Computación Cuántica

Por

Markel Álvarez Martínez

UNIVERSIDAD COMPLUTENSE
MADRID

Grado en Ingeniería Informática

Facultad de Informática

Apuntes de la asignatura Computación Cuántica

Madrid, 2022

Índice general

Tema 1

Introducción

Importante

Este documento se irá actualizando periódicamente para añadir nuevo contenido y/o corrección de erratas.

Objetivos de la asignatura:

- Familiarizarse con el lenguaje (matemático) de la Computación Cuántica (CC)
- Familiarizarse con algunos algoritmos concretos
- Correcci'on de errores (robustos)
- Modelos alternativos de computación
- "Q Cellular" autómata

1.1. Computación Cuántica

Computor: opera sobre un aparato para conseguir *output* a partir de un *input*. Los computores procesan información (una selección de un subconjunto dentro de un conjunto).

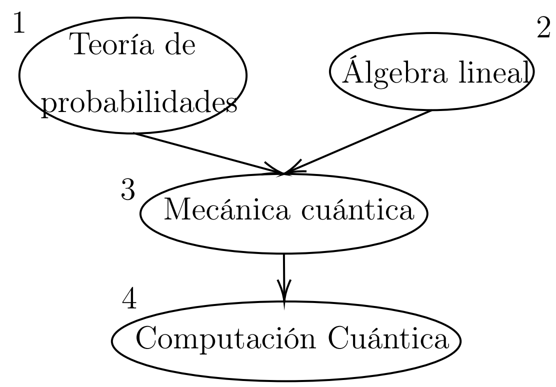
1.1.1. Principio de Landauer

La información necesita un soporte físico para su representación.

Pregunta

¿Como la naturaleza del soporte utilizado afecta a nuestra capacidad para procesar información?

¿Que pasa cuando el soporte necesita la mecánica cuántica para su descripción? ¿Limitaciones? ¿Posibilidades?



Tema 2

Probabilidad

2.1. Nociones básicas

Definición. Un experimento es un proceso que produce un *output* observable. Un experimento aleatorio es un experimento cuyo *output* no se puede predecir con certeza.

Definición. Un espacio de muestra (*sample space*), Ω, es el conjunto de todos los resultados posibles de un experimento.

Definición. Un *evento* E es un subconjunto de Ω, es decir, una colección de puntos de Ω.

Ejemplos

- Espacio aleatorio $\equiv$ tirar una moneda.
  $\Omega \equiv \{'h','t'\}$ // Cara o cruz.
  Ejemplos de eventos: $E\{'h'\}$, $E\{'t'\}$
- Espacio aleatorio $\equiv$ tirar dos monedas.
  $\Omega \equiv \{'hh','ht','tt','th'\}$
  Ejemplos de eventos: $E \equiv$ la primera moneda da $'h' \equiv \{'hh','ht'\}$

Dados dos eventos E y E' se pueden definir las siguientes operaciones:

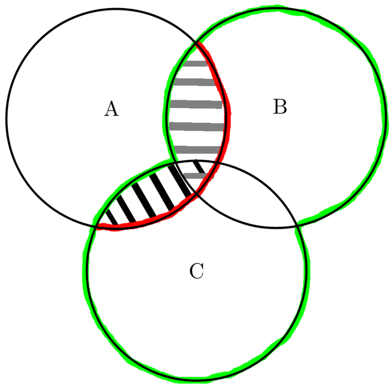
- Unión $E \cup E'$. $E \oplus E'$ ocurre durante el experimento.
- Intersección $E \cap E'$, puntos a la vez en E y E'.

- Complementario: $B^c = \frac{\Omega}{E}$

Definición. Dos eventos E y E' son mutuamente exclusivos o disyuntivos si $E \cap E' = \varnothing$

Lemma. Sean A, B, C eventos, entonces $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Pseudo-demo



$B \cup C$

$A \cap B$

$A \cap C$

> **Teorema (Leyes de De Morgan).** Sean $\{A_1, \ldots, A_n\}$ eventos
> $(\bigcup_{j=1}^n A_j)^c = \bigcap_{j=1}^n A_j^c$
> $(\bigcap_{j=1}^n A_j)^c = \bigcup_{j=1}^n A_j^c$

Es común que no nos interese todo Ω. Por ejemplo, en la medida de una longitud puede que no nos interese el resultado exacto sino un intervalo que lo contenga. En teoría de las probabilidades nos interesa más de un conjunto de eventos, F, que satisfacen:

- $\Omega \in F$
- $A_1, A_2, \ldots, A_n \in F \Rightarrow \cup_{j=1}^n A_j \in F$
- $A \in F \Rightarrow A^c \in F$

Observación. Usando las leyes de De Morgan se prueba que $\{A_j\}_{j=1}^h \subseteq F \Rightarrow \cap_{j=1}^n A_j \in F$.

Una medida de probabilidad es una función $P : F \to \mathbb{R}$ tal que

(1) $P(E) \geq 0$

(2) $P(E \cup E') = P(E) + P(E')$

$\forall E,\ E' \in F$ tal que $E \cap E' = \varnothing$

(3) $P(\Omega) = 1$

$(\Omega, F, P) \equiv$ espacio de probabilidades.

Proposición. Sean $E, E', \{A_j; j = 1, \ldots, n\}$ eventos de una G-algebra F. Entonces,

(1) $P(\varnothing) = 0$

(2) $P(E \cup E') = P(E) + P(E') - P(E \cap E')$

(3) $E \subset E' \Rightarrow P(E) \leq P(E')$

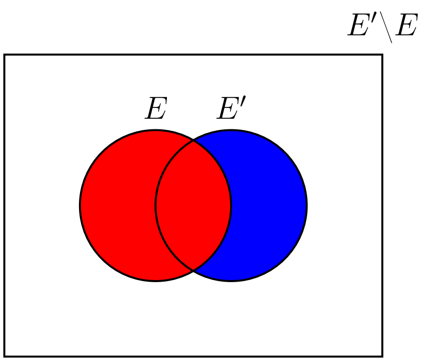
(4) $P(\bigcup_{j=1}^{n} A_j) \leq \sum_{j=1}^{n} P(A_j)$

Demostración.

(1) Consideramos E evento con probabilidad finita (ej. $E = \Omega$).

$P(E) = P(E \cup \varnothing) \underbrace{=}_{\text{axioma 2}} P(E) + P(\varnothing) \Rightarrow P(\varnothing) = 0$

(2) $E \cup E' = E \cup (E' \backslash E)$



$P(E \cup E') = P(E \cup (E' \backslash E)) \underbrace{=}_{\text{axioma 2}} P(E) + P(E' \backslash E) = P(E' \cup (E \backslash E')) = P(E') + P(E \backslash E') \Rightarrow$

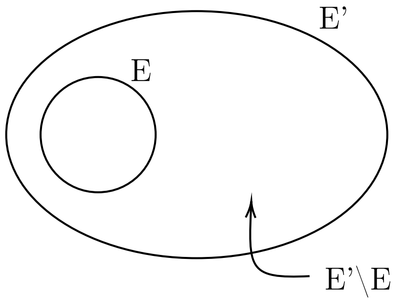
$2P(E \cup E') = P(E) + P(E') + P(E' \backslash E) + P(E \backslash E') \Leftrightarrow 2P(E \cup E') - P(E' \backslash E) - P(E \backslash E') = P(E) + P(E') \Rightarrow$

$2P(E \cup E') - \underbrace{\{P(E' \backslash E) + P(E \backslash E') + P(E \cap E')\}}_{P(E \cup E') \text{ pq } E' \backslash E, E', E \cap E' \text{ son mutuamente disjuntos}} = P(E) + P(E') - P(E \cap E') \Rightarrow$

$$\boxed{P(E \cup E') = P(E) + P(E') - P(E \cap E')}$$

Escena de unión disjunta

$$E' = E \cup (E' \backslash E) \Rightarrow P(E') \underbrace{=}_{\text{axioma } 2 \leq P(E)} P(E) + \underbrace{P(E' \backslash E)}_{\leq 0 \text{ (axioma 1)}}$$



Para asociar un número concreto a un evento hay dos maneras:

- Bayesiana
- Frecuentista

Dadas n repeticiones de un experimento aleatorio, sea $\mathcal{V}(E)$[1] $\equiv P(E) = \lim_{n\to\infty} \dfrac{\mathcal{V}(E)}{n}$

2.2. Probabilidad

Definición. Dos eventos E y E' son independientes si $P(E \cap E') = P(E)P(E')$.

2.2.1. Probabilidad condicional

$P(A|B)$ de A condicionado a B se define como P(A|B)$\begin{cases} \frac{P(A\cap B)}{P(B)} \text{ si } P(B) \neq 0 \\ 0 \text{ si no} \end{cases}$. Se verifica formalmente que $0 \leq P(A|B) \leq 1$.

Idea. $P(A)$ mide la incertidumbre sobre ocurrencia de A. $H(P_A) = -P_A * \ln P_A - (1 - P_A)\ln(1 - P_A)$ (Shennon).

> **Ejemplo.**
>
> Lanza un dado equilibrado.
>
> $P('1') = \frac{1}{6}$
>
> $P('1'|\text{hace sol}) = \frac{1}{6}$, información adicional inútil

[1] $\mathcal{V}(E)$: ocurrencias del evento E.

$P('1'|\text{resultado impar}) = \frac{1}{3}$, información adicional útil

$P('1'|\text{resultado par}) = 0$

¿Por qué $P(A|B) \underbrace{=}_{def.} \dfrac{P(A\cap B)}{P(B)}$? Consideramos n repeticiones del espacio aleatorio:

- $\mathcal{V}_n(n)$: # ocurrencias del evento A
- $\mathcal{V}_n(A\cap B)$: # ocurrencias del evento $A\cap B$ (A y B ocurren a la vez).

$\prod_n(A|B) \equiv \dfrac{\frac{\mathcal{V}_n(A\cap B)}{n}}{\frac{\mathcal{V}_n(B)}{n}}$ indica en qué medida la ocurrencia de B implica la ocurrencia de A.

$\text{lím}_{n\to\infty} \prod_n(A|B) = \dfrac{P(A\cap B)}{P(B)} = P(A|B)$.

2.2.2. Teorema de Bayes

$$\left.\begin{aligned} P(A\cap B) = P(A|B) * P(B) \\ P(B\cap A) = P(B|A) * P(A) \end{aligned}\right\} P(B|A) = \frac{P(B)}{P(A)} P(A|B)$$

Teorema. ($P(A) = P(A|\Omega)$)

$$P(A|\Omega) = \underbrace{\frac{P(A\cap\Omega)}{P(\Omega)}}_{=1} = P(A)$$

Teorema.

$\forall A \in F$ tal que $P(A) \neq 0$, $P(\Omega|A) = 1$.

Demostración.

$$P(A) = P(A\cap\Omega) = \underbrace{P(\Omega|A)}_{1} P(A)$$

Teorema.

Sea $\{B_j\}_{j=1}^n$ tal que $\bigcup_{j=1}^n B_j = \Omega$, $j \neq n \Rightarrow B_j \cap B_n = \varnothing$. Entonces, $P(A) = \sum_j P(A\cap B_j) = \sum_j P(A|B_j)P(B_j) = \sum_j P(B_j|A)P(A)$ lo cual demuestra que $\sum_j P(B_j|A) = 1$.

2.2.3. Variable aleatoria

Setup: Ω se puede dividir en eventos mutuamente exclusivos con los cuales se puede asociar un número.

Variable aleatoria $\equiv$ función $\Omega \to \mathbb{K}$. Cuerpo $\mathbb{K}$, ejemplos: $\mathbb{K} = \mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}\ldots$

Ejemplos

Distribución binomial. Consideramos un super-experimento consintiendo en n repeticiones de un mismo experimento consistiendo en tirar una moneda donde $P('h') = p$.

$P('k',' h' \text{ en } n) = \begin{pmatrix} n \\ k \end{pmatrix} p^k(1-p)^{n-k}$.

$n = 3$, $k = 1$. Los eventos que nos interesan son:

$$\left.\begin{array}{l} htt = E_1 = (\prod_1 h) \cap (\prod_2 t) \cap (\prod_3 t) \\ tht = E_2 = (\prod_1 t) \cap (\prod_2 h) \cap (\prod_3 t) \\ tth = E_3 = (\prod_1 t) \cap (\prod_2 t) \cap (\prod_3 h) \end{array}\right\} P(E_1) = P(E_2) = P(E_3) = P(1-p)^2$$

Queremos $P(E_1 \cup E_2 \cup E_3) \underbrace{=}_{mut.exc.} P(E_1) + P(E_2) + P(E_3) = 3P(1-p)^2$

Cuando una variable aleatoria tiene valor en un cuerpo continuo (ej. $\mathbb{R}$) se define la <u>demidad</u> de prueba en un punto $x \equiv p(x) = \lim_{j\to 0} \dfrac{Probabilidad[X \in B(x,\delta)]}{vol(B(x,\sigma))}$.

$Probabilidad[x \in A] = \int_A p(x)dx$ $(\forall A \in F)$.

Momentos de orden $m \equiv < X^m >= \sum_{X\in\mathbb{K}} P(x)x^m$ (si n discreto) $= \int p(x)x^m dx$ ($\mathbb{K}$ continuo).

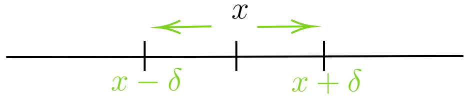
Valor medio: $m = 1$

Varianza: $< X^2 > - < X >^2$

De manera análoga a los eventos, diremos que dos variables aleatorias X e Y son independiente si su distribución de prueba junta factoriza: $P_{xy}(x,y) = P_x(x)P_y(y)$.

Ejemplos

- $\mathbb{R}$



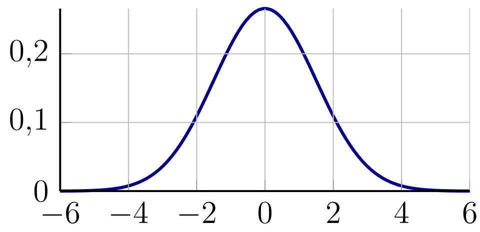
Prueba en $x = 0$ literalmente. Prueba $[x - \delta \leq X \leq x + \delta]$ si puede ser finito. $\underbrace{P(x)}_{\text{densidad en x}} = \lim_{\delta\to 0} \dfrac{Probabilidad[x-\delta \leq X \leq x+\delta]}{2\delta}$. $P[a \leq x \leq b] = \int_a^b p(x)dx$.

- Distribución Guassiana

$p(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$

$\mu \equiv$ mediana y media (altura curva)

$\sigma^2 \equiv$ varianza (anchura curva)



2.2.4. Ley de los grandes números

Sean $x_1, \ldots, x_n \equiv$ *iid* (independencia y identidad distribuida) variables aleatorias con media finita μ y varianza σ^2 y sea $S_n = x_1 + \cdots + x_n$. $\forall \varepsilon > 0$, $Probabilidad[|S_n - n\mu| \geq n\varepsilon] \leq \frac{\sigma^2(x)}{n\varepsilon^2} \rightarrow_{n\rightarrow\infty} 0$ (fundamento para hablar de ensayos clínicos).

2.2.5. La desigualdad de Hoeffding

Sean $x_1, \ldots, x_n \equiv n$ iid, variable aleatoria n. tal que $X \varepsilon [a, b]$(intervalo finito). $\forall \eta > 0$, $Probabilidad[|S_n - n\mu| \geq \eta] \leq 2exp\left[-\frac{2n\eta}{(b-a)^2}\right]$.

Cambio cualitativo en el nivel de confianza.

Tema 3

Álgebra lineal

Los estados de un sistema cuántica están en correspondencia con los elementos del espacio vectorial (EV)[1] y la suma de los vectores tiene sentido físico.

Definición. Cuerpo $\mathbb{F}$ en un conjunto equipado con las operaciones (+ y *) tal que

- $\left.\begin{array}{c} a+(b+c)=(a+b)+c \\ a(bc)=(ab)c \end{array}\right\} \forall a,b,c \in \mathbb{F}$ (Asociatividad)
- $\left.\begin{array}{c} a+b=b+a \\ a*b=b*a \end{array}\right\} \forall a,b \in \mathbb{F}$ (Conmutatividad)
- $\exists$ neutro o para +, 1 para x
- $\forall a \in \mathbb{F}$, $\exists$ inverso para +, 1 para +, -a tal que $a+(-a)=0$
- $\forall a \in \mathbb{F}-\{0\}$, $\exists$ inverso a^{-1} para x tal que $a*a^{-1}=1$

Cuerpos: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (cuerpo usado en física cuántica)

3.1. Espacio vectorial

Los espacios vectoriales (EVs) son los ámbitos en los que describiremos los estados de un sistema cuántico.

[1] Más generalmente espacios de Hilbert. Nosotros al restringirnos a cúbits en esta asignatura, no necesitaremos esta noción.

Definición (Espacio vectorial V). Un EV es un conjunto equipo con una operación $+ .VxV \to$ V tal que:

- Asociatividad $(|u\rangle + |v\rangle) + |w\rangle = |u\rangle + (|v\rangle + |w\rangle)$[2]
  $\forall\, |u\rangle,\ |v\rangle,\ |w\rangle \in V$
- Conmutatividad: $|u\rangle + |v\rangle = |v\rangle + |u\rangle$
  $\forall\, |u\rangle,\ |v\rangle \in V$
- $\exists$ neutro 0: $|u\rangle + 0 = |u\rangle$
  $\forall\, |u\rangle \in V$
- $\exists$ inverso % $+$: $\forall\, |u\rangle \in V$, $\exists\, |-u\rangle$ único tal que $|u\rangle + |-u\rangle = 0$
- $\forall a \in \mathbb{C}$, $\forall\, |u\rangle \in V$, $a\,|u\rangle \in V$
- Compatibilidad entre $X^{\text{ción}}$ en $\mathbb{C}$ y $X^{\text{ción}}$ entre escalares y vectores: $(ab)\,|u\rangle = a(b\,|u\rangle)$
  $\forall a, b \in \mathbb{C}$
  $\forall\, |u\rangle \in V$
- $1\ |u\rangle = |u\rangle$
  $\forall\, |u\rangle \in$ V
- Distributividad: $a(|u\rangle + |v\rangle) = a\,|u\rangle + a\,|v\rangle \to (a+b)\,|u\rangle = a\,|u\rangle + b\,|u\rangle$
  $\forall a, b \in \mathbb{C}$
  $\forall\, |u\rangle\,, |v\rangle \in V$

Ejemplos

- $\mathbb{C}$ mismo
- $\mathbb{C}^n \equiv$ conjunto de n-uplas complejas
  $\{(a_1, \ldots, a_n) : a_j \in \mathbb{C},\ j = 1 \ldots n\}$ equipados con $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$
- Conjunto de matrices complejas $m{*}n$ equipada con la suma de matrices habitual
- Conjunto de polinomios de una variable compleja ζ de grado $\leq$ k (entero finito) equipado con la suma habitual.

[2] $|v\rangle$: notación de Dirac común en física cuántica.

$$\left.\begin{array}{l}|v_1\rangle = a_0 + a_1\zeta + \cdots + a_k\zeta^k \\ |v_2\rangle = a_0' + a_1'\zeta + \cdots + a_k'\zeta^k\end{array}\right\} |v_1\rangle + |v_2\rangle = (a_0+a_0') + (a_1+a_1')\zeta + \cdots + (a_k+a_k')\zeta^k$$

3.2. Independencia lineal

$|v_1\rangle, \ldots, |v_n\rangle$ son linealmente independientes $\equiv a_1|v_1\rangle + \cdots + a_n|v_n\rangle = 0 \Rightarrow a_1 = \cdots = a_n = 0$.

Interpretación: ninguno de los vectores $|v_1\rangle, \ldots, |v_n\rangle$ se puede expresar como combinación lineal de los otros.

Dimensión de un EV $\equiv$ cardinalidad máxima de un conjunto de vectores linealmente independientes.

Base de un EV $\equiv$ conjunto máximo de vectores linealmente independientes.

Sea B $= |v_1\rangle, \ldots, |v_n\rangle$ con base $|w\rangle \notin$ B. Si consideramos una combinación tal que $a_0|w\rangle + a_1|w_1\rangle + \cdots + a_n|w_n\rangle = 0$, pueden pasar dos cosas:

(1) $a_0|w\rangle = 0 \Rightarrow a_0 = 0$ o $|w\rangle = 0$. Es trivial ya que solo volvemos a ver que hace falta que $a_1 = \cdots = a_n = 0$.

(2) $a_0|w\rangle \neq 0$ ya que B es un conjunto máximo, tiene que ser el caso en el que $|a_1| + \cdots + |a_n| \neq 0$ porque sino la dimensión sería $n+1$ en lugar de n. Entonces $|w\rangle = \frac{a_1}{a_0}|v_1\rangle + \cdots + \frac{a_n}{a_0}|v_n\rangle$. Es decir, $\forall |w\rangle \notin 0$ se puede expresar como combinación lineal de elementos de B.

$$|w\rangle = \underbrace{c_1|v_1\rangle + c_2|v_2\rangle + \cdots + c_n|v_n\rangle}_{\text{Componentes de } |w\rangle \text{ en la base B}}$$

Ejemplos de EV y bases

-

EV	$\mathbb{C}^2$	$\mathbb{C}^2$	$\overbrace{gl(2,\mathbb{C})}^{\text{Matrices complejas 2x2}}$
Base	{(1,0),(0,1)}	{(1,0),(1,1)}	$\left\{\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix}\right\}$

$\mathbb{C}^2$ y $\{(1,0),(0,1)\}$

Independencia lineal?

$$\underbrace{a_1(1,0)+a_2(0,1)}_{(a_1,a_2)=(0,0)\Leftrightarrow a_1=0 \text{ y } a_2=0} = 0 \Leftrightarrow a_1 = a_2 = 0$$

Conjunto máximo?

Supongamos $\exists(x,y)$ tal que $a_1(1,0)+a_2(0,1)+a_3(x,y)=(0,0) \Leftrightarrow a_1 = a_2 = a_3 = 0$. Entonces $\begin{cases} a_1 + a_3 x = 0 \\ a_2 + a_3 y = 0 \end{cases}$

Si $x \neq 0$, entonces consideramos $a_1 = -x$ y $a_3 = 1$ lo que permite satisfacer (1).

Si $x = 0$, entonces $a_1 = 0$ y $a_3 = 1$ permite satisfacer (1).

Si $y \neq 0$, entonces considerando $a_2 = -y$ y $a_3 = 1$ permite satisfacer (2).

Si $y = 0$, entonces $a_2 = 0$, $a_3 = 1$ permite satisfacer (2).

En todo caso, $(a_1, a_2, a_3) = (-x, -y, 1) \neq (0,0,0)$ es solución. {(1,0),(0,1),(x,y)} no son linealmente independientes porque $\forall(x,y) \Rightarrow \{(1,0),(0,1)\}$ es máximo.

Teorema. $\forall$ base tiene el mismo número de elementos.

Definición. Un subespacio W de un EV V es un subconjunto $W \subset V$ satisfaciendo todos los axiomas de un EV.

Ejemplos

- $\mathbb{C}^2$ es un subespacio vectorial (SEV) de $\mathbb{C}^3$
- El conjunto de matrices diagonales 2x2 es un SEV de $gl(2,\mathbb{C})$

3.3. Sumas y sumas directas

Sean W_1, W_2 subespacios vectoriales (SEVs) de un EV V.

