Lecture 1

2) Single Quantum Systems

(A) Classical information

abstraction of a device or medium that stores info

Assume we have a classical system, that can be in a finite number of distinct classical states.

↳ a configuration which can be described & recognized unambiguously.

Examples

1. A bit → states = {0, 1} (realized by any switch)

2. A dice → states = {0, 1, 2, 3, 4, 5, 6}

3. DNA nucleobase → states = {A, C, G, T}

NB → the set of states defines the classical system.

Let's introduce some notation:

- We label the system with X
- We use Σ to denote the set of states associated with X

Assumptions

→ Σ is non-empty

→ Σ is finite

↳ not strictly necessary but we keep this assumption for now.

↳ We call any finite nonempty set a "classical state set"

NB → Many different physical devices can have the same classical state set.

Sometimes we might <u>know</u> the state of X

↳ But, often our knowledge of X is uncertain!

↳ in this case we represent our knowledge of X <u>by assigning probabilities</u> to each classical state

↳ this gives us a "probabilistic state"

<u>Example</u>:

Given some past information we might know that with probability $3/4$ a bit X is in state 0, and with probability $1/4$ it is in state 1.

↳ $Pr(X=0) = 3/4 \quad Pr(X=1) = 1/4$

↳ convenient notation: $\begin{pmatrix} 3/4 \\ 1/4 \end{pmatrix} \begin{matrix} \rightarrow \text{"0"} \\ \rightarrow \text{"1"} \end{matrix}$

This is naturally generalized...

↳ any probabilistic state of a classical system can be represented by a vector of probabilities.

↳ We get to choose the ordering (Although sometimes there are conventions)

So, any probabilistic state can be represented by a column vector satisfying:

1. All entries are non-negative
2. Entries sum to 1

"probability vector"

(conversely any column vector satisfying these can be understood as a representation of a probabilistic state)

Why column vectors?

↳ Gives us a convenient way to represent operations!

Measuring probabilistic states

What do we mean by "measure"??

↳ to measure means to "look" at the system & unambiguously recognize which classical state it is in.

NB → we never "see" a system in a probabilistic state.

↳ measurement always yields one state!

Measurement changes the state of a system

Example:

Fair dice in a box   dice on the table

$$\begin{pmatrix} 1/6 \\ 1/6 \\ 1/6 \\ 1/6 \\ 1/6 \\ 1/6 \end{pmatrix} \xrightarrow{\text{"Measure"}} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

↳ open the box and look

It's helpful now to introduce some new notation...

↳ Given any system we denote the probability vector having a 1 for state a with $|a\rangle$

"ket a"

Example: A bit

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Example: A dice

$$|1\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |2\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \cdots$$

we call this basis the "standard basis"

Note: These "certain states" are a $\overbrace{\text{basis for } \mathbb{R}^{|\Sigma|}}$

↳ We can express any probabilistic vector as a linear combination of these states

Let's do another example in this notation...

↳ 1. We flip a coin & cover without looking...

$$\begin{array}{l} \text{"heads"} \\ \text{"tails"} \end{array} \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} = \tfrac{1}{2}|\text{heads}\rangle + \tfrac{1}{2}|\text{tails}\rangle$$

2. We uncover the coin and look (ie we "measure")

↳ We see either heads or tails

→ state becomes $|\text{heads}\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ or $|\text{tails}\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

3. Note: if we cover the coin again then uncover it, the classical state remains the same!

Note: • When the state of a classical system is unknown our knowledge of the system is represented by a probabilistic state.

↳ different observers can have different knowlege.

Classical operations

① Deterministic operations

↳ $\exists$ some $f : \Sigma \longmapsto \Sigma$ such that each $a \in \Sigma$ goes to $f(a)$.

Example: A bit

↳ $\exists$ only four such functions

a	$f_1(a)$
0	0
1	0

a	$f_2(a)$
0	0
1	1

NOT

a	$f_3(a)$
0	1
1	0

a	$f_4(a)$
0	1
1	1

constant (f_1) balanced (f_2, f_3) constant (f_4)

Identity: $f(a) = a$

Action of deterministic operations can be represented by matrix-vector multiplication...

↳ $\forall f : \Sigma \longmapsto \Sigma \quad \exists \; M$ st $M|a\rangle = |f(a)\rangle$

$$M_1 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad M_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad M_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad M_4 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

NB Matrices which represent deterministic functions always have entries only 1 or 0, & there is only a single 1 in each column.

→ Again we can introduce some convenient notation...

