z] = xz - zx = \emptyset$$

$$x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\quad z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\begin{cases} xz = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \frac{y}{j} \\ zx = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \frac{-y}{j} \end{cases}$$

$\Rightarrow$ so $xz \neq zx \Rightarrow [x,z] \neq 0$

we could also directly see this on the Bloch sphere:

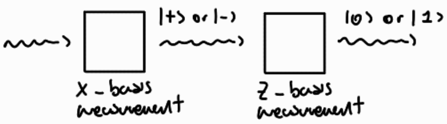


$\hat{x}$ - basis $\{|+\rangle, |-\rangle\}$

$\hat{z}$ - basis $\{|0\rangle, |1\rangle\}$

bases formed by eigenvectors are not common

we compute the fidelity as: $\cos^2\left(\frac{\pi/2}{2}\right)$



$F(|+\rangle,|0\rangle) = |\langle +|0\rangle|^2 = 1/2$

$F(|+\rangle,|1\rangle) = \dots = 1/2$

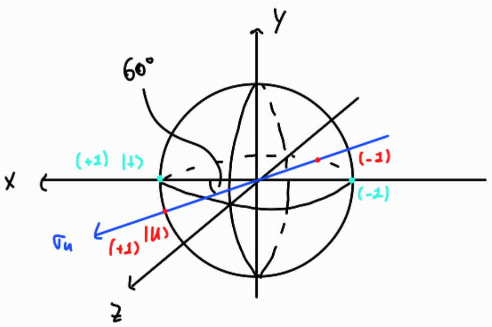
$F(|-\rangle,|0\rangle) = \dots = 1/2$

$F(|-\rangle,|0\rangle) = \dots = 1/2$

$\hookrightarrow$ 2 Pauli op. $\hat{\sigma}_{u'}, \hat{\sigma}_{u''}$ are complementary $\Leftrightarrow$ the corresponding rotation axis' on the Bloch sphere are orthogonal

$\{\hat{x},\hat{y},\hat{z}\}$ is a maximal set of mutually complementary observables

every other observable whis is mutually complementary, $\hat{A}$, is: $\hat{A} = f(\hat{x})$ or $f(\hat{y})$ or $f(\hat{z})$
(so it has the same eigenstates but diff. eigenvalues)



$P(\sigma_u = 1 | x = 1) = F(|+\rangle, |u\rangle) = \cos^2\left(\frac{60°}{2}\right) = 75\%$

so we a biasing towards $|+\rangle$ w.r.t. $|-\rangle$

(likewise $P(\sigma_u = -1 | x = 1) = 25\%$)

obs. the 2 prob. add to 100%

X, Y, Z are a maximal set of mutually complementary observables

$$\hat{A} = \sum_n a_n |e_n^{(A)}\rangle \langle e_n^{(A)}| \quad \text{observable}$$

where $\{|e_0^{(A)}\rangle, |e_1^{(A)}\rangle\}$ orthonormal eigenstates are eq. to the Pauli operator

$$\Rightarrow \hat{\sigma}_{u_A} = |e_0^{(A)}\rangle\langle e_0^{(A)}| - |e_1^{(A)}\rangle\langle e_1^{(A)}| \quad \text{spectral decomp. w/ eigenvalues } \pm 1$$

starting from a generic observable we can write it as a Pauli operator w/ the same eigenstates (equivalent Pauli op. in terms of measurement)

↳ measurement of $\hat{A}$ is equivalent (information theory ⇒ the only thing that matters is the post measurement quantum state) to the measurement of σ_A (Pauli op. w/ same eigenstates of $\hat{A}$)

having a maximal set of mutually complementary observables is fundamental for quantum information theory ⇒ how do we obtain the complete info on the qubit?

(that is, the position on the Bloch sphere of the transmitted bit)

⇒ the only way is to have a simultaneous measurement of 3 observables forming a maximal set of mutually complementary observables: this is NOT possible since, being mutually complementary, they are not compatible so we will be limited by the uncertainty principle

↳ impossible to recover the complete knowledge of a qubit

$\hat{X}_0 = \hat{\sigma}_x = \hat{\sigma}_1$
$\hat{Y}_0 = \hat{\sigma}_y = \hat{\sigma}_2$
$\hat{Z}_0 = \hat{\sigma}_z = \hat{\sigma}_3$

it is possible to demonstrate that:

$$\begin{cases} XY = jZ \\ YX = -XY \Rightarrow \text{anticommutative} \end{cases}$$

in general for a maximal set of mutually complementary Pauli operators:

$$\Rightarrow \hat{\sigma}_j \hat{\sigma}_k = j \cdot \hat{\sigma}_l$$

$(j, k, l) = (1,2,3)$ or cyclic permutation (the same rule holds)
$(3,1,2)$
$(2,3,1)$

and in general they are anticommutative:

$$\hat{\sigma}_j \hat{\sigma}_k = -\hat{\sigma}_k \hat{\sigma}_j \quad (\text{for } j \neq k)$$

involutory property: $\hat{\sigma}_k^2 = \hat{I}$ (for any Pauli op.)