Definición (Suma $\mathbf{W_1 + W_2}$). $\{w_1 + w_2;\ w_1 \in W_1,\ w_2 \in W_2\}$

Ejemplo

$W_1 = \{a(1,0);\ a \in \mathbb{C}\} \subset \mathbb{C}^2$

$W_2 = \{b(1,1);\, b \in \mathbb{C}\} \subset \mathbb{C}^2$

$W_1 + W_2 = \{a(1,0) + b(1,1), a, b \in \mathbb{C}\} = \mathbb{C}^2$ ya que $\{(1,0),(1,1)\}$ es base de $\mathbb{C}^2$.

Teorema (Fórmula de Grassmann). Sean W_1, W_2 SEVs del EV V

$dim(W_1 + W_2) = dim(W_1) + dim(W_2) - dim(W_1 \cap W_2)$.

Curiosidad: analogía con $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

Definición. Si $W_1 \cap W_2 = \{0\}$ se dice que la suma es directa y escribimos $W_1 \oplus W_2$.

Proposición $W_1 + W_2$ es una suma directa $\Leftrightarrow \forall \left|w\right\rangle \in W_1 + W_2$.

$\left|w\right\rangle$ se puede descomponer de manera única en un vector $\left|w_1\right\rangle$ de W_1 y $\left|w_2\right\rangle$ de W_2.

Proposición $\forall$ SEV W de un EV V, $\exists$ SEV complementario W^c: $V = W \oplus W^c$.

3.4. Cambio de base

Aviso

Muy importante cuando hablemos de medida en física cuántica.

Sean $\{\left|v_1\right\rangle, \dots, \left|v_n\right\rangle\} \equiv B$ y $\{\left|v_1'\right\rangle, \dots, \left|v_n'\right\rangle\} \equiv B'$ dos bases de un EV V. Sea $\left|v\right\rangle$ EV consideramos la descomposición de $\left|v\right\rangle$ en cada una de estas bases: $\begin{cases} \left|v\right\rangle = \alpha_1 \left|v_1\right\rangle + \dots + \alpha_n \left|v_n\right\rangle \\ \left|v\right\rangle = \alpha_1' \left|v_1'\right\rangle + \dots + \alpha_n' \left|v_n'\right\rangle \end{cases}$

Observación: esas descomposiciones son únicas. Supongamos que existen 2 descomposiciones $\neq$ de $\left|v\right\rangle$ en B $\begin{cases} \left|v\right\rangle = \alpha_1 \left|v_1\right\rangle + \dots + \alpha_n \left|v_n\right\rangle \\ \left|v\right\rangle = \alpha_1' \left|v_1\right\rangle + \dots + \alpha_n' \left|v_n\right\rangle \end{cases}$ donde $(\alpha_1, \dots, \alpha_n) \neq (\alpha_1', \dots, \alpha_n')$ por lo que $\{\left|v_1\right\rangle, \dots, \left|v_n\right\rangle\}$ no son linealmente independientes y son una contradicción.

Entonces $\left|v\right\rangle - \left|v\right\rangle = 0 = (\alpha_1 - \alpha_1')\left|v_1\right\rangle + \dots + (\alpha_n - \alpha_n')\left|v_n\right\rangle$. En particular $\forall \left|v_j'\right\rangle \in B'$, $\exists \{A_j^i\}$ únicos tal que $\left|v_j'\right\rangle = \sum_i A_j^i \left|v_i\right\rangle$.

$\left|v\right\rangle = \alpha_1'(\sum_i A_1^i \left|v_i\right\rangle) + \dots + \alpha_n'(\sum_i A_n^i \left|v_i\right\rangle) = \sum_i (\sum_j \alpha_i' A_j^i) \left|v_i\right\rangle$

$\alpha_i = \sum_j \alpha_i^1 A_j^i$: cambio de base.

$$\left.\begin{array}{l} B = \{|v_1\rangle, \ldots, |v_n\rangle\} \\ B' = \{|v'_1\rangle, \ldots, |v'_n\rangle\} \end{array}\right\}$$ son bases del EV de V. Vemos que $\forall\,|\phi\rangle$ EV se puede expresar como combinación lineal en B o en B'.

$$\left.\begin{array}{l} |\phi\rangle = \sum_{i=1}^n \phi_i |v_i\rangle \\ |\phi'\rangle = \sum_{j=1}^n \phi'_j \left|v'_j\right\rangle \end{array}\right\}$$ descomposiciones únicas.

$\exists$ coeficiente (B' es una base) A_{ij} tal que $|v'_i\rangle = \sum_{j=1}^n A_{ij} \left|v'_j\right\rangle$. Sustituyendo vemos que $|\phi\rangle = \sum_{i=1}^n \phi_i \sum_{j=1}^n A_{ij} \left|v'_j\right\rangle = \sum_{j=1}^n (\sum_{i=1}^n \phi_i A_{ij}) \left|v'_j\right\rangle$. Por unicidad de la descomposición $\phi'_j = \sum_{i=1}^n \phi_i A_{ij}$ por lo que $\forall$ vector $|\phi\rangle$ donde B es una base por lo que $\exists$ coeficiente $\tilde{A}_{jn}$ tal que $\left|v'_j\right\rangle = \sum_{n=1}^n \tilde{A}_{jn} |v_n\rangle$. Sustituyendo $|\phi\rangle = \sum_{j=1}^n (\sum_{i=1}^n \phi_i A_{ij}) \sum_{n=1}^n \tilde{A}_{jn} |v_n\rangle = \sum_{n=1}^n (\sum_{i=1}^n \sum_{j=1}^n \phi_i A_{ij} \tilde{A}_{jn}) |v_n\rangle$.
Unicidad: $\phi_n = \sum_{i=1}^n \phi_i \sum_{j=1}^n A_{ij}\tilde{A}_{jn} = \sum_{i=1}^n \phi_i (A\tilde{A})_{in}$.
$\forall\,|\phi\rangle \Rightarrow A\tilde{A} = 1$. Similarmente $\tilde{A}A = 1$.

Ejemplos

- $V = \mathbb{C}$

  $B = \{\underbrace{(1,0)}_{|v_1\rangle}, \underbrace{(0,1)}_{|v_2\rangle}\}$, $B' = \{\underbrace{(1,1)}_{|v'_1\rangle}, \underbrace{(1,-1)}_{|v'_2\rangle}\}$

  Halla la matriz de cambio de base.

  $$\left\{\begin{array}{l} |v_1\rangle = A_{11}|v'_1\rangle + A_{12}|v'_2\rangle \\ |v_2\rangle = A_{21}|v'_1\rangle + A_{22}|v'_2\rangle \end{array}\right\} \Leftrightarrow \left\{\begin{array}{l} (1,0) = A_{11}(1,1) + A_{12}(1,-1) \\ (0,1) = A_{21}(1,1) + A_{22}(1,-1) \end{array}\right\}$$

  $$\Leftrightarrow \left\{\begin{array}{l} 1 = A_{11} + A_{12} \\ 0 = A_{11} + A_{12} \\ 0 = A_{21} + A_{22} \\ 1 = A_{21} - A_{22} \end{array}\right\}. \text{ Solución } \left\{\begin{array}{l} A_{11} = A_{12} = \frac{1}{2} \\ A_{11} = -A_{22} = \frac{1}{2} \end{array}\right. \text{ por lo que A=} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

- Cambia de base entre entre B y B".

  $B'' = \{(1,i),(1,-i)\}$

3.5. Aplicación lineal

$\wedge$ entre dos bases vectoriales (BVs). V y W $\equiv$ una función $\wedge : v \to w$ tal que:

- $\wedge(\alpha\,|v\rangle) = \alpha \wedge (|v\rangle)$

  $\forall \alpha \in \mathbb{C}$

$\forall \, |v\rangle \in V$

- $\wedge(|v_1\rangle + |v_2\rangle) = \wedge(|v_1\rangle) + \wedge(|v_2\rangle)$

  $\forall \, |v_1\rangle, \, |v_2\rangle \in$ V

Propiedades

- $\wedge(\alpha \, |v_1\rangle + \beta \, |v_2\rangle) = \alpha \wedge (|v_1\rangle) + \beta \wedge (|v_2\rangle)$

  $\forall \alpha\beta \in \mathbb{C}$

  $\forall \, |v_1\rangle, \, |v_2\rangle \in V$

- $\wedge(0) = 0$

- $\wedge(- \, |v\rangle) = - \wedge (|v\rangle)$

- $\wedge$: v$\rightarrow$w operación lineal $\Rightarrow \wedge$ o Ω: u$\rightarrow$w es una aplicación lineal Ω: u$\rightarrow$v

Las aplicaciones lineales nos servirán para caracterizar la evolución de un sistema cuántico.

Ejemplos

- Cambio de base

  - Sea V una base vectorial (BV) con base $B = \{|v_j\rangle : j = 1 \ldots n\}$

- $\forall \, |w\rangle \in$ V, $|w\rangle = \alpha_1 \, |v_1\rangle + \cdots + \alpha_n \, |v_n\rangle$

  $\prod_k$; V$\rightarrow$ $\mathbb{C}$: $|w\rangle \rightarrow \alpha_k$ (k-isima componente de $|w\rangle$ en B). $1 \leq k \leq n$ es una aplicación lineal (quasi-proyección).

Sea $\wedge$: V$\rightarrow$W aplicación lineal

<u>Núcleo</u>: Nuc$\wedge \equiv \{|v\rangle \in V : \wedge(|v\rangle) = 0\}$

<u>Imagen</u>: Im$\wedge \equiv \{|w\rangle \in W : \exists \, |v\rangle \in V$ tal que $\wedge(|v\rangle) = |w\rangle\}$

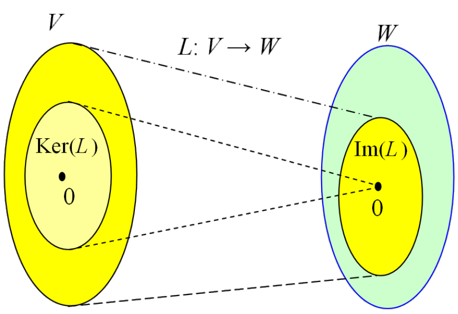


Figura 3.1: En nuestro caso en vez de L seria $\wedge$

Teorema.

(1) $\text{Ker}\wedge$ es subbase vectorial (SBV) de V

(2) $\text{Im}\wedge$ es SBV de W

Demostración

Sean $\alpha \in \mathbb{C}$, $|v_1\rangle, |v_2\rangle \in \text{Ker}\wedge$

$\wedge(\alpha|v_1\rangle) = \alpha \wedge (|v_1\rangle) = \alpha * 0 \Rightarrow \alpha|v\rangle \in \text{Ker}\wedge$

$\wedge(|v_1\rangle + |v_2\rangle) = \wedge(|v_1\rangle) + \wedge(|v_2\rangle) = 0 * 0 \Rightarrow |v_1\rangle + |v_2\rangle \in \text{Ker}\wedge$. (2) se demuestra de manera análoga.

Proposición. Sea $\wedge$: V$\rightarrow$W una aplicación lineal donde $dim(V) < \infty$. Entonces $dim(V) = dim(\text{Ker}\wedge) + dim(\text{Im}\wedge)$.

Sea $\wedge$: V$\rightarrow$W una aplicación lineal $\begin{cases} B = \{|v_1\rangle, \dots, |v_n\rangle\} \text{ es base de V} \\ B' = \{|w_1\rangle, \dots, |w_n\rangle\} \text{ es base de W} \end{cases}$ donde $\forall |v_i\rangle \in B$, $\exists$ coeficiente A_{ij} tal que $\wedge(|v_1\rangle) = \sum_{j=1}^{m} A_{ij}|w_j\rangle$. $A = \{A_{ij}\} \equiv$ matriz asociada a la aplicación lineal $\wedge$.

Definición. Sean V, W BV. $L(V, W) \equiv$ conjunto de aplicaciones lineales de V y W.

Teorema. $L(V, W)$ es un EV para la suma $\wedge_1 + \wedge_2$; V$\rightarrow$W: $|v\rangle \rightarrow (\wedge_1 + \wedge_2)(|v\rangle) \equiv \wedge_1(|v\rangle) + \wedge_2(|v\rangle)$.

$\forall \wedge_1, \wedge_2 \in L(V, W)$

Demostración. (Aplicación directa de la definición de EV)

Caso particular muy importante en física cuántica: $W = \mathbb{C}$.

Definición.

El espacio dual, V^*, de una BV V se define como $V^* \equiv L(V, \mathbb{C})$. Por motivos que se aclararán en breve notaremos $\langle u|$ los elementos de V^*.

Definiciones.

Una función lineal V$\rightarrow$W es:

- inyectivo $\equiv \text{Ker}\wedge = \{0\}$

- suprayectivo $\equiv \text{Im} \wedge = W$
- biyectivo $\equiv$ inyectivo + suprayectivo
- lineal y biyectiva $\equiv$ isomorfismo
- lineal y V = W $\equiv$ endomorfismo
- endomorfismo + biyectivo $\equiv$ automorfismo

Teorema. Sea V una BV con base $B = \{\langle v_i|\}$; V$\rightarrow \mathbb{C} : |v_j\rangle \rightarrow \begin{cases} 0 \text{ si } i \neq j \\ 1 \text{ si } i = j \end{cases}$ es una base de V^*, el dual de V.

Consideramos ahora $(V^*)^* \equiv L(V^*, \mathbb{C})$.

Teorema. $(V^*)^*$ es isomorfo a V.

Teorema. V^* es isomorfo a V.

3.6. Espectro de un endomorfismo

Definición. Un par (autovalor, autovector) asociado a un endomorfismo.

$$\wedge : V \rightarrow V \equiv \lambda \in \mathbb{C}, |v\rangle \in V$$

$$\wedge(|v\rangle) = \lambda |v\rangle$$

El conjunto de autovalores de $\wedge \equiv$ espectro de $\wedge$.

Teorema. El conjunto de autovectores asociado a un mismo autovalor es un SEV de V.

Ejercicio

Sea $\wedge$: $\mathbb{C}^2 \rightarrow \mathbb{C}^2$ $\begin{pmatrix} x \\ y \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$. Calcular los autovalores y autovectores asociados.

Sea $|v\rangle$ un autovector con autovalor λ, entonces $M|v\rangle = \lambda |v\rangle \Leftrightarrow M|v\rangle = \lambda 1 |v\rangle \Leftrightarrow (M - \lambda 1)|v\rangle = 0 \rightarrow det[M - \lambda 1] = 0$

Espectro de endomorfismo $\wedge$: V$\to$V $\equiv$ $pares(\lambda, |v\rangle)$: $\wedge |v\rangle = \lambda |v\rangle$ donde $\lambda \in \mathbb{C}$ y $|v\rangle \in V$.

Una aplicación lineal es hermítica si su matriz asociada es auto-adjunta es una base ortonormal.
El adjunto A^* de una matriz A se define como $A^*_{ij} = \bar{A}_{ji}$ (matriz conjugada y traspuesta).
Observación. $(A^*)^* = A, (AB)^*$.

Una matriz cuadrada $\mathcal{U}$ es unitaria si satisface: $\mathcal{U}\mathcal{U}^* = \mathbb{1}$ o $\mathcal{U}^*\mathcal{U} = 1$.

$$(AB)^*_{ij} = (\overline{AB})_{ji} = \sum_n \bar{A}_{jn}\bar{B}_{ni} = \sum_n \bar{B}_{ni}\bar{A}_{jn} = \sum_n B^*_{in}A^*_{nj} = (B^*A^*)_{ij}$$

En mecánica cuántica las matrices hermíticas están relacionadas con los procesos de medida, mientras que las unitarias describen la evolución temporal de un sistema.

3.7. Producto escalar

Las operaciones $<,>$: $V\text{x}V \to \mathbb{C}$ satisfacen $< v,\ \alpha w_1 + \beta w_2 >= \alpha < v,\ w_1 > +\beta < v,\ w_2 >$ donde $\forall \alpha,\ \beta \in \mathbb{C}$ y $\forall\, |v\rangle,\ |w_1\rangle,\ |w_2\rangle \in V$.

- $< v, w >=< \overline{w, v} >$ (hermiticidad) $\forall\, |v\rangle,\ |w\rangle \in V$
- $< v, v >\geq 0$ y $< v, v >= 0 \Leftrightarrow |v\rangle = 0$

Ejemplo
$\mathbb{C}^* \equiv$ BV de n-tuplas complejas con base canónica.
$|e_1\rangle = (1, 0, \dots, 0)$
$\dots$
$|e_j\rangle = (0, \dots, 0, \underbrace{1}_{j}, 0, \dots, 0)$
$\dots$
$|e_n\rangle = (0, \dots, 0, 1)$
$< u, w >\equiv \sum_{n=1}^{n} \overline{V}_n W_n$

Observación. Sean $\{S_n > 0; n = 1, \dots, n\}$, $< v, w >= \sum_{n=1}^{n} S_n\overline{V}_n W_n$ también definiría un producto escalar.

Una base $B \equiv \{|e_j\rangle\,; j = 1, \ldots, n\}$ es ortogonal $\equiv i \neq j \Rightarrow < e_i, e_j >= 0$.

Norma. Operación $V \to \mathbb{R}$ tal que

$\| \, |v\rangle \, \| = 0 \Leftrightarrow |v\rangle = 0$

$\|h \, |v\rangle \, \| = |h| \|v\|$ donde $\forall h \in \mathbb{C}$, $\forall \, |v\rangle \in V$

$\| \, |u\rangle + |v\rangle \, \| \leq \|u\| + \|v\|$ (desigualdad A)

Ejemplo

Dado un producto escalar $< v, v >^{\frac{1}{2}} = \|v\|$ proporciona una norma.

Teorema (Cauchy–Schwarz). $|\langle u, v\rangle| \leq \|u\| \|v\|$ donde $\forall \, |u\rangle$, $|v\rangle \in V$.

Definición. Una base $B = \{|ij\rangle\,; j = 1, \ldots, n\}$ considerada ortonormal $\equiv \forall_{ij} = 1, \ldots, n$,

$$< e_i, e_j >= \begin{cases} 0 \text{ si } i \neq j' \\ 1 \text{ si } i = j' \end{cases}$$

Teorema (Teorema de Riesz). Sea V BV con producto escalar $\forall \alpha \in V^*$, $\exists \, |A\rangle \in V$ tal que $\alpha(|v\rangle) =< A, v >$ donde $\forall \, |v\rangle \in V$.

Es decir, cualquier elemento del dual se puede representar como un producto escalar con un elemento determinado del BV.

En mecánica cuántica llamamos "BRA" a cualquier elemento del dual V^* y "KET" a cualquier elemento/vector de V.

Sea $B = \{|u_i\rangle\,; i = 1, \ldots, n\}$ una base ortogonal ($\perp^{(mal)}$) de una BV V.

Sea $\langle u_i|$ el elemento de V^* tal que

$\langle u_i|\phi\rangle =< u_i, \phi >$

$\langle u_i|u_i\rangle = \delta_{ij}$

Consideramos el operador $\sum_i |u_i\rangle \langle u_i|$. ¿Como actúa en V?

$\langle u_i|$: $V \to \mathbb{R}$

$|u_i\rangle \langle u_i|$: $V \to \mathbb{R} \to V$

Sea $|\phi\rangle \in V$: $(|u_i\rangle \langle u_i|) \underbrace{|\phi\rangle}_{\in V} = \underbrace{|u_i\rangle}_{\in V} < \underbrace{u_i, \phi}_{\in \mathbb{C}} >= [\sum_i |u_i\rangle \langle u_i|] \, |\phi\rangle = \sum_i |u_i\rangle \underbrace{< u_i, \phi >}_{\phi_i \text{ (unidad)}}$

En la base B $|\phi\rangle$ se expresa de la siguiente manera (ϕ_j es la componente de $|\phi\rangle$ en B):

$$|\phi\rangle = \sum_{j=1}^{n} \phi_j |u_j\rangle = \sum_{i=1}^{n} |u_i\rangle \langle u_i| \ \ |\phi\rangle = \sum_{i=1}^{n} |u_i\rangle < u_i \sum_{j=1}^{n} \phi_j u_j >$$

Linealidad, X^{to} escalar

$$\sum_i |u_i\rangle \sum_{j=1}^{n} \phi_j \underbrace{< u_i, u_j >}_{\delta_{ij}(B\perp^{mal})} = \sum_i \phi_i |u_i\rangle = |\phi\rangle$$

$\sum_{i=1}^{n} |u_i\rangle \langle u_i|$ es la aplicación de identidad denotado por 1 o Id.

Sea X: V→W operador lineal. Sea $|\phi\rangle \in$V.

$X|\phi\rangle = 1_w X 1_v |\phi\rangle$

Sea $\{|v_i\rangle ; i = 1, \ldots, dim(V)\}$: base $\perp^{mal}$ de V.

Sea $\{|w_j\rangle ; j = 1, \ldots, dim(W)\}$: base $\perp^{mal}$ de W.

$$X|\phi\rangle = \sum_{j=1}^{dim(W)} |w_j\rangle \langle w_j| X \sum_{i=1}^{dim(V)} |v_i \text{ x } v_i| |\phi\rangle = \sum_{j=1}^{dim(W)} \left[\sum_{i=1}^{dim(V)} \langle w_j| X |v_i\rangle \phi_i \right] |w_j\rangle$$

Las complejas $\{\langle w_j| x |v_i\rangle\} \equiv$ elementos de matriz del operador X relativos a las bases $\{|v_i\rangle , |w_i\rangle\}$.

Me interesa $X|\phi\rangle$:

$$\underbrace{X|\phi\rangle}_{\in W} = 1_w X \underbrace{|\phi\rangle}_{1_v|\phi\rangle} = 1_w X 1_v |\phi\rangle$$

X: V→V hermítico $\equiv \langle v_i| X |v_j\rangle = \overline{\langle v_j| X |v_i\rangle}$.

Se puede demostrar X hermítico $\equiv \langle \phi| X |\psi\rangle = \overline{\langle \psi| X |\phi\rangle}$ donde $\forall |\phi\rangle |\psi\rangle \in V$.

Teorema. Los autovalores de un operador hermítico son reales.

Demostración. Sea X hermítico y sea $|\phi\rangle$ autovector con autovalor λ.

$\langle \phi| X |\phi\rangle = \langle \phi| (X|\phi\rangle) = \langle \phi| (\lambda |\phi\rangle) = \lambda < \phi, \phi >$

$X_{herm} \Rightarrow \langle \phi| X |\phi\rangle = \overline{\langle \phi| X |\phi\rangle} = \overline{\lambda} < \phi, \phi > \Rightarrow \lambda = \overline{\lambda}$

Teorema. Sea $X = X^*$ y sean λ_1, λ_2 autovalores distintos de X, $y\,|\phi_1\rangle$, $|\phi_2\rangle$ auto-

vectores asociados
$\left.\begin{array}{l} X\left|\phi_1\right\rangle = \lambda_1\left|\phi_1\right\rangle \\ X\left|\phi_2\right\rangle = \lambda_2\left|\phi_2\right\rangle \end{array}\right\}$ por lo que $\langle\phi_1|\phi_2\rangle = 0$.

