Notas básicas de Cómputo Cuántico

En el cómputo cuántico, es necesario conocer varios conceptos básicos a partir de los cuales se construye todo la herramienta matemática a utilizar. Es importante que todos estos conceptos queden claros.

- 1.- Algebra lineal [Necesaria para entender]

- Vectores

En cuántica para dimensión finita, un estado cuántico es representado por un vector complejo. Se visualiza con kets ($|\psi\rangle$). Un qubit es un estado cuántico $|\psi\rangle$ de base 2, tal que

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad \alpha, \beta \in \mathbb{C} \quad y \quad |\alpha|^2 + |\beta|^2 = 1$$

El espacio vectorial se le conoce como Espacio de Hilbert ($\mathcal{H}_2$)

Recordatorio
Una función lineal es una función que cumple lo sig:
$f(\bar{x} + \bar{y}) = f(\bar{x}) + f(\bar{y})$
$f(\alpha \bar{x}) = \alpha f(\bar{x})$
y se representan con matrices

- Producto interno

Sean $|v\rangle$ y $|w\rangle$ 2 vectores, el producto interno de 2 vectores en el espacio de Hilbert se define como

Braket

$$\boxed{\langle v|w\rangle = \sum_i v_i^* w_i}$$

- Propiedades:
  - $\langle\psi|(a|\phi_1\rangle + b|\phi_2\rangle) = a\langle\psi|\phi_1\rangle + b\langle\psi|\phi_2\rangle$ linealidad del 2do argumento
  - $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$ Hermiticidad

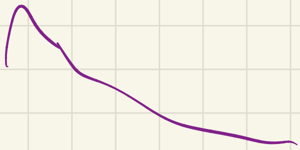
Se dice que 2 vectores son ortogonales si su producto interno es 0

- Norma

El producto interno induce una Norma, de modo que $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$.

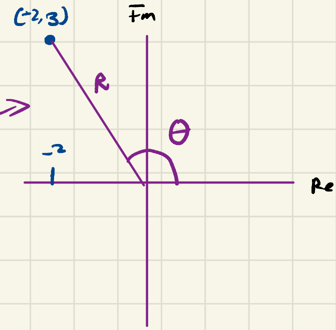
Es importante entender que en la cuántica, TODOS los estados tienen norma 1 (mas adelante veremos por que)

$e^{i\theta} = \operatorname{sen}\theta + i\cos\theta$



(a, b)

$\underset{\mathbb{R}}{a} + \underset{img}{b}i \rightarrow$



(r, θ)

$re^{i\theta}$

$r = \sqrt{(-2)^2 + (3)^2} \qquad \theta = \arctan\left(\frac{y}{x}\right)$

0 1

$\mathbb{C}^2$

$\begin{pmatrix}\alpha \\ \beta\end{pmatrix}$ α y $\beta \in \mathbb{C}$

$\boxed{|\alpha|^2 + |\beta|^2 = 1}$

probabilidades

ket = vector

$|\psi\rangle$

$\boxed{|0\rangle}$ $\boxed{|1\rangle}$

$|\psi\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$

$|\alpha|^2 =$ prob de medir $|0\rangle$

$|\beta|^2 =$ prob de medir $|1\rangle$

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

$\boxed{\begin{pmatrix}\alpha \\ \beta\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle}$

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

$\rightarrow |-\rangle$

Computacional

$|0\rangle \quad |1\rangle$

Diagonal

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

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

$|+\rangle$

$\boxed{\text{Protocolo BB84}}$

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

$$\underbrace{\langle 1|}_{\text{Bra}}\underbrace{\psi\rangle}_{\text{ket}} = \langle 1|\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\boxed{\underbrace{\langle 1|0\rangle}_{¿?}} + \frac{1}{\sqrt{2}}\boxed{\underbrace{\langle 1|1\rangle}_{¿?}}$$

$$= \frac{1}{\sqrt{2}}\cdot 0 + \frac{1}{\sqrt{2}}\cdot 1$$

$$= \frac{1}{\sqrt{2}}$$

$$|\psi\rangle = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{pmatrix}$$

Diagonal

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

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

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

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

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

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

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

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

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

$$\langle\psi| = \alpha^*\langle 0| + \beta^*\langle 1| = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}$$

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

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

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

$$= \frac{1}{2}\overset{1}{\langle 0|0\rangle} - \frac{1}{2}\overset{0}{\langle 0|1\rangle} + \frac{1}{2}\overset{0}{\langle 1|0\rangle} - \frac{1}{2}\overset{1}{\langle 1|1\rangle} = \frac{1}{2} - \frac{1}{2} = 0$$

- Independencia lineal y bases ortonormales

Una combinación lineal es una expresión matemática que nos permite construir vectores a partir de otros vectores y escalares

Ej; $|\psi\rangle = \alpha|e_1\rangle + \beta|e_2\rangle$ [el vector $|\psi\rangle$ se construye como combinación de $|e_1\rangle$ y $|e_2\rangle$

Una base es un conjunto de vectores linealmente independientes que generan al espacio vectorial (es decir, que todos los elementos del espacio vectorial se pueden ver como combinación lineal de la base

Una base ortonormal es una base cuyos vectores tienen norma 1 y son ortogonales.