"ket a"

Recall $|a\rangle$ is the <u>column vector</u> with 1 for a.
(and zero's elsewhere)

Now $\langle a|$ is the analagous <u>row vector</u>

"bra a"

<u>Example: A bit</u>

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

Now note, for any states $a, b \in \Sigma$

$\Rightarrow$ $|b\rangle\langle a|$ is the matrix with the only non-zero entry being row b column a

$$|0\rangle\langle 1| = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

row colum

very helpful!!

standard matrix multiplication

Using this notation, for any $f : \Sigma \longmapsto \Sigma$ we can write M via

$$M = \sum_{a \in \Sigma} |f(a)\rangle\langle a| \quad \rightarrow \text{how?}$$

Well, $\langle a||b\rangle$ is the inner product.

$\Rightarrow$ $$\langle a|b\rangle = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases} = \delta_{a,b}$$

eg $\begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

convenient notation!

All together we have:

$$M|b\rangle = \left(\sum_{a\in\Sigma} |f(a)\rangle\langle a|\right)|b\rangle$$

$$= \sum_{a\in\Sigma} |f(a)\rangle\langle a|b\rangle$$

$$= \sum_{a\in\Sigma} |f(a)\rangle\,\delta_{a,b}$$

$$= |f(b)\rangle \longrightarrow \text{perfect.}$$

We have now learned "Bra" "ket" notation!

// important to be fluent moving between braket & matrix/column! //

Probabilistic operations & Stochastic Matrices

Example (A bit again)

↳ Imagine a process where:

- if $0 \longmapsto$ left alone
- if $1 \longmapsto$ bit flipped with probability ½

$$M = \begin{pmatrix} 1 & \tfrac{1}{2} \\ 0 & \tfrac{1}{2} \end{pmatrix} = |0\rangle\langle 0| + \tfrac{1}{2}|0\rangle\langle 1| + \tfrac{1}{2}|1\rangle\langle 1|$$

Check: $M|0\rangle = |0\rangle$

$M|1\rangle = \tfrac{1}{2}|0\rangle + \tfrac{1}{2}|1\rangle$

NB (Do this braket & matrix/column)

M is a stochastic matrix

↳ all entries are non-negative real numbers

→ Entries in every column sum to 1

Can represent all probabilistic operations.

Probabilistic operations are those in which randomness is used or introduced...

Note: each column can be viewed as the output probabilistic state corresponding to a specific input state

$$M = \begin{array}{ccc} 0 & 1 & \\ \left(\begin{matrix} 1 \\ 0 \end{matrix}\right. & \left.\begin{matrix} 1/2 \\ 1/2 \end{matrix}\right) & \begin{matrix} 0 \\ 1 \end{matrix} \end{array}$$

$|0\rangle \longmapsto |0\rangle$

$|1\rangle \longmapsto \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle$

Note: Stochastic matrices are precisely the matrices which map probability vectors to probability vectors! ("if and only if")

Note

↳ We can view probabilistic operations as random choices of deterministic operations:

$$\begin{pmatrix} 1 & 1/2 \\ 0 & 1/2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

→ always possible!

Composition of probabilistic operations

Imagine X, with state set Σ, probabilistic operations $M_1, M_2, \ldots, M_n$ and initial state u,

2, Applying M_i then M_j we get

$$M_j(M_i u) = \underbrace{M_j M_i}_{\text{matrix multiplication}} u$$

preserves "stochasticity"

More generally applying M_1, then M_2, ..., then M_n is represented by the matrix product

$$M_n M_{n-1} \ldots M_2 M_1$$

NB: order matters! Matrix multiplication is not commutative

$$AB = BA \;!$$

(B) Quantum Information

↳ we continue with finite non-empty systems

↳ Classical state ⟼ Quantum State

" probability vector ⟼ " quantum state vector

Quantum state vectors

("First postulate of QM")

As before, indices label classical states of the system, but

- Entries of a quantum state vector are complex
- Sum of absolute values squared = 1

Recall for a classical state vector

- entries are non-negative real numbers
- entries sum to 1

These are the only differences!

Given a vector $v = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$

Euclidian norm $\|v\| = \sqrt{\sum_{k=1}^{n} \underbrace{|\alpha_k|^2}_{\alpha_k \overline{\alpha_k}}}$

$$\therefore \sum_{k=1}^{n} |\alpha_k|^2 = 1 \iff \|v\| = 1$$

<u>Crux</u>: Quantum state vectors are unit vectors with respect to the Euclidian norm.

examples

Example: A qubit ("quantum bit")

- $\Sigma = \{0, 1\}$ just like a bit
- But different states are possible

standard basis vectors are valid quantum states!