Demostración.

$$\left.\begin{array}{ll} \langle\phi_1| X\left|\phi_2\right\rangle & = \langle\phi_1| (\underbrace{X\left|\phi_2\right\rangle}_{\lambda_2|\phi_2\rangle}) = \lambda_2\left\langle\phi_1|\phi_2\right\rangle \\ & = (\overline{\langle\phi_2| X\left|\phi_1\right\rangle}) = (\overline{\lambda_1\left\langle\phi_2|\phi_1\right\rangle}) \underbrace{=}_{\lambda_1\in\mathbb{R}} \lambda_1\left\langle\phi_1|\phi_2\right\rangle \end{array}\right\} \lambda_1\left\langle\phi_1|\phi_2\right\rangle = \lambda_2\left\langle\phi_1|\phi_2\right\rangle \Rightarrow$$

$$\underbrace{\Rightarrow}_{\lambda_1\neq\lambda_2} \langle\phi_1|\phi_2\rangle = 0$$

Ejercicios

(1) Demostrar que una transformación unitaria preserva el producto escalar.

Sea $\mathcal{U}$: V→V donde $|v\rangle, |w\rangle \in V$. Sea $B = \{|b_j\rangle\}$: base $\perp^{mal}$.

- $|v'\rangle = \mathcal{U}|v\rangle = \mathcal{U}\sum_j v_j |b_j\rangle = \sum_j v_j \mathcal{U}|b_j\rangle^* = \sum_j\sum_n v_j \langle b_n|\mathcal{U}|b_j\rangle |b_n\rangle$
  $^*\mathcal{U}|b_j\rangle = \mathbb{1}\mathcal{U}|b_j\rangle = \sum_n |b_n\rangle\langle b_n|\mathcal{U}|b_j\rangle$
- $|w'\rangle = \mathcal{U}|w\rangle = \sum_l\sum_m w_l \langle b_m|\mathcal{U}|b_l\rangle |b_m\rangle$
- $\langle v|w\rangle = \langle v'|w'\rangle = \langle v'|\sum_{l,m} w_l \langle b_m|\mathcal{U}|b_l\rangle |b_m\rangle$

Linealidad = prod. escalar $\sum_{l,m} w_l \langle b_m|\mathcal{U}|b_l\rangle \langle v'|b_m\rangle$

$\langle v'|b_m\rangle \overbrace{\underbrace{=}_{p.e.}}^{herm.} \overline{\langle b_m|v'\rangle} \underbrace{=}_{linealidad} \sum_{j,n} \overline{v}_j \overline{\langle b_n|\mathcal{U}|b_j\rangle}\ \overline{\langle b_m|b_n\rangle}$

$\langle v'|w'\rangle = \sum_{j,n}\sum_{l,m} w_l\overline{v}_j \langle b_m|\mathcal{U}|b_l\rangle \overline{\langle b_n|\mathcal{U}|b_j\rangle}\ \underbrace{\overline{\langle b_m|b_n\rangle}}_{\langle b_n|b_m\rangle} =$

$= \sum_{j,n,l,m} \overline{v}_j w_l \langle b_n|b_m\rangle \langle b_m|\mathcal{U}|b_l\rangle \overline{\langle b_n|\mathcal{U}|b_j\rangle} =$

$= \sum_{j,n,l} \overline{v}_j w_l \langle b_n|\underbrace{\sum_m |b_m X b_m|}_{\mathbb{1}}\mathcal{U}|b_l\rangle \overline{\langle b_n|\mathcal{U}|b_j\rangle} =$

$= \sum_{j,n,l} \overline{v}_j w_l \underbrace{\langle b_n|\mathcal{U}|b_l\rangle}_{\mathcal{U}_{n,l}} \underbrace{\overline{\langle b_n|\mathcal{U}|b_j\rangle}}_{\mathcal{U}^*_{j,n}} =$

$= \sum_{j,l} \overline{v}_j w_l \underbrace{\sum_n \mathcal{U}^*_{n,l}\mathcal{U}_{n,l}}_{\delta_{j,l}} =$

$= \sum_j \overline{v}_j w_j =$

$= \langle v|w\rangle$

(2) Es unitario $\mathcal{U}$: $\mathbb{C}^2 \to \mathbb{C}^2$ definido en la base canónico como $\begin{cases} |0\rangle \to |1\rangle \\ |1\rangle \to |0\rangle \end{cases}$

Elementos de matriz

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

$$\mathcal{U}^*\mathcal{U} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

(3) Es unitario σ^x: $\mathbb{C}^2 \to \mathbb{C}^2$ definido en la base canónica como $\sigma^x : \begin{cases} |0\rangle \to |1\rangle \\ |1\rangle \to |0\rangle \end{cases}$,

$\sigma^y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ es unitario?

$\sigma^y = (\sigma^y)^*$, $\sigma^z = (\sigma^z)^*$ sí

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$$\begin{vmatrix} 1-\lambda & 2 \\ 2 & 1-\lambda \end{vmatrix} = (1-\lambda)^2 - 4 = \lambda^2 - 2\lambda + 1 - 4 = \lambda^2 - 2\lambda - 3$$

$$\delta = 4 + 12 = 16 \Rightarrow \lambda_{\frac{1}{2}} = \frac{2 \pm 4}{2} = \begin{cases} 3 \\ -1 \end{cases}$$

$\underline{\lambda = -2}$

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 3 \end{pmatrix} = 3 \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

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

Teorema. Si $A = A^*$ entonces $\exists D$ real y diagonal, $\mathcal{U}$ unitaria tal que $A = \mathcal{U}D\mathcal{U}^*$ (diagonalización de D) donde:

- Las columnas de $\mathcal{U}$ son autovectores de A
- La diagonal de D son autovalores de A

3.8. Postulados de la mecánica cuántica

Involucra tres nociones claves (observación, analogía con la arquitectura de Von Newman de un ordenador):

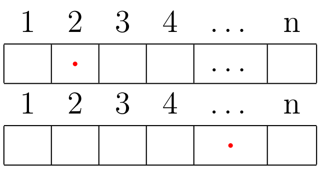
- Estado de un sistema físico ... preparación de un *input*
- Evolución de un sistema ... calculo en ALU
- Medidas sobre este sistema ... lectura de *output*

3.8.1. Postulado 1

El estado de un sistema físico en un instante t está caracterizado por un elemento de un EV. Llamaremos *kets* a cualquier vector de este EV.

Es profundo y perturbador porque se pueden sumar los vectores de una EV. Es decir, si $|\phi_1\rangle$ y $|\phi_2\rangle$ representan dos estados posibles del sistema, $|\phi_1\rangle + |\phi_2\rangle$ representa también un estado posible del sistema.

Ilustración. Consideraremos una partícula que pueda ocupar cualquiera de las posiciones de un registro de n posiciones.



V: conjunto generado por la base $\{|j\rangle : j = 1, \dots, n\}$ donde $|j\rangle \equiv$ estado con la partícula en la casilla j.

$\sum_{j=1}^{n} C_j |j\rangle$ también es un estado posible $(C, j \in \mathbb{C})$.

3.8.2. Postulado 2

Definición. Una observable es un operador (aplicación lineal) hermítica (cuyos vectores propios forman una base del espacio donde actúan).

Toda magnitud física medible sobre un sistema físico tiene una representación en términos de una observable actuando sobre el EV asociado al sistema físico.

3.8.3. Postulado 3

La medida de una magnitud física A sólo puede producir como resultado uno de los autovalores de la observable correspondiente.

3.8.4. Postulado 4

Sean $\lambda_1, \ldots, \lambda_n$ autovalores asociados a una observable A. Supongamos que todos estos autovalores son distintos y sea $|\alpha_j\rangle$ autovector asociado al autovalor λ_j.

La probabilidad de obtener el resultado λ_j suponiendo el sistema preparado en el sistema normalizado $|\psi\rangle$ está dado por:

$$\boxed{Proba[\lambda_j] = |\langle\alpha_j|\psi\rangle|^2}$$

3.8.5. Postulado 5

Definición. Proyector $\sqcap$: operador que satisface:

- $\sqcap = \sqcap*$ (auto-adjunto)
- $\sqcap \geq 0 \equiv$ todos sus autovalores no negativos
- $\sqcap^2 = \sqcap$

Ejemplo.
Consideramos una base $\perp^{mal}$ $B = \{|b_i\rangle = 1, \ldots, n\}$ de un EV V.

$\sqcap_{1,\ldots,m} = \sum_{j=1}^{m} |b_j\rangle\langle b_j|$ es un proyector.

Vimos que para un operador hermítico $X = X^*$

- Los autovalores son reales

- Autovectores correspondiendo a autovalores $\neq$ son $\perp$.

Lemma. El conjunto de autovectores asociados a un mismo autovalor λ forma un SEV.
Demostración. Sean $|x_1\rangle$, $|x_2\rangle$ autovectores de X asociados a λ sean $\alpha, \beta \in \mathbb{C}$.
$X(\alpha |x_1\rangle + \beta |x_2\rangle) = \alpha \underbrace{X |x_1\rangle}_{\lambda|x_1\rangle} + \underbrace{\beta |x_2\rangle}_{\lambda|x_2\rangle} = \lambda(\alpha |x_1\rangle + \beta |x_2\rangle)$.

Lemma. Sea V un EV y $W \subseteq V$ un SEV. Sea $B_W \equiv \{\left|\tilde{b}_j\right\rangle; j = 1, \ldots, dim(W)\}$ base de W. El operador $\sqcap_W = \sum_{j=1}^{dim(W)} \left|\tilde{b}_j\right\rangle \left\langle\tilde{b}_j\right|$ es un proyector.
Demostración. Vimos que $\exists W^c$: $W \oplus W^c = V$.

Corolario. $\forall$ autovalor λ de un operador auto-adjunto (a. a.) X, $\exists$ un proyector $\sqcap_\lambda$ sobre el SEV de autovalores asociados.

Definición. λ es degenerado $\equiv dim(SEV_\lambda) > 1 \Leftrightarrow$ rango $\sqcap_\lambda > 1$.

Si medimos un observable X sobre un sistema preparado en el estado (normalizado) $|\psi\rangle$ y si el resultado de la medida es el autovalor λ el sistema se encuentra inmediatamente (porque la evolución temporal puede cambiar el estado del sistema) después de la medida en el estado.

$$\frac{\sqcap_\lambda |\psi\rangle}{\| \sqcap_\lambda |\psi\rangle \|} = \frac{\sqcap_\lambda |\psi\rangle}{\langle\psi| \sqcap_\lambda |\psi\rangle^{\frac{1}{2}}}$$

Observación. La medida cambia en general el estado del sistema, perturba.
Observación. Si $|\psi\rangle$ es autovector de X entonces la medida no cambia su estado.

El postulado 4 dice que la probabilidad de obtener un resultado λ para una medida de un observable X sobre el estado $|\psi\rangle$ normalizado es:

$$\boxed{Proba[\lambda] = \langle\psi|\sqcap_\lambda|\psi\rangle}$$

3.8.6. Postulado 6

La evolución en el tiempo de un estado, $|\psi(t)\rangle$, se rige por la ecuación de Schrödinger $\left(i\hbar\frac{d}{dt} |\psi(t)\rangle = \mathcal{H}(t) |\psi(t)\rangle\right)$ donde $\mathcal{H}(t)$ es la observable asociado a la energía del sistema[3]; el hamiltoniano. $\hbar$ (constate de Plank): $[\hbar] = [E]T = ML^2T^{-2}T = ML^2T^{-1}$.

Ejemplo

Consideremos el observable $\sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

(1) Calcular los resultados posibles de una medida de σ^z. Calcular la probabilidad asociada a cada autovalor.

Q1) ¿Es $|\psi\rangle$ soporte en $\sqcap_\lambda$?

$\forall$ autovalor λ, $\exists$ SEV asociado $W_\lambda \subseteq \mathcal{H}$ (EV total para describir el sistema).

Sea $B \equiv$ base $\perp^{mal}$ de $\mathcal{H}\{|b_j\rangle\,; j = 1, \ldots, dim(\mathcal{H})\}$ tal que los $dim(W_\lambda)$ elementos de B sean base $\perp^{mal}$ de W_λ (siempre se puede hacer). Entonces decimos que $|\psi\rangle$ tiene soporte sobre $W_\lambda \equiv |\psi\rangle$ se puede expresar como $|\psi\rangle = \sum_{j=1}^{dim(W_\lambda)} \psi_j |b_j\rangle$. De manera equivalente $\sqcap_\lambda |\psi\rangle = |\psi\rangle$.

Sea $|\psi\rangle$ autovector asociado a un autovalor λ de una observable X: $X|\psi\rangle = \lambda|\psi\rangle$. $\forall\alpha \in \mathbb{C}$, $|\varnothing\rangle \equiv \alpha|\psi\rangle$ también es autovector con el mismo autovalor: $X|\phi\rangle = X\alpha|\psi\rangle = \alpha X|\psi\rangle = \alpha\lambda|\psi\rangle = \lambda\alpha|\psi\rangle = \lambda|\phi\rangle$.

Para resolver la ambigüedad se suelen considerar estados de norma unidad, pero no es suficiente. Si $\alpha = e^{i\theta}$, $\theta \in \mathbb{R}$ entonces $\|\phi\| = \|\psi\|$ (ejercicio). También $\langle\phi|\sqcap_\lambda|\phi\rangle = \langle\psi|e^{-i\theta} * \sqcap_\lambda * e^{i\theta}|\psi\rangle = \langle\psi|\sqcap_\lambda|\psi\rangle$.

Si $\exists\theta \in \mathbb{R}$: $|\phi\rangle = e^{i\theta}|\psi\rangle$ entonces $|\phi\rangle$ y $|\psi\rangle$ representan el mismo estado.

Resultados posibles $\equiv$ autovalores de σ^z

$$det(\sigma^z - \lambda 1) = \begin{vmatrix} 1-\lambda & 0 \\ 0 & -1-\lambda \end{vmatrix} = -(1-\lambda)(1+\lambda) = 0 \Leftrightarrow \lambda = \pm 1$$

$$SEV_{\lambda=1} \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \Leftrightarrow \begin{pmatrix} x \\ -y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

$$SEV_{\lambda=1} = \left\{\begin{pmatrix} x \\ 0 \end{pmatrix} : x \in \mathbb{C}\right\}. \text{ Base } \perp^{mal} \text{ de } SEV_{\lambda=1} \equiv \left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\} \equiv \{|{+1_z}\rangle\}$$

$$SEV_{\lambda=-1} = \left\{\begin{pmatrix} 0 \\ y \end{pmatrix} : y \in \mathbb{C}\right\}. \text{ Base } \perp^{mal} \text{ de } SEV_{\lambda=-1} \equiv \left\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\} \equiv \{|{-1_z}\rangle\}$$

[3]Consideramos un sistema aislado.

(2) Medimos σ^z sobre

$$\left.\begin{aligned}|\psi_1\rangle &= |{+1_z}\rangle\\ |\psi_2\rangle &= |{-1_z}\rangle\end{aligned}\right\}\sigma^z\,|{\pm 1_z}\rangle = \pm\,|{\pm 1_z}\rangle$$

$$|\psi_3\rangle = \tfrac{1}{2}\,|{+1_z}\rangle + \tfrac{\sqrt{3}}{2}\,|{-1_z}\rangle$$

$$|\psi_4\rangle = \tfrac{1}{\sqrt{2}}\,|{+1_z}\rangle + \tfrac{1}{\sqrt{2}}\,|{-1_z}\rangle$$

$$|\psi_5\rangle = \tfrac{1}{\sqrt{2}}\,|{+1_z}\rangle + e^{i\frac{\pi}{4}}\tfrac{1}{\sqrt{2}}\,|{-1_z}\rangle$$

$$Proba[+1|\psi_1] = \langle\psi_1|\,\sqcap_{+1}\,|\psi_1\rangle = \langle\psi_1|\;\;|{+1_z}\rangle\langle{+1_z}|\;\;|\psi_1\rangle = |\,\underbrace{\langle\psi_1|{+1_z}\rangle}_{1}\,|^2 = 1$$

$$Proba[-1|\psi_1] = \langle\psi_1|\,\sqcap_{-1}\,|\psi_1\rangle = |\,\underbrace{\langle{+1_z}|{-1_z}\rangle}_{0}\,|^2 = 0$$

$$Proba[+|\psi_3] = |\,\langle\psi_3|{+1_z}\rangle\,|^2 = \frac{1}{4}$$

$$Proba[-|\psi_3] = |\,\langle\psi_3|{-1_z}\rangle\,|^2 = \left|\frac{\sqrt{3}}{2}\right|^2 = \frac{3}{4}$$

Ejercicios

- Calcula los resultados para una medida de $\sigma^y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$.

  Diagonalizar σ^y

  $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \pm\frac{i}{\sqrt{2}} \end{pmatrix}$ son vectores propios:

  - $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix} = \dfrac{1}{\sqrt{2}}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 \\ i \end{pmatrix} = \dfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}$
  - $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} \end{pmatrix} = \dfrac{1}{\sqrt{2}}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -i \end{pmatrix} = \dfrac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ i \end{pmatrix} = -\dfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}$

  $|{\pm 1_y}\rangle \equiv \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \pm\frac{i}{\sqrt{2}} \end{pmatrix}$ es autovector con autovalor ± 1.

  Usando los postulados la probabilidad de encontrar el resultado $+1$ para un sistema preparado en estado $|\psi(\theta)\rangle$ si se mide σ^y:

$$|\langle\psi(\theta)|{+1_y}\rangle|^2 = \left|\frac{1}{\sqrt{2}}\underbrace{\langle +1_y|+1_y\rangle}_{1} + \frac{e^{-i\theta}}{\sqrt{2}}\underbrace{\langle -1_y|+1_y\rangle}_{0}\right|^2 = \frac{1}{2}$$

Para el resultado -1:

$$Pr[-1_y|\theta] = |\langle\psi(\theta)|-1y\rangle|^2 = \left|\frac{1}{\sqrt{2}}\underbrace{\langle +1_y|-1_y\rangle}_{0} + \frac{e^{-i\theta}}{\sqrt{2}}\underbrace{\langle -1_y|-1_y\rangle}_{1}\right|^2 = \left|\frac{e^{-i\theta}}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

$\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$. $\langle +1_y|-1_y\rangle = \left\langle \frac{1}{\sqrt{2}}(1,i)\middle|\frac{1}{\sqrt{2}}(1,-i)\right\rangle$ (al transformarse un *ket* en un *bra* las componentes se conyugan) $= \frac{1}{2}(1,-i)\begin{pmatrix}1\\-i\end{pmatrix} = \frac{1}{2}(1+i^2) = 0.$

$$\langle +1_y|\psi(\theta)\rangle = \left\langle \frac{1}{\sqrt{2}}(1,i), \frac{1}{\sqrt{2}}\left(1,e^{i\theta}\right)\right\rangle = \frac{1}{2}\begin{pmatrix}1 & -i\end{pmatrix}\begin{pmatrix}1\\ e^{i\theta}\end{pmatrix} = \frac{1}{2}\left(1-ie^{i\theta}\right)$$

$$Proba[+1_y|\psi(\theta)] = \left|\frac{1}{2}\begin{pmatrix}1 & -i\end{pmatrix}\begin{pmatrix}1\\ e^{i\theta}\end{pmatrix}\right|^2 = \frac{1}{4}\left|1-ie^{i\theta}\right|^2 \text{ ¡Depende de } \theta!$$

$$Proba[-1_y|\psi(\theta)] = \left|\frac{1}{2}\begin{pmatrix}1 & i\end{pmatrix}\begin{pmatrix}1\\ e^{i\theta}\end{pmatrix}\right|^2 = \frac{1}{4}\left|1+ie^{i\theta}\right|^2$$

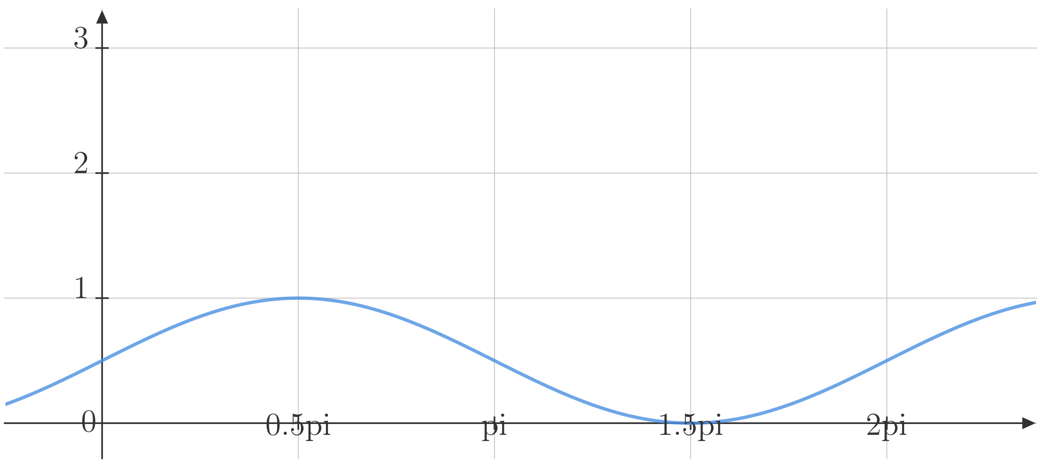
- Considera $|\psi(\theta)\rangle = \frac{1}{\sqrt{2}}|+1_y\rangle + \frac{e^{i\theta}}{\sqrt{2}}|-1_y\rangle$.

  $Probabilidad[+1_y|\phi_\theta] = \frac{1}{4}\left|1-ie^{i\theta}\right|^2 = \frac{1}{4}\left|1+e^{-i\frac{\pi}{2}}e^{i\theta}\right|^2 = \frac{1}{4}\left|1+e^{i(\theta-\frac{\pi}{2})}\right|^2 =$

  $= \frac{1}{4}\left|1+cos(\theta-\frac{\pi}{2})+i*sin(\theta-\frac{\pi}{2})\right|^2 = \frac{1}{4}\left[\left(1+cos\left(\theta-\frac{\pi}{2}\right)\right)^2 + \left(sin(\theta-\frac{\pi}{2})\right)^2\right] =$

  $= \frac{1}{4}\left[(1+sin\theta)^2 + cos^2\theta\right] = \frac{1}{4}\left[1+\underbrace{sin^2\theta}_{1}+2sin\theta+\underbrace{cos^2\theta}_{1}\right] = \frac{1}{4}\left[2+2sin\theta\right] =$

  $= \frac{1}{2}\left[1+sin\theta\right]^a$



- $Probabilidad[-1_y|\phi(\theta)] = \frac{1}{2}\,|1sin(\theta)|$ (La suma de probabilidades debe ser uno por lo que teniendo en cuenta el ejercicio anterior podemos llegar a esta conclusión.)

[a] Para ver los cálculos relativos a $cos\left(\theta - \frac{\pi}{2}\right)$ y $sin\left(\theta - \frac{\pi}{2}\right)$ puede ver el anexo 7.7.1

3.9. Valores medios, varianza y principio de incertidumbre de Heisenberg

Sea X observable con valores propios para $\lambda_1, \ldots, \lambda_n$. Si medimos X repetidamente en un estado $|\psi\rangle$ el valor medio de X será:

$$< X >_\psi \equiv \sum_{\text{v. posibles}} Proba(valor) * valor = \sum_{j=1}^{n} Proba[\lambda_j|\psi]\lambda_j = \sum_{j=1}^{n} \langle\psi| \sqcap_{\lambda_j} |\psi\rangle\, \lambda_j$$

Observación. $X = \sum_j \lambda_j \sqcap_{\lambda_j} \Rightarrow < X >_\psi \langle\psi| X |\psi\rangle$

Lemma $(Xa.a. \Rightarrow X^2 a.a.)$**.** $(X^2)^* = (XX)^*$ y vimos que $(AB)^* = B^* A^* \Rightarrow (X^2)^* = X^* X^* = X^2$

Definimos la varianza como $var(X)_\psi \equiv < X^2 > - < X >^2 = \langle\psi| X^2 |\psi\rangle - \langle\psi| X |\psi\rangle^2$

Definición. El conmutador de 2 operadores X, Y se define como $[X, Y] = XY - YX$.