En cómputo cuántico, existen varias bases ortonormales con las cuales representamos los estados de un qubit. Las 2 principales son

- Base computacional

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ y } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Rightarrow \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

El estado $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ se puede ver como $\alpha|0\rangle + \beta|1\rangle$

- Base diagonal

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ y } |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

- 1-formas

Una 1-forma es una función lineal que asocia a los vectores un elemento del campo (en este caso, un complejo). Se representan por un vector fila. El espacio de vectores es isomorfo al espacio de 1-formas y se representan con Bras ($\langle\psi|$) de modo que

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \Rightarrow \langle\psi| = (\alpha^* \ \ \beta^*)$$

Entonces si un ket se representa con un vector columna, un Bra usa un vector fila. Esta elegante representación permite visualizar los productos internos como Bra-kets

$$\Rightarrow \underbrace{\langle\phi|}_{\text{Bra}}\underbrace{\psi\rangle}_{\text{ket}}$$

Los Bras son Funciones lineales, de modo que

$$\langle x|(c_1|y_1\rangle + c_2|y_2\rangle) = c_1\langle x|y_1\rangle + c_2\langle x|y_2\rangle$$

- Producto externo

La magia de la notación Bra-ket o notación de Dirac es que podemos construir multiples objetos matemáticos con ellos de forma elegante
Podemos tratar a los kets y bras como herramientas para construir otros objetos en el espacio de Hilbert. Un ejemplo es el producto externo

Sean $|\phi\rangle$ $|\psi\rangle$ 2 elementos del espacio de Hilbert, su producto externo se visualiza:

$$\underbrace{|\phi\rangle}_{\text{ket}}\underbrace{\langle\psi|}_{\text{bra}}$$

y opera de la sig forma

$$(|\phi_1\rangle\langle\phi_2|)|\psi\rangle = |\phi_1\rangle\langle\phi_2|\psi\rangle = \langle\phi_2|\psi\rangle|\phi_1\rangle$$

Si $\{|e_i\rangle\}$ es una base ortonormal

$$\Rightarrow \quad \sum_i |e_i\rangle\langle e_i| = I \quad \Rightarrow$$

- Operador lineal

$A: \mathbb{C}^n \to \mathbb{C}^n$ es un operador lineal si cumple

$$A(c_1|x\rangle + c_2|y\rangle) = c_1 A|x\rangle + c_2 A|y\rangle$$

Los operadores se pueden representar como matrices sobre una base ortonormal con entradas A_{ij}

$$\Rightarrow \quad A_{ij} = \langle e_i|A|e_j\rangle$$

En computación cuántica, sirve para ver la evolución de los estados y su comportamiento

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\Rightarrow |\psi'\rangle = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

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

$$\left(|1\rangle\langle 0| + |0\rangle\langle 1|\right)\left(|\psi\rangle\right)$$

$$= |1\rangle\underbrace{\langle 0|\psi\rangle}_{\alpha} + |0\rangle\underbrace{\langle 1|\psi\rangle}_{\beta}$$

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

$$= \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

$$\left(|+\rangle\langle 0|\right)\left(|\psi\rangle\right)$$

$$= |+\rangle\underbrace{\langle 0|\psi\rangle}_{\alpha}$$

$$= \alpha|+\rangle$$

$$|+\rangle\langle 0|\left(\alpha \overset{|+\rangle}{|0\rangle} + \cancel{\beta|1\rangle}\right) = \boxed{\alpha|+\rangle}$$

$$|0\rangle\langle 1| + |+\rangle\langle 0|\left(\alpha|0\rangle + \beta|1\rangle\right)$$

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

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

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

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

• Conjugado Hermitiano

Sea A un operador lineal, su conjugado Hermitiano $A^\dagger$ es el operador que cumple

$$A_{u,v} = A^{\dagger *}_{v,u}$$

$$\langle u|A|v\rangle = \langle v|A^\dagger|u\rangle^*$$

Valor esperado $\boxed{\langle\psi|A|\psi\rangle}$ Real

$$A = A^\dagger$$

$$\begin{pmatrix} 1 & i \\ -i & 0 \end{pmatrix}$$

dados $|u\rangle$ y $|v\rangle$ arbitrarios

Si $A = A^\dagger \Rightarrow A$ es hermitiana.