σ_k has $\lambda_0 = 1$, $\lambda_1 = -1$

⇒ $\det(\hat{\sigma}_k)$ = prod. between eigenvalues = -1

⇒ $tr(\hat{\sigma}_k)$ = sum " " = $\emptyset$

$\hat{\sigma}_j \hat{\sigma}_k \hat{\sigma}_l = j \cdot \hat{I}$ $\quad (j,k,l) = (1,2,3)$ or cyclic permutation

e.g. an electron can be implemented as the quantum state of spin of an electron

$\vec{s}$ (classical intrinsic angular momentum)
$\vec{s} = (s_x, s_y, s_z)$ ⟶ quantum

$$\begin{cases} \hat{S}_x = \frac{1}{2}\hbar \hat{X} \\ \hat{S}_y = \frac{1}{2}\hbar \hat{Y} \\ \hat{S}_z = \frac{1}{2}\hbar \hat{Z} \end{cases}$$

(electron is a Fermion, that is, particle w/ half integer quantum spin number)
⇓
the two only possible values for the spin components along any axis are:
- $+\frac{1}{2}\hbar$ (spin up)
- $-\frac{1}{2}\hbar$ (spin down)

e^- $\Rightarrow$ $|\uparrow\rangle$ "spin up", $|\downarrow\rangle$ "spin down" $\Rightarrow$ $|\psi\rangle = \alpha|\uparrow\rangle_{\hat{v}} + \beta|\downarrow\rangle_{\hat{v}}$

orthonormal

you can build a quantum state w/ spin up and spin down around the axis $\hat{v}$ w/ proper expansion coeff.

we can associate:

$\hat{S}_x = \frac{1}{2}\hbar\hat{x}$ $\quad \{|+\rangle, |-\rangle\} \Rightarrow \{|\leftarrow\rangle, |\rightarrow\rangle\}$

$\hat{S}_y = \frac{1}{2}\hbar\hat{y}$ $\quad \{|\circlearrowright\rangle, |-\circlearrowright\rangle\} \Rightarrow \{|\swarrow\rangle, |\nearrow\rangle\}$

$\hat{S}_z = \frac{1}{2}\hbar\hat{z}$ $\quad \{|0\rangle, |1\rangle\} \Rightarrow \{|\uparrow\rangle, |\downarrow\rangle\}$

qubit implemented as state of polarization of a single photon

(diagonal) $\{|Q\rangle, |-Q\rangle\}$ is the orthonormal basis formed by the eigenstates of $\hat{Y}$

(circular) $\{|L\rangle, |R\rangle\}$ " " " " of $\hat{Z}$

(vertical/horizontal) $\{|H\rangle, |V\rangle\}$ " " " " of $\hat{X}$

$\langle X\rangle_\psi$ = x-coordinate of the point P representing ψ on the Bloch sphere

$\langle Y\rangle_\psi$ = y-coordinate of " " " "

$\langle Z\rangle_\psi$ = z-coordinate of " " " "

$\langle X\rangle_\psi = \langle\psi|\hat{x}|\psi\rangle$ w/ $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $\|\psi\|^2 = 1$

$$[\alpha^* \ \beta^*]\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix} = [\alpha^* \ \beta^*]\begin{bmatrix}\beta\\\alpha\end{bmatrix} = \alpha^*\beta + \beta^*\alpha$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \Rightarrow \langle -|\hat{x}|-\rangle = \frac{1}{\sqrt{2}}\left(\frac{-1}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}\cdot\left(\frac{-1}{\sqrt{2}}\right) = -1$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \Rightarrow \langle +|\hat{x}|-\rangle = \frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{2}} = +1$$

in general: $\langle\hat{A}\rangle_{e_n(a)} = a$

eigenstate — eigenvalue

in a finite dim. $\mathbb{H}$: $\min\{a_n\} \le \langle A\rangle_e = \langle\psi|\hat{A}|\psi\rangle \le \max\{a_n\}$

generic quantum state

for a Pauli op.: $-1 \le \langle\hat{\sigma}_n\rangle \le +1$

it is also possible to demonstrate that:

$\langle x\rangle_\psi = \alpha^*\beta + \beta^*\alpha$ is the x-coordinate of the point representing ψ on the Bloch sphere

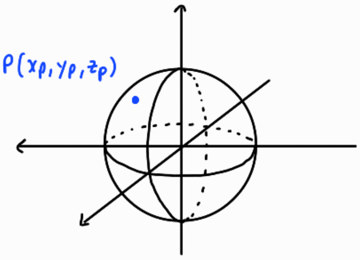
$$\begin{cases} x_P = \sin\theta\cos\phi \\ y_P = \sin\theta\sin\phi \\ z_P = \cos\theta \end{cases}$$

$$\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \begin{bmatrix}\cos(\theta/2)\\ \sin(\theta/2)\cdot e^{j\phi}\end{bmatrix}$$

$$\alpha^*\beta + \beta^*\alpha = \cos(\theta/2)\sin(\theta/2)e^{-j\phi} + \cos(\theta/2)\sin(\theta/2)e^{j\phi}$$

$$= 2\cos(\theta/2)\sin(\theta/2)\cos\phi$$

$$= \sin\theta\cos\phi$$



$\langle x\rangle_\psi = x_p$

$(\Delta x)_\psi = \sqrt{(\Delta x)^2_\psi} = \sqrt{\langle (x-\langle x\rangle)^2\rangle} = \sqrt{\langle x^2\rangle_\psi - \langle x\rangle^2_\psi}$