Sean X, Y observables actuando sobre un *ket* arbitrario $|\psi\rangle$. Consideremos la familia de estados $|\psi(\lambda)\rangle = (X + i\lambda Y)\,|\psi\rangle$ donde $\lambda \in \mathbb{R}$.
Por definición del producto escalar $\langle\phi(\lambda)|\phi(\lambda)\rangle \geq 0 \Rightarrow \langle\psi|\,(X - i\lambda Y)(X + i\lambda Y)\,|\psi\rangle \geq 0 \Rightarrow \langle\psi|\,[X^2 + i\lambda XY - i\lambda YX + \lambda^2 Y^2]\,|\psi\rangle \geq 0 \Leftrightarrow \langle\psi| Y^2 |\psi\rangle\,\lambda^2 + i\,\langle\psi|\,[X, Y]\,|\psi\rangle\,\lambda + \langle\psi| X^2 |\psi\rangle \geq 0$ donde $\forall\lambda \in \mathbb{R}$.

Recordatorio. $ax^2 + bx + c \geq 0 \Rightarrow b^2 - 4ac \leq 0$ donde $\forall x \in \mathbb{R}$. Aplicando este hecho aquí:

- a=$\langle\psi| Y^2 |\psi\rangle$

- b=$i \langle\psi| [X,Y] |\psi\rangle$
- c=$\langle\psi| X^2 |\psi\rangle$

$\Rightarrow |\langle\psi| [X,Y] |\psi\rangle|^2 - 4\langle\psi| X^2 |\psi\rangle \langle\psi| Y^2 |\psi\rangle \leq 0$ donde $\forall$ observable X, Y.
En particular consideramos:

- $X' = X- <X> \mathbb{1}$
- $Y' = Y- <Y> \mathbb{1}$

Se verifica que

- $[X,Y] = [X',Y']$
- $\langle\psi| X'^2 |\psi\rangle = \langle\psi| X^2 |\psi\rangle - \langle\psi| X |\psi\rangle^2 = var(X)$
- $\langle\psi| Y'^2 |\psi\rangle = \langle\psi| Y^2 |\psi\rangle - \langle\psi| Y |\psi\rangle^2 = var(Y)$

$\Rightarrow |\langle\psi| [X',Y'] |\psi\rangle|^2 - 4\langle\psi| X'^2 |\psi\rangle \langle\psi| Y'^2 |\psi\rangle \leq 0 \Rightarrow |\langle\psi| [X,Y] |\psi\rangle|^2 - 4var(X)var(Y) \leq 0 \Rightarrow var(X)var(Y) \geq \frac{1}{4}|\langle\psi| [X,Y] |\psi\rangle|^2$ (principio de incertidumbre de Heisenberg).

Ejercicio

$$\sigma^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma^y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Calcula $[\sigma^\alpha, \sigma^\beta]$ donde $\alpha, \beta \in \{x,y,z\}$.

3.10. Ecuación Schrödinger y unitaria

Schrödinger: $\mathcal{H} |\psi(t)\rangle = i\hbar\partial_k |\psi(t)\rangle$.
Esta ecuación es lineal en $|\psi(t)\rangle \underbrace{\Rightarrow}_{(EDO)} \exists$ operador $\mathcal{U}(t,t_0)$ tal que $|\psi(t)\rangle = \mathcal{U}(t,t_0)|\psi(t_0)\rangle$ donde $t_0 \equiv$ instante inicial. ¿Como vería (el cuadrado de) la norma de $|\psi(t)\rangle$ con el tiempo?

$$\frac{d}{dt}[\langle\psi(t)|\psi(t)\rangle|] = \underbrace{\left[\frac{d}{dt}\langle\psi(t)|\right]}_{-\frac{1}{i\hbar}\langle\psi(t)|\mathcal{H}^* \ (\mathcal{H}=\mathcal{H}^*)} |\psi(t)\rangle + \langle\psi(t)| \underbrace{\left[\frac{d}{dt}|\psi(t)\rangle\right]}_{\frac{1}{i\hbar}\mathcal{H}|\psi(t)\rangle} =$$

$$= -\frac{1}{i\hbar}\langle\psi(t)|\,\mathcal{H}\,|\psi(t)\rangle + \frac{1}{i\hbar}\langle\psi(t)|\,\mathcal{H}\,|\psi(t)\rangle = 0,\ \langle\psi(t)|\psi(t)\rangle \text{ es invariante.}$$

Se puede demostrar (álgebra) que si un operador lineal $\wedge\colon V \to V$ satisface $\langle v|\wedge|v\rangle = \langle v|v\rangle$ donde $\forall\,|v\rangle \in V$, entonces $\wedge = \mathbb{1}$.

$$\langle\psi(t_0)|\,\mathcal{U}(t,t_0)^*\mathcal{U}(t,t_0)\,|\psi(t_0)\rangle = \langle\psi(t_0)|\psi(t_0)\rangle$$

$$\mathcal{U}(t,t_0)^*\mathcal{U}(t,t_0) = \mathbb{1}$$

$\mathcal{U}(t_0,t)$ es unitaria.

Las evoluciones temporales en mecánica cuántica se describen por operadores unitarios.

3.11. Sistemas de partículas

Sean V_1 y V_2 EV (sobre $\mathbb{C}$). Definimos el producto tensorial de V_1 y V_2 ($V_1 \otimes V_2$) como el conjunto linealmente generado por pares de vectores $|v_1\rangle \in V_1$, $|v_2\rangle \in V_2$, es decir, $V_1 \otimes V_2$ se define por las siguientes reglas:

(1) $|v_1\rangle \in V_1$, $|v_2\rangle \in V_2$ entonces el par, denotado por $|v_1\rangle \otimes |v_2\rangle$ o $|v_1, v_2\rangle$ pertenece a $V_1 \otimes V_2$ (el producto cartesiano V_1xV_2 está incluido en $V_1 \otimes V_2$).

(2) Si $|w\rangle$, $|w'\rangle \in V_1 \otimes V_2$, entonces $\forall\alpha,\beta \in \mathbb{C}$, $\alpha\,|w\rangle + \beta\,|w'\rangle \in V_1 \otimes V_2$.

Teorema. $V_1 \otimes V_2$ es un EV.

Teorema. Sean V_1, V_2, V_3 EV, $(V_1 \otimes V_2) \otimes V_3 = V_1 \otimes (V_2 \otimes V_3)$

Sean $p_1, p_2, \ldots, p_n$ partículas descritas respectivamente por el EV $V_1, V_2, \ldots, V_n$. El sistema total está descrito por el EV $V_{tot} = V_1 \otimes \cdots \otimes V_n$.

Los elementos de $V_1 \otimes V_2 \otimes V_n$ de la forma $|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_n\rangle$ se denotan estados productos.

Definición. Un estado es entrelazado (*entangled*) si no es producto.

Ejemplo

$V_1 = V_2 = \mathbb{C}^2$

Sea $B = \{|0\rangle, |1\rangle\}$ base ortonormal de $\mathbb{C}^2$, ¿cuales de los siguientes estados son productos o entrelazado (*entangled*)?

- $|0\rangle \otimes |0\rangle$ (Producto)
- $\frac{1}{\sqrt{2}} |0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \otimes |1\rangle$ (Entrelazado maximalmente)
- $\frac{1}{\sqrt{2}} |0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} |0\rangle \otimes |1\rangle$ (Producto)

Teorema. Sea $\begin{cases} B_1 \equiv \left\{ \left| e_j^{(1)} \right\rangle ; j = 1, \dots, d_1 \right\} \text{ es base de EV } V_1 \\ B_2 \equiv \left\{ \left| e_j^{(2)} \right\rangle ; j = 1, \dots, d_2 \right\} \text{ es base de EV } V_2 \end{cases}$ por lo que $B = \left\{ \left| e_i^{(1)} \right\rangle \left| e_j^{(2)} \right\rangle ; i = 1, \dots, d_1, j = 1, \dots, d_2 \right\}$ es base de $V_1 \otimes V_2$. Si B_1 y B_2 son ortonormales entonces B es ortonormal.

Definición. Sean $|\psi_1, \psi_2\rangle$, $|\phi_1, \phi_2\rangle$ estados productos de $V_1 \otimes V_2$. El producto escalar $\langle \psi_1, \psi_2 | \phi_1, \phi_2 \rangle \equiv \langle \psi_1 | \phi_1 \rangle \text{ x } \langle \psi_2 | \phi_2 \rangle$ se demuestra fácilmente que está bien definido. Esta definición se extiende a todo $V_1 \otimes V_2$ por linealidad.

Ejercicios

- Calcular $\langle \psi | \phi \rangle$ en los siguientes casos:

$\|\psi\rangle$	$\|\phi\rangle$	$\langle \psi\|\phi \rangle$
$\|0,0\rangle$	$\|0,0\rangle$	1
$\|0,0\rangle$	$\|1,1\rangle$	0
$\|0,0\rangle$	$\frac{1}{\sqrt{2}}\|0,0\rangle + \frac{1}{\sqrt{2}}\|1,1\rangle$	$\frac{1}{\sqrt{2}}$
$\frac{1}{\sqrt{2}}\|0,0\rangle + \frac{1}{\sqrt{2}}\|1,1\rangle$	$\frac{1}{\sqrt{2}}\|0,0\rangle + \frac{1}{\sqrt{2}}\|1,1\rangle$	1[a]

- $|\psi\rangle = \frac{1}{\sqrt{2}} |0,1\rangle + \frac{i}{\sqrt{2}} |1,0\rangle$, $|\phi\rangle = \frac{1}{\sqrt{2}} |0,1\rangle + \frac{1}{\sqrt{2}} |1,0\rangle$

$$\begin{aligned} \langle \psi | \phi \rangle &= \left[\frac{1}{\sqrt{2}} \langle 0,1| - \frac{i}{\sqrt{2}} \langle 1,0| \right] \left[\frac{1}{\sqrt{2}} |0,1\rangle + \frac{1}{\sqrt{2}} |1,0\rangle \right] = \\ &= \left(\frac{1}{\sqrt{2}} \right)^2 \{1 + 0 + 0 - i\} = \frac{1-i}{2} \end{aligned}$$

[a] Para ver los cálculos ver el anexo 7.8.

Sean A_1, A_2 operadores actuando sobre EV V_1, V_2 respectivamente y sean $|\psi_1\rangle$, $|\psi_2\rangle$ elementos de V_1, V_2 respectivamente. Definimos el producto tensorial $A_1 \otimes A_2$ sobre $|\psi_1\rangle \otimes |\psi_2\rangle$ como $[A_1 \otimes A_2] |\psi_1, \psi_2\rangle = A_1 |\psi_1\rangle \otimes A_2 |\psi_2\rangle$.

Esta acción de $A_1 \otimes A_2$ se extiende a todo $V_1 \otimes V_2$ por linealidad. Sea V_1', V_2' EV de operadores lineales actuando sobre V_1 y V_2 respectivamente.

Teorema. $(V_1 \otimes V_2)' = V_1' \otimes V_2'$

Tema 4

Qubits, puertas y circuitos cuánticos

4.1. El qubit

Definición. Un qubit es un sistema cuántico descrito por un EV de dimensiones igual a 2: $V_{qubit} \equiv \mathbb{C}$.

Sea $B = \{|0\rangle, |1\rangle\}$ una base $\perp^{mal}$ de $\mathbb{C}^2$. Los estados de un qubit son vectores de $\mathbb{C}^2$ con norma 1:

$$\left\{\alpha |0\rangle + \beta |1\rangle ; |\alpha|^2 + |\beta|^2 = 1\right\}$$

Vimos que en la descripción de un sistema cuántico en una base dada las fases globales no importan.

$\forall x \in \mathbb{R}, \alpha |0\rangle + \beta |1\rangle$ y $e^{ix}\alpha |0\rangle + e^{ix}\beta |1\rangle$ representan el mismo estado $\Rightarrow$ se puede decir que $0 \leq \alpha$.
¿Por qué? Sea una descripción $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ donde $\alpha, \beta \in \mathbb{C}$. $\alpha \in \mathbb{C} \Leftrightarrow \exists \delta \geq 0, \mu \in \mathbb{R}$ tal que $\alpha = \delta e^{i\mu}$. Ya basta con elegir $\chi = -\mu$. El mismo estado se describe por el vector $|\alpha| |0\rangle + e^{-i\mu}\beta |1\rangle$.

$0 \leq \alpha \in \mathbb{R}$, $|\alpha|^2 + |\beta|^2 = 1$
Una manera de parametrizar este conjunto es:

$$\alpha \equiv cos\left(\frac{\theta}{2}\right) \qquad \begin{matrix} 0 \leq \theta \leq \pi \\ \text{(ángulo con vertical)} \end{matrix}$$
$$\beta \equiv e^{i\phi} sin\left(\frac{\theta}{2}\right) \qquad \begin{matrix} 0 \leq \psi \leq 2\pi \\ \text{(ángulo en ecuador)} \end{matrix}$$

Con esta parametrización cada estado está en correspondencia con la superficie de una esfera.

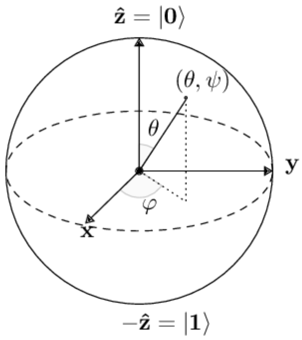


Figura 4.1: Esfera de Bloch para representar el estado de un qubit

Ejemplos de observable

$$\sigma^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma^y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

4.2. Puertas cuánticas

Se puede ver que las siguientes puertas son unitarias:

- σ^x, σ^y, σ^z (a menudo denotadas X, Y, Z)
- $\mathcal{S} \equiv \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \sqrt{\sigma^z}$
- $\mathcal{T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$ ($\frac{\pi}{8}$ phase gate).
- Rotaciones

  $R_x(\theta) = e^{-i\theta\frac{\sigma^x}{2}} = \begin{pmatrix} cos\left(\frac{\theta}{2}\right) & -isin\left(\frac{\theta}{2}\right) \\ -isin\left(\frac{\theta}{2}\right) & cos\left(\frac{\theta}{2}\right) \end{pmatrix}$, $R_y(\theta) = e^{-i\theta\frac{\sigma^y}{2}} = \begin{pmatrix} cos\left(\frac{\theta}{2}\right) & -isin\left(\frac{\theta}{2}\right) \\ sin\left(\frac{\theta}{2}\right) & cos\left(\frac{\theta}{2}\right) \end{pmatrix}$

  $R_z(\theta) = e^{-i\theta\frac{\sigma^z}{2}} = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{-i\frac{\theta}{2}} \end{pmatrix}$

4.2.1. Exponencial de una matriz cuadrada

$$e^A \underbrace{\equiv}_{Taylot} \sum_{k=0}^{\infty} \frac{A^k}{k!}$$

Las matrices de Pauli satisfacen: $(\sigma^x)^2 = (\sigma^y)^2 = (\sigma^z)^2 = \mathbb{1}$

$$R_x(\theta) = \sum_{k=0}^{\infty} \frac{1}{k!}\left(-i\frac{\theta}{2}\sigma^x\right)^k = \sum_{\text{k par}} \frac{1}{k!}\underbrace{\left(-i\frac{\theta}{2}\sigma^x\right)^k}_{\left(\frac{i\theta}{2}\right)^k \underbrace{(\sigma^x)^k}_{\mathbb{1}}} + \sum_{\text{k impar}} \frac{1}{k!}\underbrace{\left(-i\frac{\theta}{2}\sigma^x\right)^k}_{\left(-\frac{i\theta}{2}\right)^k \underbrace{(\sigma^x)^k}_{\sigma^x}}$$

$$= \underbrace{\sum_{\text{k par}} \frac{\left(-\frac{i\theta}{2}\right)^k}{k!}}_{cos\left(\frac{\theta}{2}\right)} \mathbb{1} + \underbrace{\sum_{\text{k impar}} \frac{\left(-\frac{i\theta}{2}\right)^k}{k!}}_{-isin\left(\frac{\theta}{2}\right)} \sigma^x = cos\left(\frac{\theta}{2}\right)\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - isin\left(\frac{\theta}{2}\right)\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

Veremos (sin demo?) que $\forall$ unitaria de n qubits se puede descomponer en unitarias de 2 qubits y unitarias de 1 qubit (en principio necesitamos poder implementar cualquier unitaria a un qubit).

Sin embargo, nos gustaria poder expresar $\forall$ unitaria usando sólo un número finito de unitarias.

Sea $U(1) \equiv \{e^{i\phi}\mathbb{1}; 0 \leq \phi \leq 2\pi\}$, $U(2) \equiv$ unitarias 2*2 y $SU(2) \subseteq U(2) \equiv$ unitarias $2 * 2$ con determinantes= 1.

Teorema. $U(2) = U(1)$ x $SU(2)$ donde $U(1)$ son fases globales (no físicas).

Definiciones.

- Sea $\mathcal{S} \equiv$ conjunto finito de $SU(2)$ que contiene todos sus inversos; $u \in \mathcal{S} \Leftrightarrow u^* \in \mathcal{S}$.
- $\mathcal{S}_l \equiv \{u_1, \ldots, u_l; u_j \in \mathcal{S}, j = 1, \ldots, l\} \equiv$ "palabras" de longitud l con "letras" en $\mathcal{S}$.
- $< \mathcal{S} >= U_{l=1}^{\infty}\mathcal{S}_l$
- Distancia entre 2 matrices: $D(A, B) \equiv \overbrace{tr}^{traza} \sqrt{(A^* - B^*)(A - B)}$

- $\mathcal{S} \subseteq SU(2)$ es <u>denso</u> si $\forall v \in SU(2)$, $\forall \varepsilon > 0$, $\exists u \in \mathcal{S}$ tal que $D(u, v) < \varepsilon$.
- K es una ε-red para $SU(2)$ si $\forall \varepsilon > 0$, $\forall u \in SU(2)$, $\exists w \in K$ tal que $D(u, w) < \varepsilon$.

Teorema (Solovay–Kitaev). Si $< \varphi >$ es denso en $SU(2)$, entonces φ_l es una ε-red para $l = \mathcal{O}\left(\left[log\left(\frac{1}{\varepsilon}\right)\right]^c\right)$ donde $c \simeq 4$.
Ejemplo de una *gate set* universal: $\varphi = \{H, T^{\frac{1}{2}}\}$

4.2.2. Puerta de Hadamard

$H = \dfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ en la base $B \equiv \{|0\rangle, |1\rangle\}$

Ejercicio

- ¿H unitaria?
- Representar $\mathcal{H}|0\rangle$, $\mathcal{H}(1)$ en la esfera de Bloch.
  $\mathcal{H}|0\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\mathcal{H}|1\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
  $|\psi(\theta, \varphi)\rangle = cos\left(\dfrac{\theta}{2}\right)|0\rangle + e^{i\varphi} sin\left(\dfrac{\theta}{2}\right)|1\rangle$

4.2.3. Puertas a 2 qubits

Como en computación clásica, nada interesante si nos limitamos a operaciones de 1 qubit. Queremos interacciones que crean (o destruyen) correlaciones. La manera más simple es usando puertas a 2 qubits.

Definición. Una puerta de 2 qubits es una unitaria actuando sobre $\mathbb{C}^2 \otimes \mathbb{C}^2$ que <u>no</u> sea de la forma $\mathcal{U} = \mathcal{U}_1 \otimes \mathcal{U}_2$.

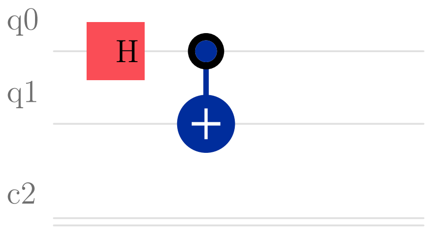
Ejemplo

Sea $B = \{|0\rangle, |1\rangle\}$; base $\perp^{mal}$ de $\mathbb{C}^2$.

CNOT: $|a, b\rangle \to \left|\underbrace{a}_{control}, \underbrace{b \oplus a}_{target}\right\rangle$ ($\oplus$: suma mod 2) en la base B.

IN	OUT
$\|0,0\rangle$	$\|0,0\rangle$
$\|0,1\rangle$	$\|0,1\rangle$
$\|1,0\rangle$	$\|1,1\rangle$
$\|1,1\rangle$	$\|1,0\rangle$

Ejercicios



- Hadamard:
  $(\mathcal{H}_1 \otimes \mathbb{1})\,|0\rangle \otimes |0\rangle = \mathcal{H}\,|0\rangle_1 \otimes |0\rangle_2 = \left(\frac{1}{\sqrt{2}}\,|0\rangle_1 + \frac{1}{\sqrt{2}}\,|1\rangle_1\right) \otimes |0\rangle_2$ (producto)

  CNOT:
  $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle = \frac{1}{\sqrt{2}}\,|0\rangle\otimes|0\rangle+\frac{1}{\sqrt{2}}\,|1\rangle\otimes|0\rangle = CNOT\left(\frac{1}{\sqrt{2}}\,|0,0\rangle + \frac{1}{\sqrt{2}}\,|1,0\rangle\right) =$
  $= \frac{1}{\sqrt{2}}CNOT\,|0,0\rangle + \frac{1}{\sqrt{2}}CNOT\,|1,0\rangle = \frac{1}{\sqrt{2}}\,|0,0\rangle + \frac{1}{\sqrt{2}}\,|1,1\rangle$ (entrelazado maximalmente)

- $q0 \equiv |i\rangle$ y $q1 \equiv |j\rangle$
  $\frac{1}{\sqrt{2}}\left(|0,j\rangle + (-)^i\,|1, 1+j \mod 2\rangle\right)$ donde $i,j \in \{0,1\}$.

  $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ en la base computacional.

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

  (1) Input= $|0,0\rangle$, out= $\frac{1}{\sqrt{2}}\underbrace{(|0,0\rangle + |1,1\rangle)}_{|\phi\rangle^+}$ (semana pasada)

  (2) Input= $|1,0\rangle$, out= $[\mathcal{H} \otimes \mathbb{1}]\,|1,0\rangle = \mathcal{H}\,|1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle =$

$$\frac{1}{\sqrt{2}}(|0,0\rangle - |1,0\rangle) \Rightarrow CNOT[\mathcal{H}\otimes\mathbb{1}]\,|1,0\rangle = CNOT\left\{\frac{1}{\sqrt{2}}\,|0,0\rangle - |1,0\rangle\right\} =$$

$$\underbrace{=}_{linealidad} \frac{1}{\sqrt{2}}\underbrace{CNOT\,|0,0\rangle}_{|0,0\rangle} - \frac{1}{\sqrt{2}}\underbrace{CNOT\,|1,0\rangle}_{|1,1\rangle} = \frac{1}{\sqrt{2}}(\underbrace{|0,0\rangle - |1,1\rangle}_{|\phi^-\rangle})$$

(3) Input= $|0,1\rangle$, output= $\frac{1}{\sqrt{2}}(\underbrace{|0,1\rangle + |1,0\rangle}_{|\psi^+\rangle})$

(4) Input= $|1,1\rangle$, output= $\frac{1}{\sqrt{2}}(\underbrace{|0,1\rangle - |1,0\rangle}_{|\psi^-\rangle})$

Los 4 estados $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$, $|\psi^-\rangle$ se conocen como estados de Bell a 2 qubits.

