Review of quizz

Probability

X, Y independent random variables taking value 0, 1

we know $P[X=0, Y=0] = 0.1$, $P[X=0, Y=1] = 0.3$

what can we say about $P[X=1, Y=*]$?

X and Y <u>indenpendent</u> : no correlation between their values ; $P[X=a, Y=b] = P[X=a]\,P[Y=b]$

in our setting : $P[X=0, Y=0] = 0.1$, $P[X=0, Y=1] = 0.3$

$\Rightarrow$ $P[Y=1]$ is 3 x more likely than $P[Y=0]$

so $P[X=1, Y=1] = 3\,P[X=1, Y=0]$

we also have $\displaystyle\sum_{\substack{a=0,1\\ b=0,1}} P[X=a, Y=b] = 1$

cont.) then $P[X=1, Y=1] = 0.45$, $P[X=1, Y=0] = 0.15$

linear algebra

A, B square matrix of size 3, $\operatorname{rk} A = 1 = \operatorname{rk} B$

what can we say about $A+B$?

$\operatorname{rk} A = 1$ means:

- $XAY = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ for some invertible matrices X, Y
- the set of vectors of the form $A\begin{bmatrix} x \\ y \\ z \end{bmatrix}$ has

dimension 1 — maximal # of linearly independent vectors

i.e. $\exists\, x_0, y_0, z_0 \;\forall\, x, y, z \;\exists\, s \quad A\begin{bmatrix} x \\ y \\ z \end{bmatrix} = s\begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix}$

$\begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix}$: first column of X^{-1}

cont.) similarly

$\mathrm{rk}\, B = 1 \Rightarrow \exists\, x_1, y_1, z_1 \quad \forall\, x, y, z \ \exists t \quad B\begin{bmatrix} x \\ y \\ z \end{bmatrix} = t\begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix}$

so $\quad (A+B)\begin{bmatrix} x \\ y \\ z \end{bmatrix} = s\begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix} + t\begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix}$

we can say: the set of vectors of the form $(A+B)\begin{bmatrix} x \\ y \\ z \end{bmatrix}$

is spanned by $\begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix}$ and $\begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix}$

$\begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix}$ and $\begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix}$ linearly independent $\Rightarrow$ dimension 2

$\Rightarrow \mathrm{rk}(A+B) = 2$

they are not lin. indep. i.e. $\begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix} = r\begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix}$

$A+B \neq 0 \Rightarrow$ dim. $1 \Rightarrow \mathrm{rk}(A+B) = 1$

$A+B = 0 \Rightarrow$ dim. $0 \Rightarrow \mathrm{rk}(A+B) = 0$

Basic setup of quantum mechanics

(Lecture 3 in main ref.)

paradigm: a state of a "discrete" quantum mechanical system is represented by a <u>unit</u> <u>vector</u> in $\mathbb{C}^N$ for some N

unit vector: $\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_N \end{bmatrix} \in \mathbb{C}^N$ such that $\sum_{i=1}^{N} \underbrace{|\alpha_i|^2}_{} = 1$

more abstract version: consider <u>Hilbert</u> <u>spaces</u> instead of $\mathbb{C}^N$ e.g. $L^2(\mathbb{R}, dx)$, $L^2(\mathbb{R}^d, dx) \otimes \mathbb{C}^N$, ...

that allow functions in continuous variables $f(x)$, ...

and operations like $f(x) \mapsto f'(x)$, ...