$\langle\psi|\hat{x}^2|\psi\rangle$ — $\hat{x}^2 = \hat{\mathbb{1}}$ involutory prop. ($\hat{x}$ is a Pauli operator)

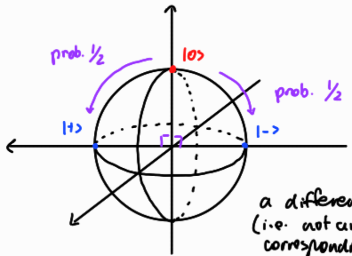
$\langle\psi|\hat{x}|\psi\rangle^2 = \langle x\rangle^2_\psi = x_p^2$

$$\Rightarrow (\Delta x)^2_\psi = \langle\psi|\hat{\mathbb{1}}|\psi\rangle - x_p^2 = \underbrace{\langle\psi|\psi\rangle}_{\|\psi\|^2 = 1} - x_p^2 = 1 - x_p^2 \Rightarrow (\Delta x)_\psi = \sqrt{1-x_p^2} \Leftrightarrow \begin{cases} x_p = +1 \\ x_p = -1 \end{cases} \Rightarrow x\text{-bases} \Rightarrow \begin{cases} |\psi\rangle = |+\rangle \\ |\psi\rangle = |-\rangle \end{cases}$$

$-1 \le x_p \le +1$, but more in general: min(eigenvalue) $\le \langle x\rangle_\psi \le$ max(eigenvalue)

(for a Pauli op.: $\gamma_{1,2} = \pm 1 \Rightarrow -1 \le \langle x\rangle_\psi \le +1$)

$\langle x\rangle_\psi = -1$ when $|\psi\rangle = |-\rangle$ (corresponding eigenstate to eigenvalue -1)
$\langle x\rangle_\psi = +1$ when $|\psi\rangle = |+\rangle$ (" " " $+1$)



a different point (i.e. not an eigenvalue corresponding to a complementary operator) would have some biasing towards $|+\rangle$ or $|-\rangle$ and $\therefore$ a lower uncertainty

$|0\rangle$ is an eigenstate of a complementary operator $\Rightarrow$ the uncertainty is maximum (indeed the probability is equiprobable $= 1/2$)

($(\Delta x)_{|0\rangle} = 1$ max. possible uncertainty)

$\Rightarrow \quad 0 \le (\Delta x)_\psi \le 1$

when $|\psi\rangle$ is an eigenstate of $\hat{x}$

when $|\psi\rangle$ is an eigenstate of a complementary Pauli op. to $\hat{x}$

likewise: $\langle y\rangle_\psi = y_p$ and $-1 \le y_p \le +1 \Rightarrow (\Delta y)_\psi = \sqrt{1-y_p^2} = 0 \Leftrightarrow y_p = \pm 1 \begin{cases} +1 \Rightarrow |\psi\rangle = |J\rangle \\ -1 \Rightarrow |\psi\rangle = |-J\rangle \end{cases}$

once again $(\Delta y)_{|0\rangle} = 1$ (proj. of $|0\rangle$ onto the y-axis is 0)

and $0 \le (\Delta y)_\psi \le 1$

$|\psi\rangle$ is an eigenstate of $\hat{y}$

$|\psi\rangle$ is an eigenstate of a complementary Pauli op. to $\hat{y}$

e.g.

$$\langle y\rangle_\psi = \langle\psi|\hat{y}|\psi\rangle \xrightarrow[\text{comp. basis}]{} [\alpha^* \ \beta^*]\begin{bmatrix} 0 & -J \\ J & 0\end{bmatrix}\begin{bmatrix}\alpha \\ \beta\end{bmatrix} = [\alpha^* \ \beta^*]\begin{bmatrix} -J\beta \\ J\alpha\end{bmatrix} = -J\alpha^*\beta + J\alpha\beta^* = J(\alpha\beta^* - \alpha^*\beta)$$

$$\Rightarrow \begin{bmatrix}\alpha \\ \beta\end{bmatrix} = \begin{bmatrix} \cos\theta/2 \\ \sin\theta/2 \cdot e^{J\phi}\end{bmatrix} \Rightarrow\ = J\left[\cos\tfrac{\theta}{2}\cdot\sin\tfrac{\theta}{2}\cdot e^{-J\phi} - \cos\tfrac{\theta}{2}\cdot\sin\tfrac{\theta}{2}\cdot e^{J\phi}\right] = -J\cdot\cos\tfrac{\theta}{2}\cdot\sin\tfrac{\theta}{2}\left[e^{J\phi} - e^{-J\phi}\right]$$

$$= -2\cdot J\cos\tfrac{\theta}{2}\cdot\sin\tfrac{\theta}{2}\cdot\left[\frac{e^{J\phi}-e^{-J\phi}}{2}\right]$$

$$= -2\cdot J\cdot J\cdot\cos\tfrac{\theta}{2}\cdot\sin\tfrac{\theta}{2}\cdot\left[\frac{e^{J\phi}-e^{-J\phi}}{2J}\right]$$

$$= 2\cos\left(\tfrac{\theta}{2}\right)\cdot\sin\left(\tfrac{\theta}{2}\right)\cdot\sin(\phi)$$