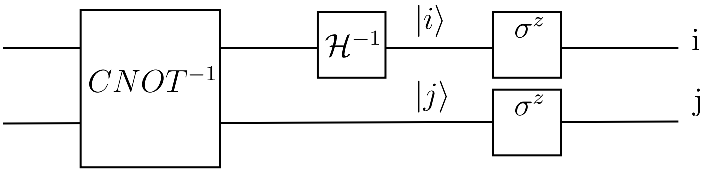
Para hacer un medida, en esta base, cogemos el circuito de arriba pero al revés:

$$\begin{pmatrix} \langle\phi^+|\phi^+\rangle & \langle\phi^+|\phi^-\rangle & \langle\phi^+|\psi^+\rangle & \langle\phi^+|\psi^-\rangle \\ \langle\phi^-|\phi^+\rangle & \langle\phi^-|\phi^-\rangle & \langle\phi^-|\psi^+\rangle & \langle\phi^-|\psi^-\rangle \\ \langle\psi^+|\phi^+\rangle & \langle\psi^+|\phi^-\rangle & \langle\psi^+|\psi^+\rangle & \langle\psi^+|\psi^-\rangle \\ \langle\psi^-|\phi^+\rangle & \langle\psi^-|\phi^-\rangle & \langle\psi^-|\psi^+\rangle & \langle\psi^-|\psi^-\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{aligned} \left\langle\phi^+\middle|\phi^+\right\rangle &= \frac{1}{\sqrt{2}}[\langle 0,0| + \langle 1,1|]\frac{1}{\sqrt{2}}[|0,0\rangle + |1,1\rangle] = \\ &= \frac{1}{\sqrt{2}}\left[\underbrace{\langle 0,0|0,0\rangle}_{1} + \underbrace{\langle 0,0|1,1\rangle}_{(<0,1>)^2=0} + \underbrace{\langle 1,1|0,0\rangle}_{0} + \underbrace{\langle 1,1|1,1\rangle}_{1}\right] = \\ &= 1 \end{aligned}$$

El producto escalar entre $\mathcal{U}\,|i,j\rangle$ y $\mathcal{U}\,|k,l\rangle$ es $\langle i,j|\underbrace{\mathcal{U}^*\mathcal{U}}_{\mathbb{1}}|k,l\rangle = \langle i,j|k,l\rangle = \langle i|k\rangle\,\langle j|l\rangle = \mathcal{S}_{i,k}\mathcal{S}_{j,l} \Rightarrow |\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$, $|\psi^-\rangle$ forman una base de EV de 2 qubits, $\mathbb{C}^2\otimes\mathbb{C}^2$

Ejercicio



$$\underbrace{\frac{1}{\sqrt{2}}(|o,j\rangle + (-)^i\,|1,1\oplus j\rangle)}_{\text{Estados de Bell}}$$

- $(CNOT)^2 = \mathbb{1}\otimes\mathbb{1} \Rightarrow CNOT = CNOT^{-1}$

  $\mathcal{H}^2 = \mathbb{1} \Rightarrow \mathcal{H} = \mathcal{H}^{-1}$

Expresan:

$$|0,0\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle) = \left[\frac{1}{\sqrt{2}}|\phi^+\rangle_{AB} + \frac{1}{\sqrt{2}}|\phi^-\rangle_{AB}\right]\frac{\alpha}{\sqrt{2}}|0\rangle_c$$
$$|0,1\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle) + \left[\frac{1}{\sqrt{2}}|\psi^+\rangle_{AB} + \frac{1}{\sqrt{2}}|\psi^-\rangle_{AB}\right]\frac{\alpha}{\sqrt{2}}|1\rangle_c$$
$$|1,0\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle) + \left[\frac{1}{\sqrt{2}}|\psi^+\rangle_{AB} - \frac{1}{\sqrt{2}}|\psi^-\rangle_{AB}\right]\frac{\beta}{\sqrt{2}}|0\rangle_c$$
$$|1,1\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle) + \left[\frac{1}{\sqrt{2}}|\phi^+\rangle_{AB} - \frac{1}{\sqrt{2}}|\phi^-\rangle_{AB}\right]\frac{\beta}{\sqrt{2}}|1\rangle_c$$

en la base de Bell:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle) = \frac{1}{2}|\phi^+\rangle_{AB}(\alpha|0\rangle_C + \beta|1\rangle_C)$$
$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle - |1,1\rangle) + \frac{1}{2}|\phi^-\rangle_{AB}(\alpha|0\rangle_C - \beta|1\rangle_C)$$
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0,1\rangle + |1,0\rangle) + \frac{1}{2}|\psi^+\rangle_{AB}(\alpha|1\rangle_C + \beta|0\rangle_C)$$
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0,1\rangle - |1,0\rangle) + \frac{1}{2}|\psi^-\rangle_{AB}(\alpha|1\rangle_C - \beta|0\rangle_C) = \text{input re-expresado.}$$

$$\frac{1}{2}|\phi^+\rangle_{AB}|\psi\rangle_C + \frac{1}{2}|\phi^-\rangle_{AB}\sigma^z|\psi\rangle_C + \frac{1}{2}|\psi^+\rangle_{AB}\sigma^x|\psi\rangle_C + \frac{1}{2}|\psi^-\rangle_{AB}\sigma^x\sigma^z|\psi\rangle_C$$

Observación.

$\sigma^x(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$

$\sigma^z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$

$\sigma^x\sigma^z(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle - \beta|0\rangle$

- Consideramos un sistema de 3 qubits inicialmente en el siguiente estado:

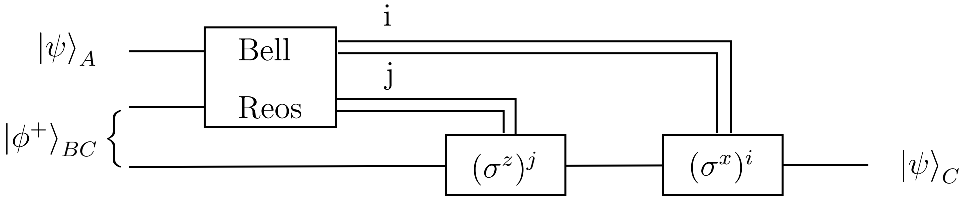
$$\begin{aligned}|\psi\rangle_A|\phi^+\rangle_{BC} &= (\alpha|0\rangle_A + \beta|1\rangle_A)\otimes\frac{1}{\sqrt{2}}(|0,0\rangle_{BC} + |1,1\rangle_{BC}) = \\ &= \frac{\alpha}{\sqrt{2}}|0,0,0\rangle_{ABC} + \frac{\alpha}{\sqrt{2}}|0,1,1\rangle_{ABC} + \frac{\beta}{\sqrt{2}}|1,0,0\rangle_{ABC} + \\ &+ \frac{\beta}{\sqrt{2}}|1,1,1\rangle_{ABC} = \text{ (se puede representar como)} \\ &= |0,0\rangle_{AB}\frac{\alpha}{\sqrt{2}}|0\rangle_C + |0,1\rangle_{AB}\frac{\alpha}{\sqrt{2}}|1\rangle_C + |1,0\rangle_{AB}\frac{\beta}{\sqrt{2}}|0\rangle_C + \\ &+ |1,1\rangle_{AB}\frac{\beta}{\sqrt{2}}|1\rangle_C\end{aligned}$$

Si hacemos una medida de Bell sobre el sistema AB, el sistema total se encuentra inmediatamente después de la medida en uno de los siguientes estados (todos con probabilidad $\frac{1}{4}$):

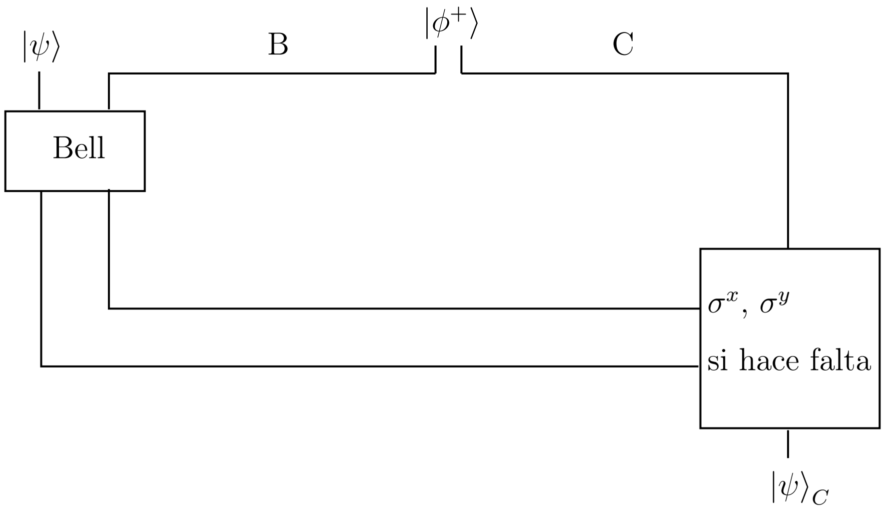
- $|\phi^+\rangle_{AB}\otimes|\psi\rangle_C$

- $|\phi^-\rangle_{AB} \otimes \sigma^z |\psi\rangle_C$
- $|\psi^+\rangle_{AB} \otimes \sigma^x |\psi\rangle_C$
- $|\psi^-\rangle_{AB} \otimes \sigma^x \sigma^z |\psi\rangle_C$

Observación. σ^x, σ^z son unitarios.



Quantum Teleportation



No se necesita conocer $|\psi\rangle$

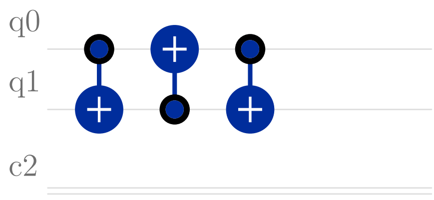
¿Se puede copiar el estado de un sistema cuántico? $\Leftrightarrow$ ¿Existe alguna unitaria $\mathcal{U}_{copy}$ tal que $\mathcal{U}_{copy}\colon \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes V_{aux} \to \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes V_{aux}$?

$|\mathcal{S}\rangle \otimes \underbrace{|\bigcirc\rangle}_{\text{estado en blanco}} \otimes |\mu\rangle_{aux} \to |\mathcal{S}\rangle \otimes |\mathcal{S}\rangle \otimes \left|\mu'_{aux}\right\rangle$ donde $\forall\, |\mathcal{S}\rangle \in \mathbb{C}^2$.

Si fuera posible funcionaria para $|\mathcal{S}\rangle = |0\rangle$ y $|\mathcal{S}\rangle = |1\rangle$.

Para $|\mathcal{S}\rangle = \alpha|0\rangle + \beta|1\rangle$, por linealidad, tendríamos $\alpha\left|0,0,\mu'_{(0)}\right\rangle + \beta\left|1,1,\mu'_{(1)}\right\rangle \neq (\alpha|0\rangle + \beta|1\rangle)^{\otimes 2}\left|\mu'(\alpha|0\rangle + \beta|1\rangle)\right\rangle$

Ejercicio



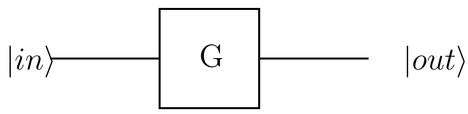
En base computacional $CNOT$: $|i,j\rangle \to |i, j\oplus i\rangle$

$$|i\rangle|j\rangle \overbrace{\to}^{CNOT_{a\to b}} |i, j\oplus i\rangle \overbrace{\to}^{CNOT_{b\to a}} |i\oplus j\oplus i, j\oplus i\rangle = |j, j\otimes i\rangle \overbrace{\to}^{CNOT_{a\to b}} |j, j\oplus i\oplus j\rangle = |j,i\rangle$$

$$|\psi_a\rangle|\psi_b\rangle = \sum_{i=0,1}\psi_i^{(a)}\sum_{j=0,1}\psi_j^{(b)}|i,j\rangle \underbrace{\to}_{linealidad} \sum_{i=0,1}\sum_{j=0,1}\psi_i^{(a)}\psi_j^{(b)}|i,j\rangle = |\psi_b\rangle|\psi_a\rangle$$

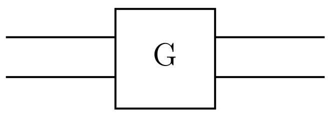
4.3. Notación gráfica

(1) Puertas a 1 qubit se representan con cajitas con 2 patas, una izquierda representando el *input* y una derecha representando el *output*.

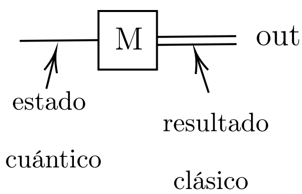


$|out\rangle$ significa $G|in\rangle$

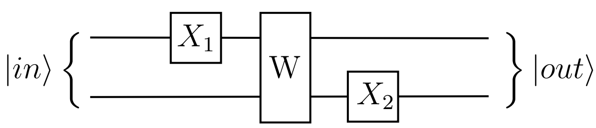
(2) Similarmente, para las puertas a 2 qubits:



(3) Una medida sobre un qubit se representa:



(4) La concatenación de operaciones se representa uniendo puertas:

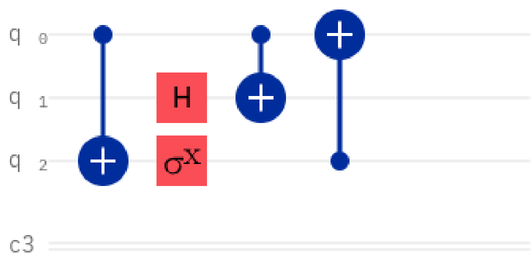


4.4. Circuitos cuánticos

Definición. Un circuito cuántico es cualquier secuencia de unitarios a 1 qubit y 2 qubits $(G_L * G_{L-1} * \cdots * G_1)$ actúan sobre un registro fijo de n qubits.

Ejemplo

$n = 3$



Los postulados de la mecánica cuántica dictan que cualquier evolución tiene que ser unitaria (consecuencia de la ecuación de Schrödinger), pero no dicen si hay posiblemente otras limitaciones que nos impiden realizar cualquier unitaria.

Teorema. Cualquier unitario de n qubits se puede aproximar (en norma ∞) a distancia ε usando puertas $\mathcal{O}\left(n^2 4^n \left[\log\left(n^2 * \frac{4^n}{\varepsilon}\right)\right]^3\right)$.

Las puertas a 1 qubit y 2 qubit permiten explorar todo el EV de n qubits donde $\forall n \in \mathbb{N}_0$.
Demostración (Nielsen & Chuang, p 200).

- <u>Lo bueno</u>: $\exists$ conjuntos de puertas universales para explorar todo $(\mathcal{C}^2)^{\otimes n}$. Esos conjuntos pueden ser reducidos.

  Ejemplo

  $$\left\{ CNOT, \mathcal{H}, \underbrace{T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}}_{\frac{\pi}{8}-gate} \right\}$$

- <u>Lo malo</u>: para algunas unitarias el número de puertas crece exponencialmente con

n. Sin embargo, se puede ver que esas unitarias no son "naturales" (ver más adelante si hay tiempo).

- Lo bello: $\exists$ circuitos con un número puertas polinómico en el tamaño del *input* n que ofrece poder computacional sin equivalente clásico.

4.5. Clases de complejidad (informalmente)

Problema. Estudiar familias de problemas cuyos miembros pueden tener tamaños distintos.

Ejemplo

m-SAT:

Se da una fórmula involucrando n bits (no qubits) $b_1, \ldots, b_n$: el AND de cláusulas que involucran m bits como mucho cada una. Por ejemplo:

- $m = 2 \rightarrow (b_1 \vee b_2) \wedge (b_1 \vee \tilde{b}_3) \wedge \ldots$
- $m = 3 \rightarrow (b_1 \vee (b_5 \wedge b_7)) \wedge (b_2 \wedge (b_4 \vee \tilde{b}_3)) \wedge \ldots$

¿$\exists$ asignación que satisfaga todas las cláusulas?

Definición. $P \equiv \{\}$ problemas resolubles con circuitos cuyo número de puertas crece polinómicamente con el tamaño del *input*. Por ejemplo: multiplicación entera, "primality test" (2004).

Definición. $NP \equiv \{\}$ problemas (de decisión) para los cuales una solución se puede verificar con un circuito cuyo tamaño crece polinómicamente con el tamaño del *input*. Por ejemplo, 3-SAT, factorización.

Definición. BQP (*Bounded quantium polynomial*) $\equiv$ quasi análogo cuántico a P.

$$Factorizacin \in BQP \Rightarrow BQP \cap NP \neq \phi$$

Sin embargo, se cree que $NP \nsubseteq BQP$. Por ejemplo, se cree que 3-SAT también es difícil para un ordenador cuántico.

Definición. QMA (*Quantum Merlin-Arthur*) $\equiv$ quasi V_{anlogo} cuántico de NP.

Dada una clase de complejidad X, una familia de problemas F es $X - hard$ si disponiendo de un oráculo proporcionando soluciones a problemas de F, se puede resolver cualquier problema de X con coste adicional (*ovehead*) polinómico en el tamaño del problema/*input*.

Teorema (Cook). Una tal familia F es $X - compleja$ si F es $X - hard$ y $F \in X$. Por ejemplo, 3-SAT es $NP - complejo$.

Teorema. Estimar la amplitud de transición $(\langle\phi_0| \times |\phi_0\rangle)$ *vacuum-vacuum* de una teoría de campos masiva en $1+1$ dimensiones, en presencia de fuentes que varían en posición y con el tiempo es $BQP - hard$.

4.6. Periodicidad

Consideramos una función $f : \{0, 1, \ldots, 2^n - 1\} \to \{0, 1, \ldots, 2^n - 1\}$. Tenemos la promesa de que f es periódica. Dado $x \in \{0, 1, \ldots, 2^n - 1\}$, $x + r < 2^r$ por lo que $f(x + r) = f(x)$ para algún periodo r.

Hipótesis. El entorno r más pequeño que vuelva f periódica es tal que:

$$\underbrace{1 << r}_{\substack{\text{para volver}\\ \text{la situación}\\ \text{interesante}}} < \underbrace{2^{\frac{n}{2}}}_{\substack{\text{para usar un}\\ \text{resultado técnico}\\ \text{más adelante}}}$$

El problema reside en determinar r.

Clásicamente muy difícil, no se conoce ningún algoritmo clásico operando en tiempo polinómico en n que realice esta tarea.

Clásicamente, el teorema de Shannon indica como proceder:

- *Sampling* (Superposición cuántica de *inputs*)
- Transformada de Fourier sobe datos (Transformada de Fourier cuántica)

4.6.1. QFT

Opera como la Transformada de Fourier (TF) clásica pero sobre elementos de la base computacional en lugar de datos.

Sea $\{|0\rangle, \ldots, |N-1\rangle\}$ base ortonormal de un EV V_N. En esta base,

$$QFT; V_N \to V_N : |x\rangle \to \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i y x/N} |y\rangle$$

$$|\psi\rangle \to QFT \to QFT |\psi\rangle$$

Ejercicio

Demuestra que QFT es unitaria.

$$\begin{array}{lcl} \text{QFT}^* \text{ QFT}=\mathbb{1} & & \text{Operadores} \\ \Updownarrow & & \\ \underbrace{\langle m| QFT^* QFT |j\rangle}_{\langle m|QFT^* \mathbb{1} QFT|j\rangle} = \underbrace{\langle m| \mathbb{1} |j\rangle}_{\mathcal{S}_{ij}} = & & \text{Matrices } \forall i, j = 0, \ldots, N-1 \end{array}$$

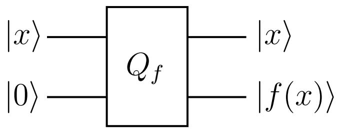
$$= \langle m| QFT^* \sum_{k=0}^{N-1} |K\mathrm{x}K| QFT |j\rangle = \mathcal{S}_{ij} \Leftrightarrow \sum_{k=0}^{N-1} \langle m| QFT^* |k\rangle \langle k| QFT |j\rangle = \mathcal{S}_{ij}$$

$$\langle k| QFT |j\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i j y/N} \underbrace{\langle k|y\rangle}_{\substack{\delta_{ky} \\ \text{(base ortonormal)}}} = \frac{1}{\sqrt{N}} e^{2\pi i j k/N}$$

$$\langle m| QFT^* |k\rangle = \overline{\langle k| QFT |m\rangle} = \frac{1}{\sqrt{N}} e^{-2\pi i m k/N}$$

$$\underbrace{\frac{1}{N}\sum_{k=0}^{N-1} e^{2\pi i(j-m)k/N}}_{\langle m|QFT^{*}QFT|j\rangle} = S_{mj}$$

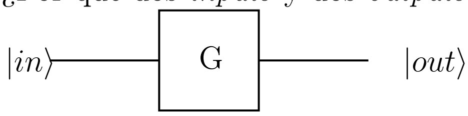
Volviendo a la función f cuyo periodo queremos determinar. Suponiendo que tenemos acceso a un oráculo, es decir, una aja Q_f actuando en la base canónica como



Supondremos que Q_f tiene una profundidad polinómica en n y m. Hay ejemplos de función interesantes en los cuáles esta hipótesis se cumple.

Ejercicio

¿Por qué dos *inputs* y dos *outputs*? ¿Por qué no simplemente



? El motivo es que si f no es inyectiva, Q_f no puede ser unitaria. Una función periódica no puede ser unitaria.

Si damos a Q_f la superposición $\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$ como *input* de Q_f obtenemos $\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\,|f(x)\rangle$.

Hagamos una medida sobre el segundo registro de este estado y supongamos que encontramos un resultado f_0. Entonces, por el postulado de la medida, el primer registro se encuentra proyectado en la superposición de todos los x tales que $f_x = f_0$. Sea $f^{-1}(f_0) = \{x \in \{0,\dots,2^n-1\}; f(x) = f_0\}$.

Con esta notación, el primer registro está en el estado $\underbrace{\frac{1}{|f^{-1}(f_0)|^{\frac{1}{2}}}}_{\text{const. de normalización}}\sum_{x\in f^{-1}(f_0)}|x\rangle$. $f^{-1}(f_0)$es un conjunto finito cuyo tamaño llamaremos A, y cuyo mínimo llamaremos x_0. Observamos que $x_0 < r$ (de lo contrario $x_0 - r$ pertenece a $f^{-1}(f_0)$ y sería inferior a x_0 por lo que sería una contradicción). Usando la hipótesis de que r es el más periódico de f, podemos expresas $\underbrace{\frac{1}{|f^{-1}(f_0)|^{\frac{1}{2}}}}_{\text{const. de normalización}}\sum_{x\in f^{-1}(f_0)}|x\rangle$ como $\frac{1}{A^{\frac{1}{2}}}\sum_{j=0}^{A-1}|x_0+jr\rangle$. Si operamos una QFT sobre este estado obtenemos $\frac{1}{A^{\frac{1}{2}}}\sum_{j=0}^{A-1} QFT\,|x_0+jr\rangle$ (linealidad) $= \frac{1}{A^{\frac{1}{2}}}\sum_{j=0}^{A-1}\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{2\pi i(x_0+jr)y/N}\,|y\rangle = \frac{1}{N^{\frac{1}{2}}A^{\frac{1}{2}}}\sum_{y=0}^{N-1}\left[\sum_{j=0}^{A-1} e^{2\pi ijry/N}\right] e^{2\pi ix_0y/N}\,|y\rangle$ (llamemos $|\phi\rangle$ a este estado).