Propiedades:

$(A+B)^\dagger = A^\dagger + B^\dagger$ $\quad (AB)^\dagger = B^\dagger A^\dagger$ $\quad (cA)^\dagger = c^* A^\dagger$ $\quad |v\rangle^\dagger = \langle v|$ $\quad (A^\dagger)^\dagger = A$

La matriz del operador $A^\dagger$ es la matriz traspuesta conjugada de A

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow A^\dagger = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}$$

• Matrices especiales

Hermitiano:

$$A = A^\dagger$$

Unitaria:

$$\boxed{A^\dagger = A^{-1}} \qquad A \cdot A^{-1} = I_d$$

• Una matriz unitaria conserva la norma de cualquier vector

$$\| |\psi\rangle \| = \| A|\psi\rangle \|$$

Matrices de Paulli

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

$X|0\rangle = |1\rangle \quad Y|0\rangle = i|1\rangle \quad Z|+\rangle = |-\rangle$

$X|1\rangle = |0\rangle \quad Y|1\rangle = -i|0\rangle \quad Z|-\rangle = |+\rangle$

$X|+\rangle \quad Y|+\rangle \quad Z|0\rangle \quad$ Tarea

$X|-\rangle \quad Y|-\rangle \quad Z|1\rangle$

- Producto Tensorial

2 qubit

$|\psi\rangle = a|0\rangle + b|1\rangle$

$|\phi\rangle = c|0\rangle + d|1\rangle$

$$\underset{m\times n}{A} \otimes \underset{p\times q}{B} = \begin{pmatrix} a_{11}B & a_{12}B & \cdots \\ a_{21}B & a_{22}B & \cdots \\ \vdots & & \end{pmatrix}$$

$|\psi\rangle \otimes |\phi\rangle$

$$= \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix}$$

$$= \begin{pmatrix} a\begin{pmatrix} c \\ d \end{pmatrix} \\ b\begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

$(|a\rangle + |b\rangle) \otimes |\psi\rangle = |a\rangle \otimes |\psi\rangle + |b\rangle \otimes |\psi\rangle$

$(A \otimes B)(|\psi\rangle \otimes |\phi\rangle) = A|\psi\rangle \otimes B|\phi\rangle$

$\boxed{10}$

$$|1\rangle \otimes |0\rangle = \begin{pmatrix} 0\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1\begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \boxed{1} \\ 0 \end{pmatrix} \begin{matrix} -0 \\ -1 \\ -2 \\ -3 \end{matrix}$$

$\quad 1 \quad 0 \quad 1$

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

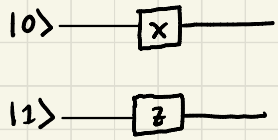
$|01\rangle = |0\rangle \otimes |1\rangle$

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

$Z|+\rangle = |-\rangle$

$(X \otimes Z)(|01\rangle) = |1\rangle \otimes -|1\rangle$

$= -|11\rangle$



Hadamard

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

$H|0\rangle = |+\rangle$

$H|1\rangle = |-\rangle$

$H|+\rangle = |0\rangle$

$H|-\rangle = |1\rangle$

1.- Explicar que hacen X, Y, Z, H, I sobre $|0\rangle\ |1\rangle\ |+\rangle\ |-\rangle$

2.- Intenten hacer un sistema de 3 qubits y apliquen X sobre el primero, Z sobre el segundo y H sobre el tercero

3.- Demuestren que X, Y, Z son Hermitianas y unitarias

$$(X \otimes Z \otimes H)|000\rangle$$

$$= X|0\rangle \otimes Z|0\rangle \otimes H|0\rangle$$

$$= \boxed{|1\rangle \otimes |0\rangle \otimes |+\rangle}$$

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

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

$$= \frac{1}{\sqrt{2}}\left(|10\rangle \otimes (|0\rangle + |1\rangle)\right)$$

$$= \frac{1}{\sqrt{2}}(|100\rangle + |101\rangle)$$

$$(|a\rangle + |b\rangle) \otimes |\psi\rangle = |a\rangle \otimes |\psi\rangle + |b\rangle \otimes |\psi\rangle$$

$$(A \otimes B)(|\psi\rangle \otimes |\phi\rangle) = A|\psi\rangle \otimes B|\phi\rangle$$

$$cA \otimes B = A \otimes cB = c(A \otimes B)$$

- Mediciones cuánticas

Las mediciones se describen por un conjunto de operadores de nombre operadores de medición $\{M_m\}$ tales que $\sum_m M_m^\dagger M_m = I$

La probabilidad de medir m es $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$

y el estado post-medición es $\dfrac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$

$(|a\rangle\langle b|)^\dagger = |b\rangle\langle a|$

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

$M_0 = |0\rangle\langle 0|$

$M_1 = |1\rangle\langle 1|$

$M_0^\dagger = |0\rangle\langle 0|$

$\langle a|b\rangle = \langle b|a\rangle^*$

$M_0^\dagger \cdot M_0 = |0\rangle\overbrace{\langle 0|0\rangle}^{1}\langle 0|$

$= |0\rangle\langle 0|$

$p_0 = \langle\psi|M_0^\dagger \cdot M_0|\psi\rangle$

$= \langle\psi|0\rangle\langle 0|\psi\rangle$

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

$= \underbrace{\langle 0|\psi\rangle}(\underbrace{\langle 0|\psi\rangle})^*$

$= \alpha \cdot \alpha^*$

$= |\alpha|^2$