[$\sin(2\alpha) = \sin\alpha\cos\alpha + \cos\alpha\sin\alpha = 2\sin\alpha\cos\alpha$
$\Rightarrow \alpha = \frac{\theta}{2} \Rightarrow 2\cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right) = \sin\theta$]

$\Rightarrow \quad = \sin\theta\cdot\sin\phi$

$$\begin{cases} x_p = \sin\theta\cos\phi \\ y_p = \sin\theta\sin\phi \\ z_p = \cos\theta \end{cases}$$

e.g. 2

$$\langle z\rangle_\psi = \langle\psi|\hat z|\psi\rangle = [\alpha^* \ \beta^*]\begin{bmatrix}1&0\\0&-1\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix} = [\alpha^* \ \beta^*]\begin{bmatrix}\alpha\\-\beta\end{bmatrix} = \alpha^*\alpha - \beta^*\beta = |\alpha|^2 - |\beta|^2$$

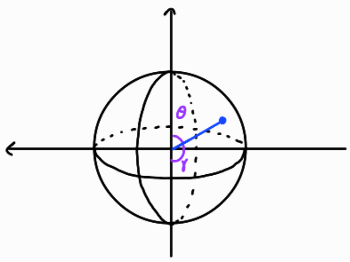
$$= \underbrace{(+1)|\alpha|^2 + (-1)|\beta|^2}_{\text{values weighted by their probability}}$$

Born rule: prob. of a collapse into $|0\rangle$ $\Leftrightarrow$ prob. of measuring $z=+1$ $\Rightarrow$ $F(\psi,0) = |\langle 0|\psi\rangle|^2 = |\alpha|^2$

$$\hat z \underset{\text{spectral decomp.}}{=} (+1)|0\rangle\langle 0| + (-1)|1\rangle\langle 1| = |0\rangle\langle 0| - |1\rangle\langle 1| \Rightarrow \langle\psi|\hat z|\psi\rangle = \underbrace{\langle\psi|0\rangle\langle 0|\psi\rangle}_{\substack{\text{norm of the orthogonal}\\ \text{proj. of } |\psi\rangle \text{ onto } |0\rangle}} - \langle\psi|1\rangle\langle 1|\psi\rangle = \underbrace{|\langle 0|\psi\rangle|^2}_{F(0,\psi)} - \underbrace{|\langle 1|\psi\rangle|^2}_{F(1,\psi)}$$

$\Rightarrow F(\psi,0) = |\langle 0|\psi\rangle|^2 \overset{!}{=} \langle 0|\psi\rangle\langle 0|\psi\rangle^*$

(likewise: $\hat y = |J\rangle\langle -J| - |J\rangle\langle -J|$ and $\hat z = |+\rangle\langle +| - |-\rangle\langle -|$)



$F(\psi,0) = \cos^2(\theta/2)$

$F(\psi,1) = \cos^2(\gamma/2) = \cos^2\left(\frac{\pi}{2} - \frac{\theta}{2}\right) = \sin^2(\theta/2)$

$\Rightarrow F(\psi,0) + F(\psi,1) = \cos^2\theta/2 + \sin^2\theta/2 = 1$ (sum of prob. $= 1$)

this is true in general for eigenstates that are opposite e.g. $|0\rangle$ and $|1\rangle$

so:

$$\hat z = \underbrace{F(\psi,0)}_{\text{eigenstate}} - \underbrace{F(\psi,1)}_{\text{opposite eigenstate}} = \cos^2(\theta/2) - \sin^2(\theta/2) \underset{[\cos 2\alpha = \cos^2\alpha - \sin^2\alpha]}{=} \cos\theta = z_p$$

this is true in general for a Pauli op. $\hat\sigma_u$

$$(\Delta x)(\Delta y) \geq \frac{1}{2}|\langle[\hat x, \hat y]\rangle|$$

$$[\hat x, \hat y] = \hat x\hat y - \hat y\hat x \underset{\text{[Pauli op. are anticommutative]}}{=} \hat x\hat y + \hat x\hat y = 2\hat x\hat y = 2J\hat z$$

($[\hat\sigma_j, \hat\sigma_k] = 2J\hat\sigma_l$ for (j,k,l) or cyclic permutations)

$$\Rightarrow (\Delta x)(\Delta y) \geq \frac{1}{2}|\langle 2J\hat z\rangle| \Rightarrow (\Delta x)_\psi(\Delta y)_\psi \geq |\langle z\rangle_\psi\rangle$$

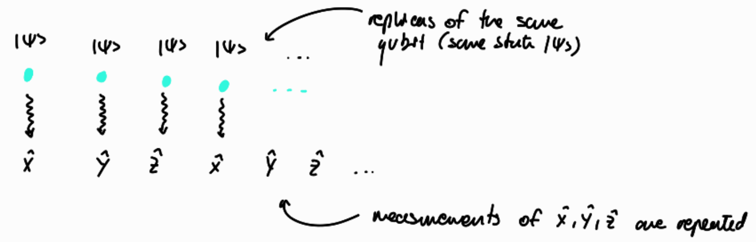
e.g.