Si se hace una medida en la base canónica sobre este estado se encuentran el resultado y con probabilidad: $Proba[y] = |\langle y|\phi\rangle|^2$ donde:

$$\langle y|\phi\rangle = \frac{1}{\sqrt{NA}}\sum_{z=0}^{N-1}\left[\sum_{j=0}^{A-1} e^{2\pi ijrz/N}\right] e^{2\pi ix_oz/N}\underbrace{\langle y|z\rangle}_{\delta_{yz}} = \frac{1}{\sqrt{NA}}e^{2\pi ix_oy/N} * \sum_{j=0}^{A-1} e^{2\pi ijry/N}$$

Una vez obtenido el valor de $\langle y|\phi\rangle$ podemos calcular $Proba[y]$:

$$Proba[y] = \frac{1}{NA}\left|\sum_{j=0}^{A-1} e^{2\pi ijry/N}\right|^2 = \frac{1}{NA}\left|\frac{e^{2\pi iAry/N}-1}{e^{2\pi iry/N}-1}\right|^2$$

Resumen hasta ahora:

1 Construir $\frac{1}{N^{\frac{1}{2}}}\sum_{x=0}^{N-1}|x\rangle\otimes|\gamma\rangle$

2 $\downarrow\ \downarrow$ $\boxed{Q_f}$ $\downarrow\ \downarrow$

$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\otimes|f(x)\rangle$

$\downarrow$ **4** QFT $\downarrow$ **5** Medida

$\downarrow$ **3** Medida f_0

Vamos a ver que con relativamente alta probabilidad el resultado de la última medida proporciona información sobre el periodo r. Para eso necesitamos resultados técnicos.

Lemma 1. $N - r \leq x_0 + (A-1)r < N$

Demostración. $x_1 + (A-1)r = \max f^{-1}(f_0) < N$. Por otra parte, $N - r \leq \max f^{-1}(f_0)$ (fácil de comprobar). Si no fuera el caso, tendríamos que $\max f^{-1}(f_0) + \underbrace{r}_{>0} < N \Rightarrow$ $\max f^{-1}(f_0)$ debería de ser el máximo, de lo contrario sería una contradicción.

Lemma 2. $A - 1 < \frac{1}{2} < A + 1$

Lemma 3. Hay r valores $y \in \{0, \ldots, N-1\}$ tal que $\left|\frac{y}{N} - \frac{k}{r}\right| \leq \frac{1}{2N}$ para algún k en $\{0, \ldots, r-1\}$.

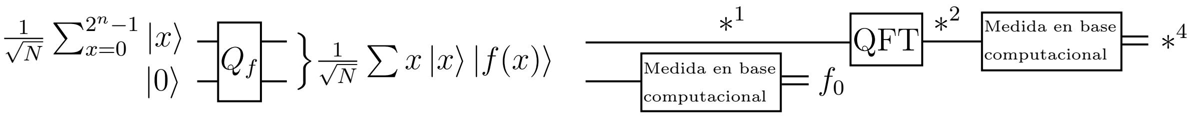
Demostración. El conjunto $\mathcal{S} \equiv \{0, \ldots, rN-1\}$ contiene el conjunto $T \equiv \{kN; k = 0, \ldots, r-1\}$ donde $\forall kN \in T$, veremos que $\exists$ y en $\{0, \ldots, N-1\}$ tal que $|yr - kN| \leq \frac{r}{2}$. En efecto, para $kN \in T$, $\exists \alpha \in \{0, \ldots, N-1\}$ tal que $\underbrace{\alpha r}_{\in \mathcal{S}} \leq kN \leq \underbrace{(\alpha+1)r}_{\in \mathcal{S}}$ ya que $T \subseteq \mathcal{S}$. Por lo tanto, $\sigma|kN - \alpha r| \leq \frac{r}{2}$ y $\sigma|kN - (\alpha+1)r| \leq \frac{r}{2}$.

En el primer caso elegimos $y = \alpha$; en el segundo, elegimos $y = \alpha + 1$. En ambos casos tendremos $|kN - yr| \leq \frac{r}{2} \underbrace{\Rightarrow}_{\substack{\text{dividiendo} \\ \text{por } rN}} \left|\frac{k}{r} - \frac{y}{N}\right| \leq \frac{1}{2N}$

4.6.2. Periodicidad

$f : \{0, \ldots, 2^n - 1\} \to \{0, \ldots, 2^m - 1\}$. $N \equiv 2^n$. $f(x+r) = f(x)$. Pb: $r =?$.

Estamos considerando el proceso

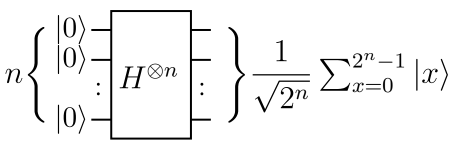


$*^1$: este registro se encuentra en el estado $\frac{1}{A^{\frac{1}{2}}} \sum_{j=0}^{A-1} |x_0 + jr\rangle$, $(f(x_0) = f_0)$ y $A = |f^{-1}(f_0)|$: tamaño de la preimagen de f_0.

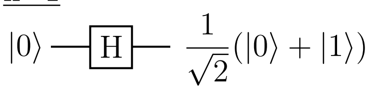
$*^2$: $\frac{1}{\sqrt{NA}} \sum_{y=0}^{N-1} e^{2\pi i x_0 y/N} \sum_{j=0}^{A-1} e^{2\pi i j r y/N} \, |y\rangle$.

$*^3$: y: este resultado contiene información sobre r con alta probabilidad.

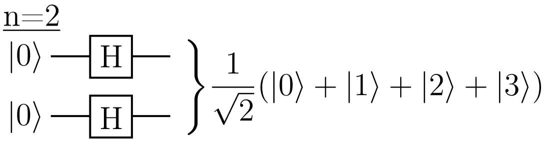
Ejercicio



n=1



n=2



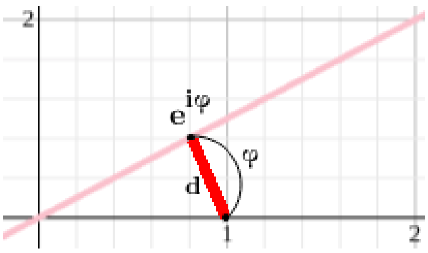
$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} = \frac{1}{\sqrt{2^n}}\sum_{j_{n-1}=0,1}\cdots\sum_{j_0=0,1}\underbrace{\left|j_0+j_12^1+j_22^2+\cdots+j_{n-1}2^{n-1}\right\rangle}_{\substack{\text{representado como}\\ |j_0,j_1,\ldots,j_{n-1}\rangle}} =$$

$$= \left(\frac{1}{\sqrt{2}}\sum_{j_{n-1}=0,1}|j_n\rangle\right)\otimes\cdots\otimes\left(\frac{1}{\sqrt{2}}\sum_{j_0=0}^{1}|j_0\rangle\right) =$$

$$= (\mathcal{H}\,|0\rangle)\otimes\cdots\otimes(\mathcal{H}\,|0\rangle)$$

Lemma 4. Sea $\varphi \in \left[-\frac{\pi}{2},\frac{\pi}{2}\right] \Rightarrow |1-e^{i\varphi}|$

Demostración. Si $0 \leq \varphi \leq \frac{\pi}{2}$



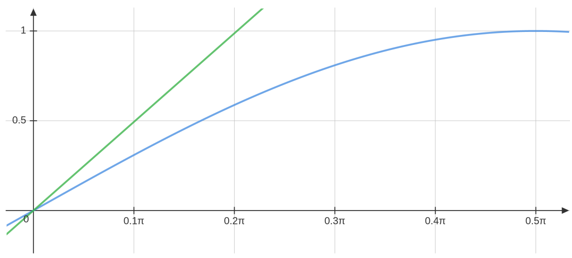
φ: la demostración es parecida entre 1 y $e^{i\varphi}$

$d \leq \varphi$. Observamos que $d = |1-e^{i\varphi}|$.

La demostración es similar si $-\frac{\pi}{2} \leq \varphi \leq 0$

Lemma 5. $0 \leq x \leq \frac{\pi}{2} \Rightarrow \frac{2x}{\pi} \leq \sin x$.

Demostración. $(\sin x)' = \cos x \geq 0$ donde $\forall x \in \left[0,\frac{\pi}{2}\right]$. $(\sin x)'' = -\sin x \leq 0$ donde $\forall x \in \left[0,\frac{\pi}{2}\right]$



Por lo tanto, $\sin x$ es no-decreciente convexa en $\left[0,\frac{\pi}{2}\right] \Rightarrow$ En este intervalo, $\sin x$ supera la recta que une los puntos $(0,0)$ y $\left[\frac{\pi}{2},1\right]$.

$y = \sin x$ - $y = \frac{2}{\pi}x$

Lemma 6. Sean 2 funciones f, g derivables en $\mathbb{R}$ tal que $f(x) \leq g(x)$ $\forall x \in [a,b]$. Sea $\varepsilon > 0$. $\forall x \in [b,(1+\varepsilon)b]$, $g(x) \geq f(b) - \left(\underset{x\in[b,(1+\varepsilon)b]}{max}\left|\frac{dg}{dx}\right|\right)\varepsilon b.$

Demostración. El teorema fundamental del cálculo nos dice que

$q(x)-q(b) = \int_b^x \frac{dg}{dx}dx \underbrace{=}_{\substack{\text{teorema}\\ \text{valor}\\ \text{medio}}} \left.\frac{dg}{dx}\right|_{\tilde{x}}(x-b)$ donde $\tilde{x} \in [x,b]$. Concluimos observando que $g(b) \geq f(b)$.

Volviendo el lema 3, $\left|\frac{y}{N}-\frac{k}{r}\right| \leq \frac{1}{2N} \Leftrightarrow \exists \delta$ tal que $\frac{y}{N}=\frac{k}{r}+\delta$ con $|\delta| \underbrace{\leq}_{*^1} \frac{1}{2N}$. Si y satisface ..., entonces $e^{i2\pi ry/N}=e^{i2\pi k}e^{i2\pi r\delta}=e^{i2\pi r\delta}$.

$*^1$: dijimos que suponíamos que $r << N \Rightarrow |2\pi 2\delta| \leq \pi\frac{r}{N} < \frac{\pi}{2} \underbrace{\Rightarrow}_{\text{Lema 4}} |e^{i2\pi r\delta}-1| \leq 2\pi r|\delta|$.

Por otra parte, ... $\Rightarrow e^{i2\pi Ary/N}=\underbrace{e^{i2\pi Ar\frac{k}{r}}}_{1}e^{i2\pi Ar\delta}$

$$\left|e^{i2\pi Ar\delta}-1\right| = \left|e^{i2\pi Ar\frac{\delta}{2}}\left(e^{i2\pi Ar\delta/2}-e^{-i2\pi Ar\delta/2}\right)\right|$$

$$|wz|=|w|*|z|=2|sin(\pi Ar\delta)|$$

El lema 1 implica que $Ar < N+r \Rightarrow |\pi Ar\delta| \leq \left|\pi\frac{N+r}{N}\underbrace{N\delta}_{\frac{1}{2}}\right| = \frac{N+r}{N}\frac{\pi}{2} = \left(1+\frac{r}{N}\right)\frac{\pi}{2}$.

Si $|\delta|$ es tan pequeño que $|\pi Ar\delta| \leq \frac{\pi}{2}$ entonces la probabilidad de un resultado y asociado se puede obtener como:

$$Probabilidad(y) = \frac{1}{NA}\left|\sum_{j=0}^{A-1}e^{2\pi ijry/N}\right|^2 = \frac{1}{NA}\left|\frac{e^{i2\pi Ary/N}-1}{e^{i2\pi ry/N}-1}\right|^2 = \frac{4}{NA}\frac{|sin(\pi rA\delta)|^2}{|1-e^{i2\pi r\delta}|^2} \underbrace{\geq}_{\substack{\text{Lemas}\\ \text{4 y 5}}} =$$

$$= \frac{4}{NA}\frac{\left|\frac{\pi Ar|\delta|}{\frac{\pi}{2}}\right|^2}{|2\pi r\delta|^2} = \frac{4}{\pi^2}\frac{A}{N} \underbrace{>}_{\substack{\text{Lema}\\ 2}} \frac{4A}{\pi^2}\frac{1}{r(A+1)}$$

Si $A > 1$ (pasará para $1 << r$), $\frac{A}{A+1} > \frac{1}{2} \Rightarrow Proba(y) \geq \frac{2}{\pi^2 r}$. Si $\frac{\pi}{2} \leq \pi Ar|\delta| \leq \frac{\pi}{2}\frac{N+r}{N}$ entonces (lema 6) $sin(\pi rA|\delta|) \geq 1-\frac{r}{N}\frac{\pi}{2}\text{x}1 = 1-\frac{\pi r}{2N}$.

Por lo tanto, $Proba(y) \geq \frac{4}{NA}\left|\frac{1-\frac{r}{N}\frac{\pi}{2}}{2\pi r\delta}\right|^2 \geq \frac{4}{NA}\left|\frac{1-\frac{r}{N}\frac{\pi}{2}}{2\pi r\frac{1}{2N}}\right| = \frac{(2N-r\pi)^2}{NA\pi^2 r^2}$.

Como asumimos $r << N$, podemos suponer que $2\pi < 2N \Rightarrow Proba(y) > \frac{1}{\pi^2}\frac{4N^2}{NAr^2}$.

Teorema 1. Si y es tal que $\left|\frac{y}{N}-\frac{k}{r}\right| \leq \frac{1}{2N}$ para algún $k \in \{0,\dots,r-1\}$, entonces $Proba(g) \geq \frac{2}{\pi^2 r}$ y hay r tales valores de y.

Lemma 7. Si y satisface $\left|\frac{y}{N}-\frac{k}{r}\right| \leq \frac{1}{2N}$ para algún $k \in \{0,\dots,r-1\}$ entonces este k es único.

Teorema 2. $\exists$ algoritmo clásico eficiente para encontrar el racional q más cercano al racional $\frac{y}{N}$ con denominador inferior a $\underbrace{N^{\frac{1}{2}}}_{*^1}$ (algoritmo de fracción continua).
$*^1$: esta condición es compatible con nuestra hipótesis $1 << r << N$: se puede suponer $r < N^{\frac{1}{2}}$.

Combinando los teoremas 1 y 2 vemos que con probabilidad superior a $\overbrace{\frac{2}{\pi^2 r}}^{\text{Prob. buen valor } y} * \overbrace{r}^{\text{n° "buenos" valores}} = \frac{2}{\pi^2}$ sacamos un valor y del cual se puede extraer un racional $q = \frac{k}{r}$.

Podría ocurrir que k y r tenga factores comunes. En este caso, no se sacan k y r sino un número $q = \frac{k_1}{r_1} = \frac{k}{r}$. Es decir, en general la información que se saca es algún divisor del periodo. Incluso en este caso, hay manera de obtener r. Repitamos la operación y supongamos que obtenemos $q' = \frac{k_2}{r_2}$.

Se puede demostrar:

- $mcd(k_1, k_2) = 1 \Rightarrow r = mcd(r_1, r_2)$
- Usando el teorema 1 se puede demostrar que $Proba[mcd(k_1, k_2) = 1] \geq \underbrace{\left(\frac{2}{\pi^2}\right)^2 \frac{1}{4}}_{\text{esta cuota inferior sobre la prob. de existo es indep. del num. de (q) y el periodo } r}$

Supongamos que repetimos zl veces el experimento siguiente (tiempo polinómico en n):

(1) Preparación de $|0 \dots 0\rangle$

(2) Aplicación del circuito cuántico y medido

(3) Extracción de $q = \frac{k'}{r'}$ usando el algoritmo de fracción continua

Sean $(k_{1,1}, r_{1,1}), (k_{2,2}, r_{1,2}), \dots, (k_{l,1}, r_{l,1}), (k_{l,2}, r_{l,2})$ los resultados obtenidos. Llamaremos <u>evento suficientemente favorable</u> a la aparición de un par $(k_{j,1}, r_{j,1}), (k_{j,2}, r_{j,2})$ tal que $\frac{k_{j,1}}{r_{j,1}} = \frac{\tilde{k}_1}{r}$ y $\frac{k_{j,2}}{r_{j,2}} = \frac{\tilde{k}_2}{r}$ y $mcd(k_{j,1}, k_{j,2}) = 1$. Cuando ocurre un tal evento podemos extraer r.

Lemma 8. Sea una variable aleatoria con 2 posibles resultados: "sufi. fav." y "resto". Sea $\varphi \equiv Proba(\text{"sufi. fav."})$. La probabilidad de observar un evento "sufi. fav." despues de l

repeticiones está dada por $1(1-\varphi)^l$.

Demostración. $(1-\varphi)^l \equiv Proba[l\ eventos\ \text{“}resto\text{”}\ consecutivos]$ y $P(E) = 1 - P(E^c)$ $\forall$ evento de E.

La probabilidad de sacar el periodo r después de l repeticiones del experimento es el menor $1 - \left(1 - \frac{1}{\pi^2}\right)^l$.

4.6.3. QFT

$|x\rangle \to \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{i2\pi xy/N} |y\rangle$. $N = 2$ (bits que recibe el función j en el *input*).

$$X = x_1 2^{n-1} + x_2 2_2^{n-2} + \cdots + x_n 2^0 = \sum_{l=1}^{n} x_l 2^{n-l} = x_1 x_2 \dots x_n$$

$$|x\rangle = |x_1, \dots, x_n\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle \overbrace{\rightarrow}^{QFT} \frac{1}{2^n} \sum_{y=0}^{2^n-1} e^{2\pi i y \left(\sum_{l=1}^{n} x_l 2^{n-l}\right) 2^n |y\rangle}$$

$$\begin{aligned} QFT\,|x_1, \dots, x_n\rangle &= \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i y \left(\sum_{l=1}^{n} x_l 2^{-l}\right)} |y\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} \prod_{l=1}^{n} e^{2\pi i y x_l / 2^l} |y\rangle = \\ &= \frac{1}{2^{\frac{n}{2}}} \sum_{y_1=0,1} \cdots \sum_{y_n=0,1} e^{2\pi i \left(\sum_{\alpha=1}^{n} y\alpha 2^{n-\alpha}\right) x_l / 2^l} |y_1 \dots y_n\rangle = \\ &= \frac{1}{2^{\frac{n}{2}}} \left(\sum_{y_1=0,1} \prod_{l=1}^{n} e^{2\pi i y_1 2^{n-1} x_l / 2^l} |y_1\rangle \right) \otimes \cdots \otimes \left(\sum_{y_n=0,1} \prod_{l=1}^{n} e^{2\pi i y_n 2^0 x_l / 2^l} |y_n\rangle \right) \end{aligned}$$

Notación para números inferiores a 1 en notación binaria: 0. $j_1 j_2 j_3 \cdots \equiv j_1 2^{-1} + j_2 2^{-2} + j_3 2^{-3} + \dots$

$$\frac{y}{2^l} = \frac{y_1 \cdots y_n}{2^l} = y_1 2^{n-1-l} + \cdots + y_{n-l} 2^0 + y_{n-l+1} 2^{-1} + \cdots + y_n 2^{-l} = (y_1 2^{n-1-l} + \cdots + y_{n-l} 2^0) + 0$$

$y_{n-l+1} y_{n-l+2} + \cdots + y_n$

$$e^{2\pi i y/2^l} = \underbrace{e^{2\pi i \overbrace{\left(y_1 2^{n-1-l} + \cdots + y_{n-l} 2^0\right)}^{entero}}}_{1} e^{2\pi i o.y_{n-l-1} \cdots y_n} = e^{2\pi i o.y_{n-l\pi} \cdots y_n}$$

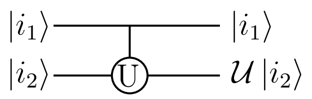
Usando esta identidad vemos que:

$$QFT\,|x_1 \dots x_n\rangle = \frac{(|0\rangle + e^{2\pi i o.x_n}|1\rangle) + (|0\rangle + e^{2\pi i o.x_n - 1 x_n}|1\rangle + \cdots + (|0\rangle + e^{2\pi i o.x_1 x_2 \dots x_n}|1\rangle))}{2^{\frac{n}{2}}}$$

De esta identidad derivamos un circuito cuántico para la QFT sea:

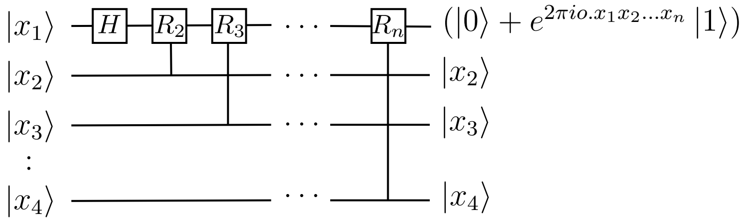
$$\text{Sea } R_k = \begin{pmatrix} 1 & 0 \\ 0 & 2^{2\pi i/2^n} \end{pmatrix} \qquad (R_k^{-1} = R_k^*)$$

Notación. Sea $\mathcal{U}$ unitario a un qubit definimos



(en base computacional)

Ejercicio



$\#$ gates $= (1+n)+(1+(n-1)) + \cdots + (1+1) = n + \dfrac{n(n-1)}{2} = poly(n)$

Problema

Consideremos la ecuación de Schrödinger $\mathcal{H}\,|\varphi(t)\rangle = i\hbar\partial_t\psi(t)$ con condición inicial $|\psi(t=0)\rangle = |\psi_0\rangle$. Queremos información sobre esta evolución. En particular, dado un observable X queremos conocer el valor medio de X con el tiempo:

$$< x(t) >= \langle\psi(t)|\, x\, |\psi(t)\rangle$$

En general es difícil[a], sin embargo, hay muchas soluciones en las que nos gustaría resolver este problema aunque sea de manera aproximada (física nuclear, química cuántica, superconductores. . .).

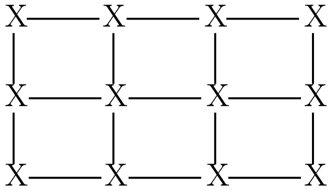
Pregunta: ¿Puede ayudar un ordenador cuántico? Tal vez. . .

Nos focalizaremos en una clase de hamiltonianos conexos.

$$H \equiv -\sum_{i\in V} h_i \sigma_i^x - \sum_{<i,j>\in E} J_{ij}\sigma_i^z \sigma_j^z$$

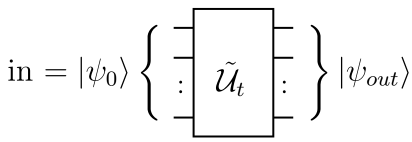
Modelo de Ising relevante en física de la materia condensada, física de altas energías ($X = \sum_{i\in V}\sigma_i^z$: magnetización).

$\wedge = (V, E)$ es una red con grafo.

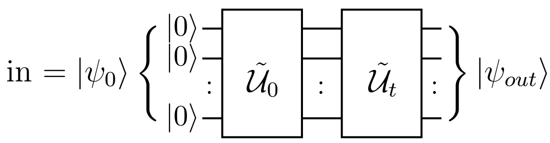


Pequeño abuso de notación: $\sigma_i^x \equiv \otimes_{k\neq i}\mathbb{1}_k \otimes \sigma_i^x$.