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$\left|1/\sqrt{2}\right|^2 + \left|1/\sqrt{2}\right|^2 = 1$

$$\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\begin{pmatrix} \frac{1+2i}{3} \\ -2/3 \end{pmatrix} = \frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle$$

$$\left(\frac{1+2i}{3}\right)\left(\frac{1-2i}{3}\right) + 4/9 = 5/9 + 4/9 = 1$$

quantum state vectors are $\underbrace{\text{complex linear combinations}}_{\text{"superposition"}}$ of standard basis vectors.

Sometimes we want to give a quantum state vector a name, to do this we normally write

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

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

There are also some states which are very useful to get their own names

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

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

<u>Note</u>: Let $\Sigma = \{a_1, \ldots, a_n\}$

& $\forall\ |\psi\rangle$ we have that $\langle a_i|\psi\rangle = a_i$

<u>Example</u>: $\Sigma = \{0, 1\}$

Do this matrix/column & braket!

$$|\psi\rangle = \frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle = \begin{pmatrix} \frac{1+2i}{3} \\ -2/3 \end{pmatrix}$$

$$\langle 0|\psi\rangle = \frac{1+2i}{3} \qquad \langle 1|\psi\rangle = -2/3$$

Important:

↳ for a classical state vector $|v\rangle = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$

we had $\langle v| = (v_1 \;\; v_2)$

↳ is the transpose

↳ for a quantum state vector $|\psi\rangle$, the bra $\langle\psi|$ is the conjugate transpose of $|\psi\rangle$

Eg: $|\psi\rangle = \frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle = \begin{pmatrix} \frac{1+2i}{3} \\ -2/3 \end{pmatrix}$

$$\langle\psi| = \frac{1-2i}{3}\langle 0| - \frac{2}{3}\langle 1| = \left(\frac{1-2i}{3} \;\; -\frac{2}{3} \right)$$

So far we have looked at quantum states of a bit $\rightarrow$ ie qubit states

But we can have quantum states of any classical state set Σ

Example: quantum states of a dice

$$\Sigma = \{1, 2, 3, 4, 5, 6\}$$

$$|\psi\rangle = \begin{pmatrix} 1/2 \\ 0 \\ 0 \\ -i/2 \\ 1/\sqrt{2} \\ 0 \end{pmatrix}$$

complex!

In general $|\psi\rangle = \sum_{a \in \Sigma} \psi_a |a\rangle$

$$\underbrace{\langle\psi|\psi\rangle = \sum_a |\psi_a|^2 = 1}_{\text{quantum normalization}}$$

!

There is one type of quantum state we will encounter often...

uniform superposition

$$|\psi\rangle = \frac{1}{\sqrt{|\Sigma|}} \sum_{a \in \Sigma} |a\rangle$$

$$\psi_a = \frac{1}{\sqrt{|\Sigma|}} \text{ for all } a \in \Sigma$$

Note: Braket notation allows us to not specify ordering of indices

much more convenient

$$\underbrace{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}_{\text{much more convenient}} = \underbrace{\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \text{ or } \begin{pmatrix}\beta\\ \alpha\end{pmatrix}}_{\text{we have to specify}}$$

Just remember: $\langle a|b\rangle = \delta_{ab}$

Measuring quantum states

↳ For now we focus on one simple type of measurement

↳ "standard basis measurement"

→ When a measurement is made the observer will see a classical state

↳ Measurements are how we extract information from quantum states!

So, given $|\psi\rangle = \sum_{a \in \Sigma} \psi_a |a\rangle$ → $\psi_a = \langle a|\psi\rangle$

↳ $\sum_a |\psi_a|^2 = 1$

↳ a measurement will yield $|a\rangle$ with probability $|\psi_a|^2$!

Example

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

$$\Big\downarrow \text{Measure}$$

$$\Pr(\text{outcome} = 0) = |\langle 0|+\rangle|^2 = 1/2$$

$$\Pr(\text{outcome} = 1) = |\langle 1|+\rangle|^2 = 1/2$$

Note: We have the same probabilities for $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

↳ We cannot tell apart $|+\rangle$ & $|-\rangle$ using standard basis measurements!

Note: measuring any standard basis state $|a\rangle$ yields $|a\rangle$ with certainty

Why do we need quantum state vectors??

↳ Given $|\psi\rangle = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_n \end{pmatrix}$ why not just use the purely classical state $v = \begin{pmatrix} |\psi_1|^2 \\ \vdots \\ |\psi_n|^2 \end{pmatrix}$

valid classical state vector! ⟷

Answer: The set of allowed operations is different!