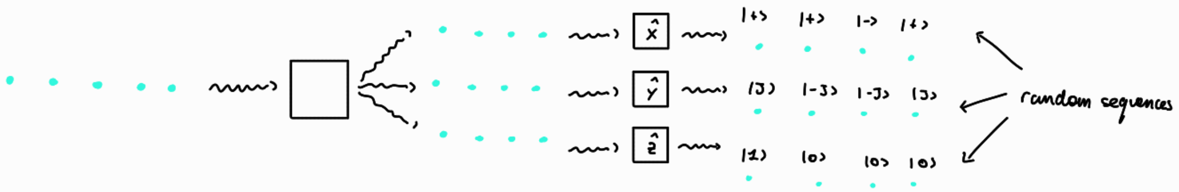
$|\psi\rangle = \underset{\text{eigenstate of } \hat x}{|+\rangle} \Rightarrow \Delta x = 0,\ \Delta y = 1,\ \underbrace{\langle z\rangle_\psi}_{\text{verifies the inequality}} \underset{(\Delta z = 1)}{=} 0$

when one uncertainty is min., the other is max. (complementary operators)

$|\psi\rangle = \underset{\substack{\text{generic eigenstate}\\ \text{of } \hat z \text{ i.e. } |0\rangle \text{ or } |1\rangle}}{|\cdot\rangle} \Rightarrow \Delta x = 1,\ \Delta y = 1,\ \underset{(\Delta z) = 0}{\langle z\rangle_\psi} = \pm 1 \Rightarrow \underbrace{|\langle z\rangle_\psi| = 1}_{\text{verifies the inequality}}$

to obtain the whole info on ρ i.e. x_ρ, y_ρ, z_ρ we need to know the expected values $\langle X \rangle_\psi$, $\langle Y \rangle_\psi$, $\langle Z \rangle_\psi$

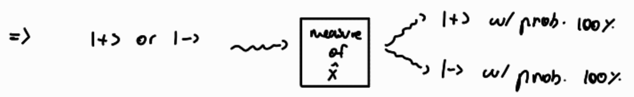




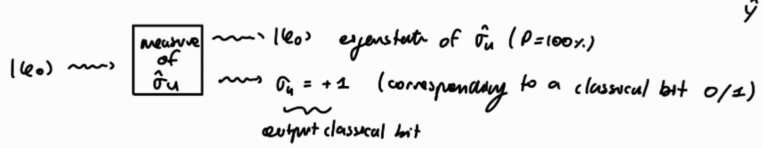
for a large n° of qubits ($\to \infty$): the avg. val. of the sequences $\to \langle X \rangle_\psi, \langle Y \rangle_\psi, \langle Z \rangle_\psi$

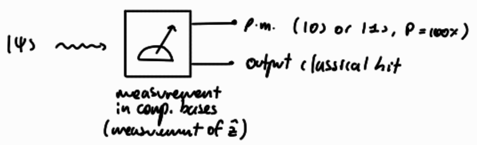
it is possible to reconstruct the state of a single qubit w/ no uncertainty (in theory) w/ a single measurement if and only if we know beforehand that the qubit is an eigenstate of some observable

e.g. if we know the initial qubit is an eigenstate of $\hat{x}$ it can only be $|+\rangle$, $|-\rangle$



we know the complete info on the qubit. This is valid for other observables $\hat{y}$ or $\hat{z}$

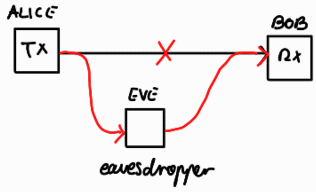




classical communications are ~~NOT~~ secure

classical bits can be copied because they can be measured w/out perturbation

↳ we can have an interceptor and resender



an eavesdropper can intercept and extract information w/out perturbation

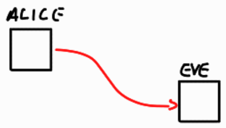
on the other hand, quantum communication CAN be made secure

an arbitrary unknown quantum bit $\underbrace{\text{cannot be copied (cloned)}}_{\text{non cloning theorem}}$

this is related to the quantum measurement process: it is not possible to measure in a deterministic way w/ out perturbing the system

there are only 2 cases when the measurement of a qubit is equivalent to the classical case => that is, when the qubit is one of the two measurement basis states

↳ transmission must occur w/ qubits belonging to diff. basis, they must be selected between basis states of complementary operators



if the ALICE stream of qubits are elements of the basis chosen by EVE we have a random measurement. For ALICE it is suff. to produce her stream choosing between 2 complementary basis.

if ALICE transmits in the z-BASIS: $|0\rangle, |1\rangle, |1\rangle, |0\rangle \dots$ this is just classical communication, and if EVE measures in the z-BASIS, EVE can eavesdrop the communication. The idea is to add another bit of information

e.g. ALICE can choose between: $\left\{ \begin{array}{ll} \{|0\rangle, |1\rangle\} & \text{z-BASIS} \\ \{|+\rangle, |-\rangle\} & \text{x-BASIS} \end{array} \right\}$ they are mutually unbiased

complementary basis guarantee max. randomicity: if we measure $|+\rangle$ in the z basis get $|0\rangle$ or $|1\rangle$ w/ 50% prob. each (max. fidelity = ½ for both)

e.g.