Queremos $< x(t) >= \langle\psi(t)| X |\psi(t)\rangle$ donde $X = \sum_{i\in V}\sigma_i^z$. ¿Como? Quisiéramos algún circuito $\tilde{\mathcal{U}}_t$ tal que $\langle\psi_{out}| X |\psi_{out}\rangle \simeq < x(t) >$ y que se puede hacer $\forall t > 0$.



Idealmente quisiéramos más:



La simulación solo es posible si $|\psi_0\rangle$ se puede preparar de manea eficiente.

¿Donde está la dificultad?

$|\psi(t)\rangle = e^{-i\mathcal{H}t}|\psi_0\rangle$ ($\mathcal{H}$ es independiente del tiempo en nuestro ejemplo).

$e^{-i\mathcal{H}t} = \sum_{\alpha=0}^{\infty}\dfrac{(-i\mathcal{H}t)^\alpha}{\alpha!}$

$\mathcal{H} = \sum_a \varepsilon_a \prod_a$ donde $\sum_a$ hace referencia a la <u>indexación de autovalores distintos</u>, ε_a

hace referencia al autovalor asociado al índice a, por ultimo, $\prod_a$ hace referencia al proyector sobre el SEV asociado al autovalor ε_a.

$$\mathcal{H}^2 = \left(\sum_{a_1}\varepsilon_{a_1}\prod_{a_1}\right)\left(\sum_{a_2}\varepsilon_{a_2}\prod_{a_2}\right) = \sum_{a_1 a_2}\varepsilon_{a_1}\varepsilon_{a_2}\underbrace{\prod_{a_1}\prod_{a_2}}_{\substack{\prod_{a_1} \text{ si } a_1=a_2 \\ 0 \text{ si } a_1\neq a_2}} = \sum_{a_1}\varepsilon_{a_1}^2\prod_{a_1}$$

De la misma manera se demuestra mediante inducción que $\mathcal{H}^\alpha = \sum_a \varepsilon_a^\alpha \prod_a$.

$$\Rightarrow e^{-i\mathcal{H}t} = \sum_{\alpha=0}^{\infty}\sum_a \frac{(-i\varepsilon_a t)^\alpha}{\alpha!}\prod_a = \sum_a e^{-i\varepsilon_a t}\prod_a$$

$$\frac{\partial}{\partial t}\left[e^{-i\mathcal{H}t}|\psi_0\rangle\right] = \left[\frac{\partial}{\partial t}e^{-i\mathcal{H}t}\right]|\psi_0\rangle = \left[\sum_a -i\varepsilon_a e^{-i\varepsilon_a t}\prod_a\right]|\psi_0\rangle$$

Por otra parte:

$$-i\mathcal{H}e^{-i\mathcal{H}t} = -i\sum_a\varepsilon_a\prod_a\sum_{a'}e^{-i\varepsilon_{a'}t}\prod_{a'} \overbrace{=}^{\prod_a\prod_{a'}=\delta_{aa'}\prod_a} -i\sum_a\varepsilon_a e^{-i\varepsilon_a t}\prod_a$$

$$\Rightarrow \frac{\partial}{\partial t}|\psi(t)\rangle = -i\mathcal{H}|\psi(t)\rangle = |\psi(t)\rangle \text{ es la solución de la ecuación de Schrödinger}$$

[a]Salvo en casos especiales el esfuerzo requerido usando recursos clásicos crece exponencialmente con el número de partículas del sistema que se pretende simular.

Hemos reformulado el problema: queremos ahora aproximar el operador de evolución $\mathcal{U}(t) \equiv e^{-i\mathcal{H}t}$ por un circuito cuántico $\tilde{\mathcal{U}_t}$. Para ello vamos a (aproximadamente) descomponer $\mathcal{U}(t)$ en una secuencia de puertas a 1 qubit y puertas a dos qubits. Ingredientes claves:

Teorema (Descomposición de Suzuki-Trotter). Sean X e Y operadores actuando sobre un EV V, entonces:

$$\|e^{\varepsilon(X+Y)} - e^{\varepsilon X/2}e^{\varepsilon Y}e^{\varepsilon X/2}\|_\infty = \mathcal{O}(\varepsilon^2\|[X,Y]\|_\infty)$$

$$\|A\|_\infty \overbrace{=}^{def} sup_{|\psi\neq 0\rangle}\frac{\|A|\psi\rangle\|}{\||\psi\rangle\|}$$

Si $A = A^*$, $\|A\|_\infty =$ máximo autovalor de A en valor absoluto.

¿Por qué necesitamos esta descomposición? Nos interesa $e^{-it(-\sum_i h_i\sigma_i^x - \sum_{<i,j>} J_{ij}\sigma_i^z\sigma_j^z)} = e^{-i\mathcal{H}t}$.

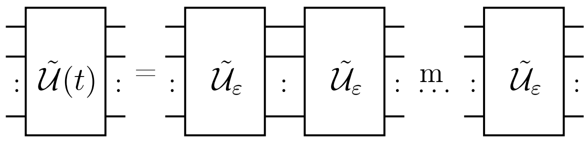
Es muy tentador igualar $e^{-it(-\sum_i h_i\sigma_i^x - \sum_{<i,j>} J_{ij}\sigma_i^z\sigma_j^z)}$ con $\prod_i \underbrace{e^{ith_i\sigma_i^x}}_{\text{1-qubit gate}} \prod_{<i,j>} \underbrace{e^{itJ_{ij}\sigma_i^x\sigma_j^x}}_{\text{2-qubit gate}}$. La "tentación" viene de que para v, $w \in \mathbb{C}$ $e^{v+w} = e^v e^w$.

Pero para operadores X, Y que no conmutan $e^{X+Y} \neq e^X e^Y$. Lo más parecido a $e^{X+Y} \neq e^X e^Y$ en este caso es la descomposición de Suzuki-Trotter. Para usarla expresamos

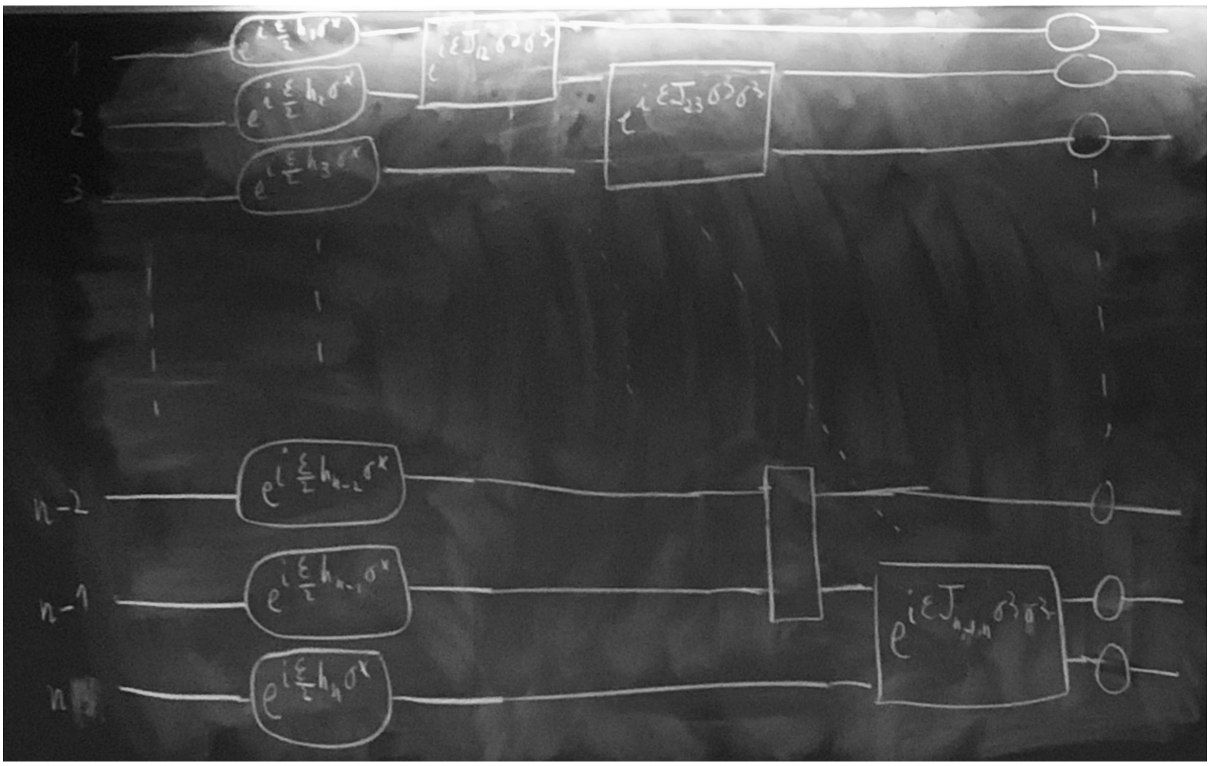
$$\mathcal{U}(t) = e^{-i\mathcal{H}t} \overbrace{\underbrace{=}_{[\mathcal{H},\mathcal{H}]=0}}^{m\gg 2} \left(e^{-i\mathcal{H}\frac{t}{m}}\right)^m \equiv \mathcal{U}(\varepsilon)^m \text{ con } \varepsilon = \frac{t}{m}$$

$$e^{-i\mathcal{H}t} = e^{-i\mathcal{H}\frac{t}{m}m} = e^{-i\overbrace{\mathcal{H}\frac{t}{m} + \mathcal{H}\frac{t}{m} + \cdots + \mathcal{H}\frac{t}{m}}^{m \text{ veces}}} = \prod_{j=1}^{m} e^{-i\mathcal{H}\frac{t}{m}} = \prod_{j=1}^{m} \mathcal{U}(\varepsilon)$$

En diagramas:



Usaremos la descomposición de ST para aproximar cada $\mathcal{U}_\varepsilon$ con un circuito cuántico.



Elijamos $X = i\sum_i h_i\sigma_i^x$, $Y = i\sum_{<i,j>} J_{ij}\sigma_i^z\sigma_j^z$.

$$e^{-i\varepsilon(-\sum_i h_i\sigma_i^x - \sum_{<i,j>} J_{ij}\sigma_i^3\sigma_j^3)} = e^{-i\varepsilon\mathcal{H}} \overset{\text{S. T.}}{\simeq} \prod_{i\in V} \underbrace{e^{i\frac{\varepsilon}{2}h_i\sigma_i^x}}_{\text{1-qubit gate}} \prod_{<i,j>\in V} \underbrace{e^{i\varepsilon J_{ij}\sigma_i^z\sigma_j^z}}_{\text{2-qubit gate}} \prod_{i\in V} e^{i\frac{\varepsilon}{2}h_i\sigma_i^x} \equiv \tilde{\mathcal{U}}_\varepsilon$$

Ejemplo

Ising en 1D.

$$H = -\sum_{i=1}^{n} h_i\sigma_i^x - \sum_{i=1}^{n-1} J_{i,i+1}\sigma_i^z\sigma_{i+1}^z$$

$\underline{n=3}$

$$e^{i\frac{\varepsilon}{2}h_3\sigma_3^x}e^{i\frac{\varepsilon}{2}h_2\sigma_2^x}e^{i\frac{\varepsilon}{2}h_1\sigma_1^x} \times e^{i\varepsilon J_{23}\sigma_2^z\sigma_3^z}e^{i\varepsilon J_{12}\sigma_1^z\sigma_2^z}e^{i\frac{\varepsilon}{2}h_3\sigma_3^x}e^{i\frac{\varepsilon}{2}h_2\sigma_2^x}e^{i\frac{\varepsilon}{2}h_1\sigma_1^x}$$

Importante

$$e^{i\frac{\varepsilon}{2}h_k\sigma_k^x} = \otimes_{j\neq k}\mathbb{1}_j \otimes e^{i\frac{\varepsilon}{2}h_k\sigma_k^x}$$

$$e^{i\varepsilon J_{k,k+1}\sigma_k^z\sigma_{k+1}^z} = \otimes_{j\neq k,k+1}\mathbb{1}_j \otimes e^{i\varepsilon J_{k,k+1}\sigma_k^z\sigma_{k+1}^z}$$

¿Precisión de la aproximación?

Vamos a acotar $\|\mathcal{U}(t) - \tilde{\mathcal{U}}_\varepsilon^m\|_\infty$. $ST \Rightarrow \mathcal{U}(\varepsilon) = \tilde{\mathcal{U}}_\varepsilon + \varepsilon^2\triangle(\varepsilon,\mathcal{H})$ donde $\triangle(\varepsilon,\mathcal{H})$ es un operador cuya norma $\underbrace{\to}_{\varepsilon\to 0}$ constante.

$$\mathcal{U}(t) = \mathcal{U}(\varepsilon)^m = \left(\tilde{\mathcal{U}}_\varepsilon + \varepsilon^2\triangle\right)^m = \sum_{l=1}^{m} K_l(\tilde{\mathcal{U}}_\varepsilon, \varepsilon^2\triangle)$$

$K_l(X,Y)$ es un polinomio de grado $m-1$ en X, l en Y y contiene $\begin{pmatrix} m \\ l \end{pmatrix}$ términos.

$$\|K_l\|_\infty \leq \begin{pmatrix} m \\ l \end{pmatrix} \left\|\tilde{\mathcal{U}}_\varepsilon\right\|_\infty^{m-1} \|\varepsilon^2\triangle\|^l$$

Observamos también que $K_0 = \tilde{\mathcal{U}}_\varepsilon$. Por lo tanto:

$$\left\|\mathcal{U}(t) - \tilde{\mathcal{U}}_\varepsilon^m\right\|_\infty = \left\|\sum_{l=1}^{m} K_l\right\|_\infty \leq \sum_{l=1}^{m} \varepsilon^{2l} \|\triangle\|_\infty^l = \underbrace{\left(1 + \varepsilon^2 \|\triangle\|_\infty\right)^m - 1}_{\text{se puede probar que [...] } \underbrace{\to}_{m\to\infty} 0}$$

Tema 5

Códigos cuánticos correctores de error

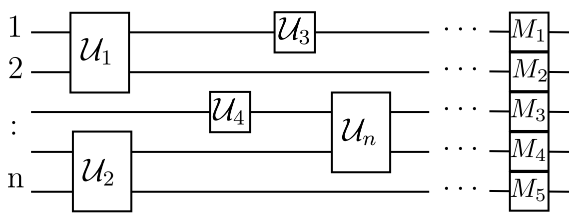
El ruido afecta al buen funcionamiento de un ordenador cuántico, ¿se puede combatir?

Causa del ruido: todo sistema físico interactivo con su entorno. Los algoritmos cuánticos que hemos visto hasta ahora suponen:

- Los qubits forman un sistema aislado
- Las puertas cuánticas se pueden aplicar perfectamente

¿Que pasa cuando se relajan estas dos hipótesis?

<u>Ideal</u>:



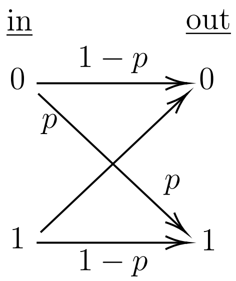
<u>Realidad</u>:

$\tilde{\mathcal{U}}_1, \tilde{\mathcal{U}}_2 \ldots$ en lugar de $\mathcal{U}_1, \mathcal{U}_2 \ldots$

$\tilde{M}_1$, $\tilde{M}_2 \ldots$ en lugar de M_1, $M_2 \ldots$

5.1. Corrección de errores clásica

Consideramos un canal que transmite bits de uno en uno. Este canal tiene ruido:



Sea p la probabilidad de error. Supongamos que $p < \frac{1}{2}$, ¿qué pasa si usamos 3 bits físicos para codificar un bit lógico? $0_L = 000$, $1_L = 111$.

In	Out	p(out/in)
000	000	$(1-p)^3$
000	001	$p(1-p)^2$
000	110	$p^2(1-p)$
000	111	p^3

5.2. Códigos correctores de errores

Imaginemos que el receptor decide descodificar una señal de tres bits usando la siguiente tabla:

000	0_L
001	0_L
010	0_L
011	0_L
100	1_L
101	1_L
110	1_L
111	1_L

¿Probabilidad de mala descodificación?

- Puertas con 2 errores:
  $\binom{3}{2} \times p^2(1-p)$
- Puertas con 3 errores:
  p^3

La probabilidad de cometer un error, usando este código, es:

$$\tilde{p} = \binom{3}{2} p^2(1-p) + p^3 = 3p^2 - 2p^3$$

Logramos reducir el ruido si $\tilde{p} < p$.

$$3p^2 - 2p^3 < p \Leftrightarrow 3p - 2p^2 < 1 \Leftrightarrow 2p^2 - 3p + 1 > 0$$

$$2p^2 - 3p + 1 = 0 \Leftrightarrow P_A = \frac{3 \pm \sqrt{1}}{4} \begin{cases} 1 \\ \frac{1}{2} \end{cases}, \delta = 9 - 8 = 1$$

Shannon: $\underbrace{h(p)}_{-p\ln(p)-(1-p)\ln(1-p)}$ $info/bit$

5.2.1. Bottom line

- $in \rightarrow ENCODING \rightarrow RUIDO \rightarrow DECODING \rightarrow out$
- El ruido se puede combatir introduciendo redundancia.

¿En el caso cuántico? ¿Se puede introducir redundancia también para combatir el ruido? Respuesta corta, si. Respuesta honesta, si pero no es tan simple.

5.3. Teorema de no-clonación

Supongamos que $\exists$ un unitario $\mathcal{U}$ tal que $\mathcal{U}$: $\underbrace{|\phi\rangle}_{\text{input a clonar}} \underbrace{|M_0\rangle}_{\text{estado de un sistema auxiliar}} \rightarrow |\phi\rangle^{\otimes n} \otimes |M_\phi\rangle$. Entonces si consideramos 2 *inputs* distintos, $|\phi\rangle$ y $|\psi\rangle$, por unitaridad:

$$\langle\phi|\psi\rangle \langle M_0|M_0\rangle = \langle\phi|\psi\rangle \left\langle M_\phi^n \middle| M_\psi \right\rangle \Rightarrow |\langle\phi|\psi\rangle| = |\langle\phi|\varphi\rangle|^n | \underbrace{M_\phi |M\psi\rangle}_{\leq 1} |$$

$$|\langle\phi|\psi\rangle| \underbrace{\leq}_{*^1} |\langle\phi|\varphi\rangle|^n \Rightarrow 1 \leq |\underbrace{\langle\phi|\varphi\rangle}_{*^2}|^{n-1}$$

$*^1$: si $|\phi\rangle$ y $|\psi\rangle$ no son ortogonales.

$*^2$: estrictamente inferior a 1 si ϕ y ψ no son idénticas. <u>Contradicción</u>

Un ejemplo de código cuántico corrector de errores es el código a 9 qubits de Shor:

$$\left.\begin{array}{l} |0_L\rangle = \left(\dfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\right)^{\otimes 3} \\ |1_L\rangle = \left(\dfrac{1}{\sqrt{2}}(|000\rangle - |111\rangle)\right)^{\otimes 3} \end{array}\right\} \text{ protege contra 1 error en cualquier qubit de los 9.}$$

Ejemplo

Verifica que $\underbrace{\langle i_L|j_L\rangle}_{*^1} = \delta_{ij}$ donde $i = 0$ y $j = 1$.

$$*^1 = \frac{1}{2^3}[(\langle 000| + \langle 111|)(|000\rangle - \langle 111|)]^3$$

$$\begin{aligned} \langle i_2|j_2\rangle &= \frac{1}{2^3}\left(\langle 000| + (-)^i \langle 111|)(|000\rangle + (-)^j \langle 111|\right)^3 = \\ &= \frac{1}{2^3}\left[\langle 000|000\rangle + (-)^{i+j}\langle 111|111\rangle + 0 + 0\right]^3 = \\ &= \frac{1}{2^3}[2\delta_{ij}]^3\delta_{ij} \end{aligned}$$

El siguiente código protege contra un *bit flip*:

Ejemplo

$$|\psi\rangle = \varphi_0|0_L\rangle + \varphi_1|1_L\rangle \to \left|\tilde{\psi}\right\rangle = \sigma_2^x|\psi\rangle$$

$$\begin{aligned} |\psi\rangle &= \frac{\psi_0}{2^{\frac{3}{2}}}(|010\rangle + |101\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \\ &+ \frac{\psi_1}{2^{\frac{3}{2}}}(|010\rangle - |101\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) \end{aligned}$$

Ejercicio

$\sigma_1^z\sigma_2^z\left|\tilde{\psi}\right\rangle =?$

$\sigma_2^z\sigma_3^z\left|\tilde{\psi}\right\rangle =?$

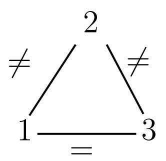
$$\begin{aligned} |0_L\rangle &= |GHZ+\rangle^{\oplus 3} \\ &= |GHZ+\rangle_{123} \otimes |GHZ\rangle_{456} \otimes |GHZ\rangle_{789} \\ |1_L\rangle &= |GHZ-\rangle^{\oplus 3} \\ &= |GHZ-\rangle_{123} \otimes |GHZ\rangle_{456} \otimes |GHZ\rangle_{789} \end{aligned}$$

$$|GHZ\pm\rangle \equiv \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle)$$

$$
\begin{aligned}
\sigma_1^z\sigma_2^z\left|\tilde{\psi}\right\rangle &= \frac{\varphi_0}{\sqrt{8}}\sigma_1^2\sigma_2^2(|010\rangle + |101\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \\
&+ \frac{\varphi_1}{\sqrt{8}}\sigma_1^2\sigma_2^2(|010\rangle - |101\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) = \\
&= -\left|\tilde{\psi}\right\rangle
\end{aligned}
$$

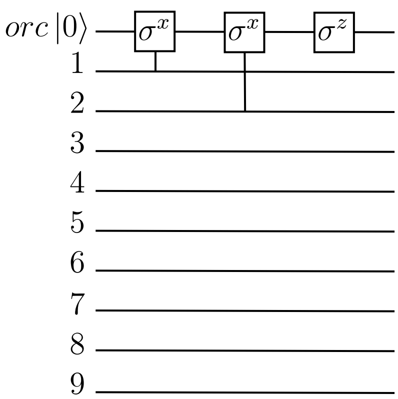
De la misma manera se ve que $\begin{cases} \sigma_1^2\sigma_2^2\left|\tilde{\psi}\right\rangle = -\left|\tilde{\psi}\right\rangle \\ \sigma_2^2\sigma_3^2\left|\tilde{\psi}\right\rangle = \left|\tilde{\psi}\right\rangle \end{cases}$

Conclusión:



El error está en el qubit 2.

Circuito para medir $\sigma_1^z\sigma_2^z$:



Crucial! Esta medida <u>NO</u> perturba el estado (ejecución)

5.4. Código a 9 qubits

Sea un estado $|\psi\rangle = \psi_0\,|0_L\rangle + \psi_1\,|1_L\rangle$. Imaginemos un error σ_2^x: $|\psi\rangle \to \left|\tilde{\psi}\right\rangle = \sigma_2^x\,|\psi\rangle$. ¿Qué pasa cuando se hacen las medidas siguientes sobre el sistema? ¿Efecto de cada una de estas medidas sobre $\left|\tilde{\psi}\right\rangle$?

Ejemplo

Medida $\sigma_a^z\sigma_b^z$. Ayer vimos que $\sigma_1^z\sigma_2^z\sigma_2^x\,|\psi\rangle = \sigma_2^z\sigma_3^z\sigma_2^x\,|\psi\rangle = \overbrace{-}^{*^1}\sigma_2^x\,|\psi\rangle$.

$*^1$: este signo "-" nos dice que hay un error de tipo *bit flip* en el qubit 2.