(but require <u>functional</u> <u>analysis</u> to handle difficulties in ∞-dimensional spaces) in this course, we stick to finite dimensional case

so $\mathbb{C}^N$ is enough. but

$\underline{\mathbb{C}^N \otimes \mathbb{C}^N \otimes \cdots \otimes \mathbb{C}^N}$ $(\simeq \mathbb{C}^{N^k})$ tensor product space

$\underline{M_d(\mathbb{C})}$ $(\simeq \mathbb{C}^{d^2})$ matrix space

are sensible candidates for state spaces

simplest nontrivial example : $N=2$ qubit space $\mathbb{C}^2$

$\rightsquigarrow$ generic elements $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ $\alpha, \beta \in \mathbb{C}$

unit vectors $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ with $|\alpha|^2 + |\beta|^2 = 1$

α, β : amplitudes for two possibilities "0", "1"

$|\alpha|^2, |\beta|^2$: probabilities

Notation (bra - ket)

$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \in \mathbb{C}^2$

generic vector (in $\mathbb{C}^2$) $|\psi\rangle$, $|\varphi\rangle$, ... <u>ket</u> vectors

for $|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, write $\langle 0|\psi\rangle = \alpha$, $\langle 1|\psi\rangle = \beta$

for $|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, $|\varphi\rangle = \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix}$, write $\langle \psi|\varphi\rangle = \alpha^* \alpha' + \beta^* \beta'$

<u>Hermitian inner product</u> of $\mathbb{C}^2$

$\langle\psi| = \alpha^* \langle 0| + \beta^* \langle 1|$ <u>bra</u> functional ;

"take inner prod. with $|\psi\rangle$"

! $|0\rangle \neq 0$ ← origin of vector space

↑ index of basis

$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \end{bmatrix}$

When is the bra-ket notation useful?

we can write $|00\rangle = |0\rangle \otimes |0\rangle$, $|01\rangle = |0\rangle \otimes |1\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$

for tensor product

tensor product space $\cong \mathbb{C}^4$

when T is a transform, $\langle \psi | T | \varphi \rangle$ to represent

"apply T to φ, then take inner product with $|\psi\rangle$"

Some important unit vectors

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$

<u>Hadamard basis</u>

$|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix}$, $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{i}{\sqrt{2}} \end{bmatrix}$,

Norm of $|\psi\rangle$: $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$ (2-norm) $\mathbb{C}^N \simeq \mathbb{R}^{2N}$

$\|\psi\| = 0 \Leftrightarrow |\psi\rangle = 0$, $\|\varphi + \psi\| \leq \|\varphi\| + \|\psi\|$ $\|\psi\| \leftrightarrow$ Euclidean norm $\sqrt{x_1^2 + \cdots + x_{2N}^2}$

unit vector : $\|\psi\| = 1$

Transformation of quantum states

want : scheme to transform unit vectors to unit vectors

Proposition : suppose U is a 2×2 complex matrix

if $U\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$ is a unit vector whenever $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$ is a unit vec.

then U is unitary: $U^\dagger = U^{-1} \Leftrightarrow U^\dagger U = I_2 \Leftrightarrow UU^\dagger = I_2$

$$U = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \rightsquigarrow U^\dagger = \begin{bmatrix} x^* & z^* \\ y^* & w^* \end{bmatrix}$$

another convention $U^* = \begin{bmatrix} \bar{x} & \bar{z} \\ \bar{y} & \bar{w} \end{bmatrix}$

Outline of the proof

point 1 : $\dagger$ makes sense for vectors : $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}^\dagger = [\alpha^* \ \beta^*]$

$\rightsquigarrow$ $|\psi\rangle^\dagger = \langle\psi|$; $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}^\dagger \begin{bmatrix}\alpha'\\ \beta'\end{bmatrix} = \alpha^*\alpha' + \beta^*\beta'$; $(U|\psi\rangle)^\dagger = \langle\psi| U^\dagger$

point 2 : the transform $|\psi\rangle \rightsquigarrow |\varphi\rangle = U|\psi\rangle$ sends unit vectors to unit vectors $\Longleftrightarrow$ $\langle\psi|\psi\rangle = \langle\varphi|\varphi\rangle$ in general

$\Rightarrow$ we want $\langle\psi| U^\dagger U |\psi\rangle = \langle\psi|\psi\rangle$ for any $|\psi\rangle$