ALICE

$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$
(z)	(x)	(x)	(z)	(x)

second random choice

the second sequence of the chosen basis is itself a bit. We can associate for example ∅ to z and 1 to x so:

$\left(\begin{array}{l} \emptyset \Leftrightarrow |0\rangle \text{ and } |+\rangle \\ 1 \Leftrightarrow |1\rangle \text{ and } |-\rangle \end{array} \right)$ $a_k = \{\emptyset, \emptyset, \emptyset, 1, 1, \dots, \}$

$b_k = \{0, 1, 1, 0, 1, \dots,\}$

(sequence of the basis chosen by ALICE)

note: the two sequences a_k, b_k must be statistically indipendent

w/ these choices, EVE cannot make a deterministic measurement of all the qubits. To clone the sequence, EVE must perfectly know b_k so as to choose the right measurement basis each time.

the security is given by the complementarity of the basis (the two sequences a_k, b_k)

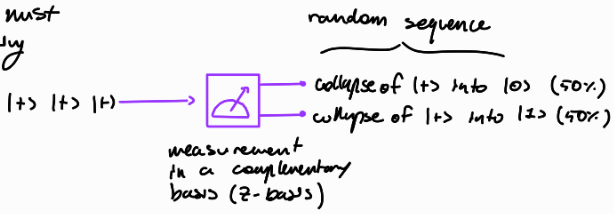
EVE could choose a random seq. b_k or a single basis e.g. Z-basis:

$$b_k' = \{0, 0, 0, \dots, \}$$

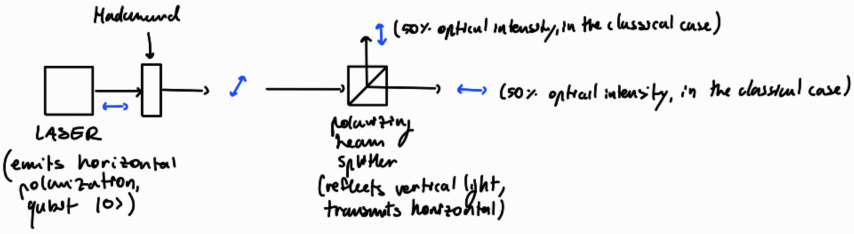
when the basis is different, the result will be random, and the measurement will cause a perturbation

The problem is: BOB is in the same situation as EVE! So BOB must also choose b_k'. So he may choose to generate a sequence using

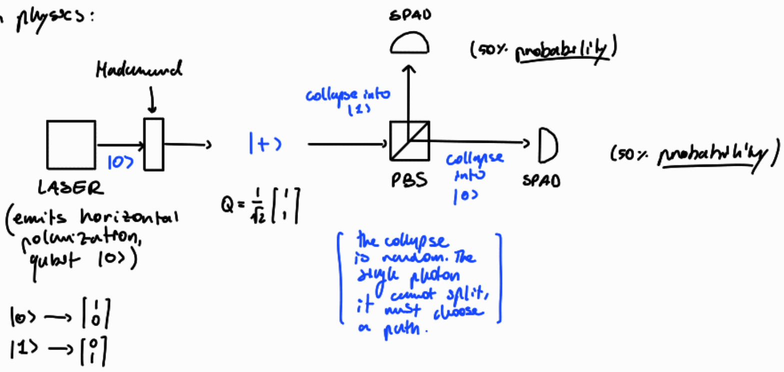
↳ QUANTUM RANDOM NUMBER GENERATOR



physical implementation: (polarized single photons)



in quantum physics:



so BOB generates $b_k' = \{0, 0, 1, 0, 0, 1, 0, \dots\}$. According to this measurement, BOB will perform the measurements.

when $b_k = b_k'$, then $a_k' = a_k$ (classical bits sequence of the results of measurement)

(typically we consider a destructive measurement e.g. SPAD)

$$b_k = \{0, 1, 1, 0, 1, \dots\} \qquad\qquad a_k = \{0, 0, 1, 1, 1, \dots\}$$

$$b_k' = \{0, 0, 1, 0, 0, \dots\} \quad \Rightarrow \quad a_k' = \{0, ?, 1, 1, ?, \dots\}$$

(meaningful measurement)

⇒ **SIFTED KEY** ⇒ at the end of transmission, ALICE and BOB will share publicly, b_k and b_k' (so can be intercepted by EVE) and then ALICE and BOB compare b_k and b_k' separately. BOB will keep valid only the meaningful measurements (ideally w/ no errors)

- sifted key length ~ ½ length of a_k on average (we waste ½ the qubits)

↳ this procedure is fundamental for security

EVE must perform the measurement in real time so the choice of b_k'' (sequence chosen by EVE) must be made before the communication between ALICE and BOB. So, it must also be random (like b_k' of BOB). But when EVE intercepts, the sifted keys of ALICE and BOB are no longer equal, but w/ a probability error of 25%.