↳ Classical operations:

$$\text{classical state} \xmapsto{\text{stochastic matrix}} \text{classical state}$$

→ Quantum operations

$$\text{quantum state} \xmapsto[\text{unitary matrix}]{} \text{quantum state}$$

// unitary matrix //

What are the properties of unitary matrices?

- A square matrix is unitary if

$$UU^\dagger = \mathbb{1} \leftarrow \text{identity matrix}$$

$$\underbrace{U^\dagger}_{\text{conjugate transpose}} U = \mathbb{1}$$

$$U^\dagger = \overline{U^T}$$

↳ implies $U^{-1} = U^\dagger$

Note: Unitary matrices preserve euclidian norm

↳ $\underbrace{\| U|\psi\rangle \| = \| |\psi\rangle \| \quad \forall \ |\psi\rangle}_{\text{necessary \& sufficient!}}$

↳ Therefore unitary matrices take quantum states to quantum states!

(They are exactly the set of linear maps with this property)

Now, we have some important unitary operations!

① Pauli Operations

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \underset{\underset{X}{\parallel}}{\sigma_x} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \underset{\underset{Y}{\parallel}}{\sigma_y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \underset{\underset{Z}{\parallel}}{\sigma_z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

<u>Note</u>: X is sometimes called NOT

$\hookrightarrow X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle$

Z is called <u>phase flip</u>

$Z|0\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle$

② Hadamard

$$H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$

③ Phase operations

$$P_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

$\to S = P_{\pi/2} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

$T = P_{\pi/4} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix}$

$\to \mathbb{1} = P_0 \quad \& \quad Z = P_\pi$

Lets explore the Hadamard gate more carefully..

$$H^\dagger H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}^\dagger \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$

$H^\dagger = H$

$$= \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$

$$= \begin{pmatrix} 1/2 + 1/2 & 1/2 - 1/2 \\ 1/2 - 1/2 & 1/2 + 1/2 \end{pmatrix} = 1$$

Also, one can check

$$\left.\begin{aligned} H|0\rangle &= |+\rangle \\ H|1\rangle &= |-\rangle \\ \\ H|+\rangle &= |0\rangle \\ H|-\rangle &= |1\rangle \end{aligned}\right\}$$

we can use this to say something interesting!

Imagine we have a qubit prepared either in $|+\rangle$ or $|-\rangle$

↳ remember that measuring both of these states in the standard basis gives $Pr(\text{outcome} = 0) = Pr(\text{outcome} = 1) = 1/2$

↳ we can't tell them apart!
(we get no useful information)

But, if we apply a Hadamard then measure we can tell them apart!

$$H|+\rangle = |0\rangle \xrightarrow{\text{measure}} |0\rangle \text{ with } Pr\ 1$$

$$H|-\rangle = |1\rangle \xrightarrow{\text{measure}} |1\rangle \text{ with } Pr\ 1$$

$\therefore$ $|+\rangle$ & $|-\rangle$ can be perfectly discriminated

↳ changing phases can be significant!

(29)

$$T|+\rangle = T\left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right)$$

$$= \tfrac{1}{\sqrt{2}}T|0\rangle + \tfrac{1}{\sqrt{2}}T|1\rangle$$

$$= \tfrac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{2}|1\rangle$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix}\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

Note, knowing the action on basis states is sufficient (because of linearity!)

2, $H\left(\tfrac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{2}|1\rangle\right)$ $\quad \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}\begin{pmatrix} 1/\sqrt{2} \\ \frac{1+i}{2} \end{pmatrix}$

$$= \tfrac{1}{\sqrt{2}}H|0\rangle + \frac{1+i}{2}H|1\rangle$$

$$= \tfrac{1}{\sqrt{2}}|+\rangle + \frac{1+i}{2}|-\rangle$$

$$= \left(\tfrac{1}{2}|0\rangle + \tfrac{1}{2}|1\rangle\right) + \left(\frac{1+i}{2\sqrt{2}}|0\rangle - \frac{1+i}{2\sqrt{2}}|1\rangle\right)$$

$$= \left(\tfrac{1}{2} + \frac{1+i}{2\sqrt{2}}\right)|0\rangle + \left(\tfrac{1}{2} - \frac{1+i}{2\sqrt{2}}\right)|1\rangle$$

We can use either method!

Compositions of unitary operations

↳ Matrix multiplication as before!

Example: $R = HSH = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$

↳ note $R^2 = \overset{\text{NOT}}{\overset{\shortparallel}{X}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

↳ R = square root of X

↳ This is not possible classically!