$\Rightarrow$ $U^\dagger U = I_2$ $\square$

Remark this holds for square matrices of arbitrary size : $\left\| U \begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_N\end{bmatrix} \right\| = \left\| \begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_N\end{bmatrix} \right\|$ for all $\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_N\end{bmatrix} \in \mathbb{C}^N$

$\Longleftrightarrow$ $U^\dagger = U^{-1}$

Examples

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad NOT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \underset{\text{"phase shift"}}{\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}}, \quad \underset{\text{"rotation"}}{\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}}$$

So $NOT|0\rangle = |1\rangle$, $NOT|1\rangle = |0\rangle$, etc.

Remark : $|\psi_1\rangle, |\psi_2\rangle$ orthonormal basis of $\mathbb{C}^2$

$$\langle \psi_i | \psi_j \rangle = \begin{cases} 1 & (i=j) \\ 0 & (i \neq j) \end{cases}$$

$|\varphi_1\rangle, |\varphi_2\rangle$ another orthonormal basis

$\Rightarrow$ $\exists!$ unitary matrix U s.t. $U|\psi_1\rangle = |\varphi_1\rangle$, $U|\psi_2\rangle = |\varphi_2\rangle$

$$U = \underbrace{|\varphi_1\rangle\langle\psi_1|}_{|\xi\rangle \mapsto \langle\psi_1|\xi\rangle\,|\varphi_1\rangle} + \underbrace{|\varphi_2\rangle\langle\psi_2|}_{\text{same with } |\psi_2\rangle,\, |\varphi_2\rangle} = |\varphi_1\rangle\left(|\psi_1\rangle\right)^\dagger + |\varphi_2\rangle\left(|\psi_2\rangle\right)^\dagger$$

Quantum interference

let U be the 2×2 unitary matrix s.t.

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

so U creates a "random state" $|+\rangle$ from

↳ outcome 0 with prob. $\frac{1}{2}$

1 with prob. $\frac{1}{2}$

a "determinate" state $|0\rangle$

↳ outcome 0 with prob. 1

1 with prob. 0

what happens when we do this twice?

apply $U^2 = UU$

we have $U = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$ from $U\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$, etc.

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

determines first column of U

cont.) so $U^2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \Rightarrow U^2|0\rangle = |0\rangle,\ U^2|1\rangle = -|1\rangle$

$\rightsquigarrow$ we get a deterministic answer for U^2 !

in classical probabilistic setting :

no (probabilistic state) $\rightsquigarrow$ (deterministic state)

$$\underset{\substack{\text{stoch.}\\\text{mat.}}}{M}\ \underset{\begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}}{(\text{deterministic state})} = (\text{deterministic state})\ \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$$

$\Rightarrow$ M : permutation matrix

M_1, M_2 : stoch. mat which is not a perm. mat.

$\Rightarrow$ $M_1 M_2$ not permutation mat.

Phase

complex num. of unit modulus $|z| = 1$

$|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ is physically indistinguishable:

$$|\psi\rangle = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_N \end{bmatrix} \rightsquigarrow e^{i\theta}|\psi\rangle \text{ has amplitudes } e^{i\theta}\alpha_1, \dots, e^{i\theta}\alpha_N$$

$$\rightsquigarrow \text{probabilities } |e^{i\theta}\alpha_1|^2 = |\alpha_1|^2, \dots, |e^{i\theta}\alpha_N|^2 = |\alpha_N|^2$$

but $|\varphi\rangle + e^{i\theta}|\psi\rangle$ can be distinguishable from

$|\varphi\rangle + |\psi\rangle$

i.e. $\begin{bmatrix} \alpha_1' + e^{i\theta}\alpha_1 \\ \vdots \\ \alpha_N' + e^{i\theta}\alpha_N \end{bmatrix}$ lead to different prob. than $\begin{bmatrix} \alpha_1' + \alpha_1 \\ \vdots \\ \alpha_N' + \alpha_N \end{bmatrix}$