~~e.g.~~

ALICE

sifted key: 1000 bits

↳ 100 bits are extracted (900 bits wasted)

BOB

sifted key: 1000 bits

↳ 100 bits are extracted

the 100 bits are publicly shared. If the error is close to 25%, this means that there has been an interception by EVE ⇒ the key is discarded

↳ the perturbation introduced by EVE is reflected in quite a high error in the sifted key

why 25% ?

$b_k'' = \{1, \cancel{0}, 1, \times, \dots, \}$

$b_k' = \{0, \cancel{0}, 1, \cancel{1}, \dots, \}$

$b_k = \{0, 1, 1, 0, \dots, \}$

50% of the time EVE may have chosen the correct basis

50% of the time the basis is diff., resulting in perturbation and a random output bit $\langle\, |0\rangle$ 50%, $|1\rangle$ 50%

50% → no error

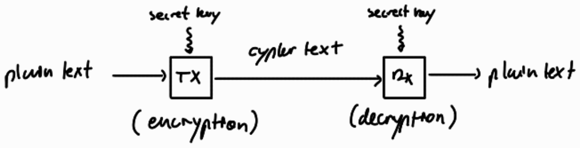
50% → error ⇒ perturbation → 50% $|0\rangle$, 50% $|1\rangle$

⇒ so overall 25% chance of error

BB84 protocol for quantum key distribution (QKD)

we have a symmetrical key that can be used for symmetrical cryptography (AES, OTP)

the only way to have theoretical security



symmetrical because both TX and RX use the same key

w/ OTP the encryption/decryption is:

key and text must have the same length => expensive in terms of updating the key

furthermore, every message must have a new key

↳ so the issue is the secure key distribution

=> QKD is unconditionally secure

against any possible attack w/ ∞ comp. resources

an alternative: RSA asymmetric cryptography (public + private key) however it is only computationally secure

security is guaranteed by the computational difficulty e.g. factorizing prime numbers

moreover, Shor's quantum algorithm for factorization of an integer into prime numbers, if implemented onto a quantum computer, is able to break RSA in a short time

there have been advances in post-quantum assymetric cryptography which is robust to Shore's algorithm (not based on factorization). However, these may also be broken in the future. On the other hand, QKD is unconditionally secure

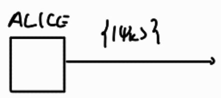
ex. 1

Z-BASIS $\{|0\rangle, |1\rangle\}$

X-BASIS $\{|+\rangle, |-\rangle\}$

mutually unbiased basis

TX:



$\{|\psi_k\rangle\} = \{|0\rangle, |+\rangle, |+\rangle, |1\rangle, |-\rangle, |1\rangle, |-\rangle, |0\rangle\}$

$\{a_k\} = \{0, 0, 0, 1, 1, 1, 1, 0\}$ $\left(\begin{matrix} 0: |0\rangle, |+\rangle \\ 1: |1\rangle, |-\rangle \end{matrix}\right)$

$\{b_k\} = \{0, 1, 1, 0, 1, 0, 1, 0\}$ $\left(\begin{matrix} 0: \text{Z-BASES} \\ 1: \text{X-BASES} \end{matrix}\right)$

random and statistically independent sequences of bits (generated w/ a quantum random num. gen.)

a_k	b_k	$\lvert\psi_k\rangle$
0	0	$\lvert 0\rangle$
0	1	$\lvert +\rangle$
1	0	$\lvert 1\rangle$
1	1	$\lvert -\rangle$

RX:

$\{|\psi_k\rangle\} \longrightarrow \boxed{\text{BOB}} \longrightarrow \{a_k'\}$

$\{b_k'\} = \{z, z, x, z, z, x, x, x\}$ random seq.

$= \{0, 0, 1, 0, 0, 1, 1, 1\}$

$\begin{pmatrix} 0 : z \\ 1 : x \end{pmatrix}$

$\{a_k'\}$ obtained by the measurement by BOB, so NOT a random seq.

then, ALICE and BOB publicly share $\{b_k\}$ and $\{b_k'\}$ to each other

$\{a_k\} = \{0, \cancel{0}, 0, 1, \cancel{1}, \cancel{1}, 1, \cancel{0}\}$

$\{b_k\} = \{0, 1, 1, 0, 1, 0, 1, 0\}$

$\{b_k'\} = \{0, 0, 1, 0, 0, 1, 1, 1\}$

$\{a_k'\} = \{0, ?, 0, 1, ?, ?, 1, ?\}$

it is fundamental that a_k, b_k are independent

$\Rightarrow$ sifted key $= \{0, 0, 0, 1\}$ this key is known to ALICE and BOB only!

In the presence of EVE:

for a given k when $b_k = b_k'$

- 50%: $b_k'' = b_k$ $\Rightarrow a_k'' = a_k$ (right bit of the sifted key is acquired w/out perturbation, and so no error in the sifted key)
- 50%: $b_k'' \neq b_k$ (completely random measurement result and perturbation)
  - 50%: $a_k'' = a_k$
  - 50%: $a_k'' \neq a_k$ so 25% prob. of error (for BOB)

note: during the transmission EVE does not know b_k and b_k', they are only shared at the end of transmission

$$\text{error prob. for BOB} = \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot \frac{1}{2} = 25\%$$

$\frac{1}{2}$ prob. — zero error — $\frac{1}{2}$ prob — $\frac{1}{2}$ error

ALICE's key:	$\{0, 0, 1, 1\}$
BOB's key:	$\{0, 1, 1, 1\}$ (25% error w.r.t. ALICE's key)
EVE's key:	$\{0, 0, 0, 1\}$ (25% error w.r.t. ALICE's key)

BB84 is a "prepare and measure" QKD. The engineering challenge is managing single photons.

preparation:

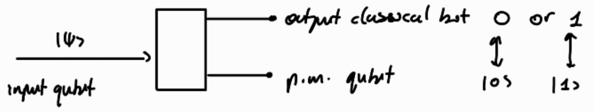
$|0\rangle \longrightarrow \boxed{\hat{X}^{a_k}} \xrightarrow{|0\rangle \text{ or } |1\rangle} \boxed{\hat{H}^{b_k}} \xrightarrow{|+\rangle \text{ or } |-\rangle \text{ or } |0\rangle \text{ or } |1\rangle}$

with inputs $\{a_k\}$ and $\{b_k\}$

$\hat{H}^{b_k}$: $\hat{H}^0 = \hat{I}$ when $b_k = 0$; $\hat{H}^1 = \hat{H}$ when $b_k = 1$

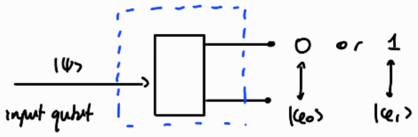
$\hat{X}^{a_k}$: $\hat{X}^0 = \hat{I}$ when $a_k = 0$; $\hat{X}^1 = \hat{X}$ when $a_k = 1$ (NOT) reception:

(Z-BASIS measurement)

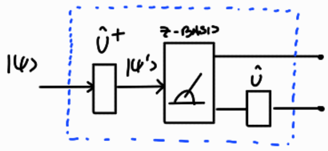


(however generally it is destructive)

in a generic basis: $\{|\varphi_0\rangle, |\varphi_1\rangle\}$



we may consider an equivalent device =>



$$P_0' = F(\psi', \varphi_0) = |\langle\psi'|\varphi_0\rangle|^2$$
$$P_1' = F(\psi', \varphi_1) = |\langle\psi'|\varphi_1\rangle|^2$$

$$\begin{cases} |0\rangle \xrightarrow{\hat{U}} |\varphi_0\rangle \\ |1\rangle \xrightarrow{\hat{U}} |\varphi_1\rangle \end{cases}$$ (there are ∞ possible choices of $\hat{U}$, where $\hat{U}$ is a unitary operator)

to have equivalence

dim.

Hp. $\begin{cases} \hat{U}|0\rangle = |\varphi_0\rangle \\ \hat{U}|1\rangle = |\varphi_1\rangle \end{cases}$; $|\psi'\rangle = \hat{U}^+|\psi\rangle$

we have to show that the fidelities are the same

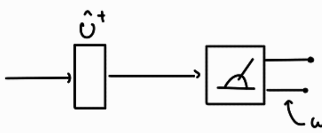
$$P_0' = F(\hat{U}^+|\psi\rangle, |0\rangle) = |\langle\psi|\hat{U}|0\rangle|^2 = |\langle\psi|\varphi_0\rangle|^2 = F(\psi, \varphi_0) = P_0$$

$[(\hat{U}^+|\psi\rangle)^+ = \langle\psi|\hat{U}]$ $[\hat{U}|0\rangle]$

and since $P_0' + P_1' = 1 \Rightarrow P_1' = 1 - P_0' = 1 - P_0 = P_1$

so : $\begin{cases} P_0' = P_0 \\ P_1' = P_1 \end{cases}$ => equivalence between the 2 devices

=>



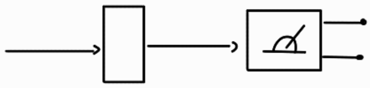
we can omit the $\hat{U}$ block if we are not interested in the p.m. state i.e. when the measurement is destructive we can apply this to measure in the X-BASIS:

$$\begin{cases} |e_0\rangle = |+\rangle \\ |e_1\rangle = |-\rangle \end{cases}$$

=> we need to map $|0\rangle \longrightarrow |+\rangle$ and $|1\rangle \longrightarrow |-\rangle$

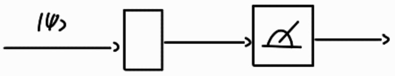
which is the Hadamard gate (other gates are possible if we consider a phase shift)

=>



$\hat{U}^\dagger = \hat{H}^\dagger = \hat{H}$

so the circuit for BOB is:



if $b_k = 0$ => $\hat{I}$ => Z-BASIS measurement

if $b_k = 0$ => $\hat{H}$ => X-BASIS measurement

$$\hat{H}^{b_k} \begin{cases} \hat{H}^0 = \hat{I} & \text{if } b_k = 0 \\ \hat{H}^1 = \hat{H} & \text{if } b_k = 1 \end{cases}$$