Error recovery: $\sigma_2^x \left|\tilde{\psi}\right\rangle = \sigma_2^x \sigma_2^x \left|\psi\right\rangle = \left|\psi\right\rangle$.

En cambio, $\sigma_1^z \sigma_2^z \left|\psi\right\rangle = \left|\psi\right\rangle$. Se verifica que en los resultados para medidas los dos siguientes sobre los estados siguientes:

	$\sigma_1^x \left|\psi\right\rangle$	$\sigma_2^x \left|\psi\right\rangle$	$\sigma_3^x \left|\psi\right\rangle$
$\sigma_1^z \sigma_2^z$	-1	-1	1
$\sigma_2^z \sigma_3^z$	1	-1	-1
$\sigma_4^z \sigma_5^z$	1	1	1
$\sigma_5^z \sigma_6^z$	1	1	1
$\sigma_7^z \sigma_8^z$	1	1	1
$\sigma_8^z \sigma_9^z$	1	1	1

Esas observables permiten localizar un error de tipo *bit flip*. Una vez localizado, este error se puede corregir aplicando σ^x en el lugar adecuado.

Ejemplo

¿Este código también protege frente a errores de tipo σ^z? Por ejemplo $\left|\psi\right\rangle \to \left|\tilde{\psi}\right\rangle = \sigma_7^z \left|\psi\right\rangle$.

$\sigma_1^x \sigma_2^x \sigma_3^x \sigma_4^x \sigma_5^x \sigma_6^x$

$\sigma_4^x \sigma_5^x \sigma_6^x \sigma_7^x \sigma_8^x \sigma_9^x$

¿Protege sobre $\left|\psi\right\rangle$ y sobre $\sigma_7^z \left|\psi\right\rangle$?

Miremos el caso $\left|\psi\right\rangle = \left|0_L\right\rangle$[a]:

$$\begin{aligned}
\left|\psi\right\rangle &= \otimes_{j=1}^{6} \sigma_j^x \left|GHZ^+\right\rangle_{123} \left|GHZ^+\right\rangle_{456} \left|GHZ^+\right\rangle_{789} = \\
&= \sigma_1^x \sigma_2^x \sigma_3^x \left|GHZ^+\right\rangle_{123} \otimes \sigma_4^x \sigma_5^x \sigma_6^x \left|GHZ^+\right\rangle_{456} \otimes \left|GHZ^+\right\rangle_{789} = \\
&= \left|0_L\right\rangle
\end{aligned}$$

De la misma manera $\otimes_{j=1}^{6} \sigma_j^x \left|1_L\right\rangle = (-)^2 \left|1_L\right\rangle = \left|1_L\right\rangle$

[a] Ver anexo 7.9.1 para los cálculos correspondientes

Ejercicio

$\sigma^z \sigma^x + \sigma^x \sigma^z = 0 \to \sigma^x \sigma^z = -\sigma^z \sigma^x$[a]

$$\sigma_1^x\sigma_2^x\sigma_3^x\sigma_4^x\sigma_5^x\sigma_6^x{\color{red}\sigma_7^z}\left|\psi\right\rangle = {\color{red}\sigma_7^z}\underbrace{\sigma_1^x\sigma_2^x\sigma_3^x\sigma_4^x\sigma_5^x\sigma_6^x\left|\psi\right\rangle}_{\left|\psi\right\rangle}\ ([\sigma_1^x\ldots\sigma_6^x,\sigma_7^z]=0) = {\color{red}\sigma_7^z}\left|\psi\right\rangle$$

$$\begin{aligned}
\sigma_4^x\sigma_5^x\sigma_6^x\sigma_7^x\sigma_8^x\sigma_9^x{\color{red}\sigma_7^z}\left|\psi\right\rangle &= ([\sigma_4^x,\ldots,\sigma_9^x,\sigma_7^z]\neq 0) = \\
\sigma_4^x\sigma_5^x\sigma_6^x\sigma_7^x{\color{red}\sigma_7^z}\sigma_8^x\sigma_9^x\left|\psi\right\rangle &= ([\sigma_7^z,\sigma_8^x\sigma_9^x]=0) = \\
{\color{red}-}\sigma_4^x\sigma_5^x\sigma_6^x{\color{red}\sigma_7^z}\sigma_7^x\sigma_8^x\sigma_9^x\left|\psi\right\rangle &= ([\sigma_4^x\sigma_5^x\sigma_6^x,\sigma_7^z]=0) = \\
{\color{red}-\sigma_7^z}\underbrace{\sigma_4^x\sigma_5^x\sigma_6^x\sigma_7^x\sigma_8^x\sigma_9^x\left|\psi\right\rangle}_{\left|\psi\right\rangle} &= {\color{red}-\sigma_7^z\left|\psi\right\rangle}
\end{aligned}$$[b]

	$\sigma_1^x\sigma_2^x\sigma_3^x\sigma_4^x\sigma_5^x\sigma_6^x$	$\sigma_4^x\sigma_5^x\sigma_6^x\sigma_7^x\sigma_8^x\sigma_9^x$
$\left|\psi\right\rangle = \psi_0\left|0_L\right\rangle + \psi_1\left|1_L\right\rangle$	1	1
σ_1^z	-1	1
σ_2^z	-1	1
σ_3^z	-1	1
σ_4^z	-1	-1
σ_5^z	-1	-1
σ_6^z	-1	-1
σ_7^z	1	-1
σ_8^z	1	-1
σ_9^z	1	-1

[a]Ver anexo 7.9.2 para los cálculos correspondientes

[b]Sea A y B actuando en V_a y V_b respectivamente $[A_a\otimes \mathbb{1}_b, \mathbb{1}_a\otimes B_b]=0$.

Sea un estado $\left|\psi\right\rangle = \psi_0\left|0_L\right\rangle + \psi_1\left|1_L\right\rangle$ en donde los errores $\{\sigma_1^z,\sigma_2^z,\sigma_3^z\}$ tienen el mismo efecto y se pueden corregir aplicando σ_1^z, σ_2^z o σ_3^z. Por ejemplo, $\sigma_1^Z{\color{red}\sigma_3^z}\left|GHZ^{\pm}\right\rangle = \sigma_1^z\left|GHZ^{\mp}\right\rangle = \left|GHZ^{\pm}\right\rangle$

Observación: $\sigma_a^z\left|GHZ^{\pm}\right\rangle_{abc} = \sigma_b^z\left|GHZ^{\pm}\right\rangle_{abc} = \sigma_c^z\left|GHZ^{\pm}\right\rangle_{abc} = \left|GHZ^{\mp}\right\rangle_{abc}$

Ejercicio

¿Qué pasa con un error σ_i^y donde $i = 1\ldots$?

Pista: $\sigma^z\sigma^x = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} = i\sigma^y$.

$$\sigma_2^y\left|\psi\right\rangle = \frac{1}{i}\sigma_2^z\sigma_2^x(\psi_0\left|0_L\right\rangle + \psi_1\left|1_L\right\rangle)$$

$$Z_1Z_2(Y_2\left|\psi\right\rangle) = \frac{1}{i}\underbrace{Z_1Z_2Z_2}_{Z_2Z_1Z_2}X_2\left|\psi\right\rangle = \frac{1}{i}Z_2\underbrace{Z_1Z_2X_2\left|\psi\right\rangle}_{-X_2\left|\psi\right\rangle} = -\frac{1}{i}Z_2X_2\left|\psi\right\rangle = -Y_2\left|\psi\right\rangle$$

Se pueden hacer cálculos análogos para los otros observables.

5.5. Estados mezcla

Hemos visto que el estado de un sistema cuántico se representa con elementos de un EV. Sin embargo, hay situaciones en las que esta descripción no es la más adecuada (aunque es correcta). Por ejemplo, consideremos un experimento en el que tenemos una moneda y si el resultado es "cero" preparamos un qubit en el estado $|0\rangle$, si el resultado en "cruz" preparamos un qubit en el estado $|1\rangle$. Para un observador sin acceso a la información "lado de la moneda" ¿cual es el estado del qubit?

Para responder a esa pregunta introducimos la noción mezcla estadística. Vamos a reformular (algunos de) los postulados de la mecánica cuántica de manera que se pueda tener en cuenta las carencias de información sobre el estado de un sistema.

Definición. Llamaremos operador densidad puro asociado a un estado $|\psi\rangle$, el operador $f = |\psi \times \psi|$.

Observaciónes.

- tr[1]$*f = 1$
  $\mathrm{trf} = \sum_{\mathrm{j}} \langle \mathrm{v_j} | \mathrm{f} | \mathrm{v_j} \rangle = \underbrace{\sum_j \langle v_j|\psi\rangle \langle\psi|v_j\rangle}_{\substack{\text{el producto es} \\ \text{conmutativo en } \mathbb{C}}} = \sum_{\mathrm{j}} \langle\psi|\mathrm{v_j}\rangle \langle \mathrm{v_j}|\psi\rangle = \langle\psi| \sum_{\mathrm{j}} |\mathrm{v_j} \times \mathrm{v_j}\, |\psi\rangle ==$
  $\langle\psi|\psi\rangle = 1$

- f es un proyector
  $f^2 = f.\ |\psi \times \underbrace{\psi\,|\psi\rangle}_{1} \langle\psi| = |\psi \times \psi|$
  $f \geq 0$: $\forall\, |\phi\rangle \in V$, $\langle\phi|\, f\, |\phi\rangle = |\,\langle\phi|\psi\rangle\,|^2 \geq 0$

Definición. Un operador densidad es cualquier combinación conversa de proyectores asociados a estado, es decir cualquier operador de la forma $f = \sum_{j=1}^{A} P_\alpha |\psi_\alpha \times \psi_\alpha|$ donde

$$\begin{cases} P_\alpha \geq 0 \text{ donde } \forall_\alpha = 1, \ldots, A \\ \sum_{\alpha=1}^{A} P_\alpha = 1 \end{cases}$$

[1]Dada una base $\perp^{mal}\{|v_i\rangle\}$ de un EV, la traza de un operador x. Ver anexo 7.10 para más información.

Interpretación de (*). Considera un proceso en el que se muestre una variable aleatoria $\alpha \in \{1, \dots, A\}$ según la distribución de probabilidad $\{P_\alpha\}$ y se prepara el sistema en el estado $|\psi_j \times \psi_j|$ cuando se obtiene el resultado α. Esta interpretación no es única. El ejemplo anterior del qubit y la moneda:

$$f = Proba(\text{“cero”})|0 \times 0| + Proba(\text{“cruz”})|1 \times 1| = \frac{1}{2}|0 \times 0| + \frac{1}{2}|1 \times 1|$$

Como para los operadores densidad puros $\mathrm{tr} f = 1$ y $f \geq 0$. Sin embargo, $f \neq f^2$ en general.

Para entender la no-unicidad a través de un ejemplo sean
$$|\pm z\rangle \text{ estado propios de } \omega^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$|\pm x\rangle \text{ estado propios de } \omega^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

y $\begin{matrix} f = \frac{1}{2}|+z \times +z| + \frac{1}{2}|-z \times -z| \\ f = \frac{1}{2}|+x \times +x| + \frac{1}{2}|-x \times -x| \end{matrix}$. Sea $\begin{matrix} |\psi\rangle = \psi + |^+z\rangle + \psi - |^-z\rangle \\ |\phi\rangle = \phi + |^+z\rangle + \phi - |^-z\rangle \end{matrix}$. Comparar $\langle\psi| f |\phi\rangle$ con $\langle\psi| f' |\phi\rangle$ o si preferimos podemos comparar f y f' directamente:

$$\begin{aligned} |^+x\rangle &= \frac{1}{\sqrt{2}}|+z\rangle + \frac{1}{\sqrt{2}}|-z\rangle, \ \langle^+x| = \frac{1}{\sqrt{2}}\langle+z| + \frac{1}{\sqrt{2}}\langle-z| \\ |^-x\rangle &= \frac{1}{\sqrt{2}}|+z\rangle - \frac{1}{\sqrt{2}}|-z\rangle, \ \langle^-x| = \frac{1}{\sqrt{2}}\langle+z| - \frac{1}{\sqrt{2}}\langle-z| \end{aligned}$$

$$|^+x \times^+ x| = \left(\frac{1}{\sqrt{2}}\right)^2 \left[|+z\rangle\langle^+z| + |^-z\rangle + |^+z \times^- z| + |^-z \times^+ z|\right]$$
$$|^-x \times^- x| = \left(\frac{1}{\sqrt{2}}\right)^2 \left[|^+z \times^+ z| + |^-z \times^- z| - |^+z \times^- z| - |^-z\rangle\langle^-z|\right]$$

$$\begin{aligned} f' &= \frac{1}{2}|^+x \times^+ x| + \frac{1}{2}|^-x \times^- x| = \frac{1}{2}x^2x\left(\frac{1}{2}\right)^2|^+z \times^+ z| + \frac{1}{2}x2x\left(\frac{1}{\sqrt{2}}\right)^2|^-z \times^- z| = \\ &= \frac{1}{2}|^+z \times^+ z| + \frac{1}{2}|^-z \times^- z| = \\ &= f \end{aligned}$$

Pregunta

“En possent”: ¿Cómo se prepara un qubit en un estado puro? $|^+ \times^+ z| = |0 \times 0|$ por ejemplo. Lo veremos más adelante.

5.5.1. Evolución temporal de un operador densidad

$$
\begin{aligned}
\frac{\partial}{\partial t} f(t) &= \frac{\partial}{\partial t}\left(\sum_\alpha P_\alpha |\psi_\alpha(t) \times \psi_\alpha(t)|\right) = \sum_\alpha P_\alpha \frac{\partial}{\partial t}\left[|\psi_\alpha(t)\rangle \langle\psi_\alpha(t)|\right] = \\
&= \sum_\alpha P_\alpha \left\{ \left(\frac{\partial}{\partial t}|\psi_\alpha(t)\rangle\right)\langle\psi_\alpha(t)| + |\psi_\alpha(t)\rangle \left(\underbrace{\frac{\partial}{\partial t}\langle\psi_\alpha(t)|}_{((fg)'=f'g+fg')}\right)\right\} = \\
&= \sum_\alpha P_\alpha \left\{\frac{1}{i\hbar}\mathcal{H}|\psi_\alpha(t)\rangle\langle\psi_\alpha(t)| + |\psi_\alpha(t)\rangle \frac{1}{-i\hbar}\langle\psi_\alpha(t)|\mathcal{H}\right\} = \\
&= \sum_\alpha P_\alpha \frac{1}{i\hbar}\left\{\mathcal{H}|\psi_\alpha(t)\rangle\langle\psi_\alpha(t)| - |\psi_\alpha(t)\rangle\langle\psi_\alpha(t)|\mathcal{H}\right\} = \frac{1}{i\hbar}\left\{\mathcal{H}f(t) - f(t)\mathcal{H}\right\} = \\
&= \frac{1}{i\hbar}[\mathcal{H}, f(t)] = i\hbar\frac{\partial}{\partial} f(t) = [\mathcal{H}, P(t)] \text{ evolución temporal del operador densidad}
\end{aligned}
$$

5.5.2. Postulados de la mecánica cuántica (versión 2)

- El estado de un sistema cuántico esta dado por un operador densidad actuando sobre un espacio vectorial.
- Si un observable A tiene autovalores $\{G_n; n = 1, \dots, real(A)\}$ $Proba(G_n)$ para un sistema en estado δ viene dado por $\mathrm{tr(\pi_n f)}$ donde π_n es el proyector sobre el SEV de V asociado al autovalor G_n.
- Si se encuentra el resultado G_n el estado inmediatamente después de la medida: $f' = \dfrac{\pi_n f \pi_n}{\mathrm{tr(\pi_n f \pi_n)}}$.

Ejemplo

Un input en estado δ desconocido. Medimos σ^z y los resultados posibles son $|^{\pm}z\rangle$. Si se obtiene $|^{-}z\rangle$ (puerta Hadamard) $\frac{1}{\sqrt{2}}|+\rangle_z - \frac{1}{\sqrt{2}}|-\rangle_z$ y se repite la medida

$$
\begin{cases}
|^{+}z\rangle \text{ con probabilidad } \left(\frac{1}{2}\right) \\
|^{-}z\rangle \text{ con probabilidad } \left(\frac{1}{2}\right)
\end{cases}
\text{etc.}\dots
$$

Ejercicio

Probabilidad de obtener el estado $|^{+}z\rangle$ en n repeticiones como mucho:

$$1-\left(\frac{1}{2}\right)^{n}$$

5.5.3. Traza parcial

A veces la información incompleta sobre un sistema proviene del hecho de que el sistema considerado es parte de un sistema más amplio.

Definición. Un operador densidad de un producto tensorial de EV $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ es producto si es de la forma $\delta_1 \otimes \delta_2 \otimes \cdots \otimes \delta_n$.

Los operadores densidad que no son producto son muy interesantes. Para satisfacer, consideraremos $n = 2$ y consideraremos la medida de observables de la forma X_1, es decir, observables cuyo soporte es el subsistema 1. Nos gustaria tener una manera de describir nuestra ignorancia del subsistema Z. Sea δ el estado del sistema 1 y 2. Sea $f_{1,2}$ operador densidad asociado al sistema. Queremos encontrar un operador de densidad f_1 tal que $\forall$ operador X actuando en V_1:

$$\mathrm{tr(f(X_1 \otimes \mathbb{1}_2) = tr(f_1X_1)(*^1)}$$

Ejemplo

$$\begin{aligned}
f &= (\mathbb{1}_1 \otimes \mathbb{1}_2) f (\mathbb{1}_1 \otimes \mathbb{1}_2) = \\
&= \left(\sum_{j_1} |v_{j_1}\rangle \langle v_{j_1}|\right) \otimes \left(\sum_{j_2} |w_{j_2}\rangle \langle w_{j_2}|\right) f \left(\sum_{k_1} |v_{k_1}\rangle \langle v_{k_1}|\right) \otimes \left(\sum_{k_2} |w_{k_2}\rangle \langle w_{k_2}|\right) = \\
&= \sum_{\substack{j_1 j_2 \\ k_1 k_2}} \langle v_{j_1}, w_{k_1}| f |v_{j_2}, w_{k_2}\rangle |v_{k_1}, w_{k_2}\rangle \langle v_{j_1}, w_{j_2}|
\end{aligned}$$

donde $\begin{cases} \{|v_j\rangle : j = 1, \ldots, dim(V_1)\} \text{ base } \perp^{mal} \text{ de } V_1 \\ \{|w_k\rangle : k = 1, \ldots, dim(V_2)\} \text{ base } \perp^{mal} \text{ de } V_2 \end{cases}.$

$$\begin{aligned} \mathrm{tr}\left(\mathrm{f}(\mathrm{X}_1 \otimes \mathbb{1}_2)\right) &= \sum_{\substack{j_1 j_2 \\ k_1 k_2}} \langle v_{j_1} w_{k_1}| \, f \, |v_{j_2} w_{k_2}\rangle \langle v_{j_1}| \, X_1 \, |v_{k_1}\rangle \, \delta_{k_2 j_2} = \\ &= \sum_{j_1 k_1} \left(\sum_{j_2} \langle v_{j_2} w_{k_1}| \, f \, |v_{j_2} w_{k_2}\rangle \right) \langle v_{j_1}| \, X_1 \, |v_{k_1}\rangle \end{aligned}$$

$(**)$ Caracteriza f_A completamente:

$$f_A = \mathbb{1}_A f_A \mathbb{1}_A = \sum_{j_2} |v_{j_2}\rangle \langle v_{j_2}| \, f_A \sum_{j_1} |v_{j_1}\rangle \langle v_{j_1}| = \sum_{j_1 j_2} \langle v_{j_2}| \, f_A \, |v_{j_1}\rangle \, |v_{j_2}\rangle \langle v_{j_1}|$$

$\mathrm{trf_A} = 1$ $f_A = f_A^* \Leftarrow f_{AB} = f_{AB}^*$

Queremos:

$$\underbrace{\sum_{jk} \langle v_j, w_k| \, f_{1,2}(X_1 \otimes \mathbb{1}_2) \, |v_j, w_k\rangle}_{LHS} = \underbrace{\sum_j \langle v_j| \, f_1 X \, |v_j\rangle}_{RHS}$$

$$\begin{aligned} LHS = \sum_{jk} \langle v_j, w_k| \, f_{1,2} &\Bigg(\underbrace{\sum_{j_1 j_2} \langle v_{j_1}| \times |v_{j_2}\rangle \, |v_{j_1} \times v_{j_2}|}_{X_1} \otimes \underbrace{\sum_l |w_l \times w_l|}_{\mathbb{1}_2} \Bigg) |v_j, w_k\rangle = \\ &= \sum_{j,k} \sum_{j_1,j_2} \sum_l \langle v_{j_1}| \times |v_{j_2}\rangle \langle v_{j_1}, w_k| \, f_{1,2} \, |v_{j_1}, w_l\rangle \langle v_{j_2}, w_l|v_j, w_k\rangle = \\ &= \sum_{j,k} \sum_l \sum_{j_1,j_2} \langle v_{j_1}| \times |v_{j_2}\rangle \langle v_j, w_k| \, f_{1,2} (\underbrace{|v_{j_1}\rangle \langle v_{j_2}| \otimes |w_l \times w_l|}_{|v_{j_1}, w_l\rangle \langle v_{j_2}, w_l|}) \, |v_j, w_k\rangle = \\ &= \sum_{j,k,l,j_1,j_2} \langle v_{j_1}| \times |v_{j_2}\rangle \langle v_j, w_k| \, f_{1,2} \, |v_{j_1}, w_l\rangle \underbrace{\langle v_{j_2}, w_l|v_j, w_k\rangle}_{\delta_{j_1 j_2} \delta_{lk}} = \\ &= \sum_{k,j_1,j_2} \langle v_{j_1}| \times |v_{j_2}\rangle \langle v_{j_2}, w_k| \, f_{1,2} \, |v_{j_1}, w_k\rangle \end{aligned}$$

$$\begin{aligned} RHS &= \sum_j \langle v_j| \, f_1 \sum_{j_1 j_2} |v_{j_1}\rangle \langle v_{j_1}| \times |v_{j_2}\rangle \underbrace{\langle v_{j_2}|v_j\rangle}_{\delta_{j_1 J-2}} = \\ &= \sum_{j_1 j_2} \langle v_{j_2}| \, f_1 \, |v_{j_1}\rangle \langle v_{j_1}| \times |v_{j_2}\rangle \end{aligned}$$

RHS es la solución de $(*^1)$.

Caracteriza f_1 completamente:

$$f_1 = \mathbb{1}_1 f_1 \mathbb{1}_1 = \sum_{j_2} |v_{j_2}\rangle \langle v_{j_2}| f_1 \sum_{j_1} |v_{j_1}\rangle \langle v_{j_1}| = \sum_{j_1 j_2} \langle v_{j_2}| f_1 |v_{j_1}\rangle |v_{j_2}\rangle \langle v_{j_1}|$$

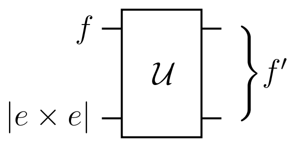
$\mathrm{tr} f_1 = 1$ donde $f_1 = f_1^* \Leftarrow f_{1,2} = f_{1,2}^*$, $f_1 \geq 0 \Leftarrow f_{1,2} \geq$

$$\mathrm{trf_1} = \sum_{\mathrm{j}} \langle \mathrm{v_j}| \mathrm{f_1} |\mathrm{v_j}\rangle = \sum_{\mathrm{j}} \left(\sum_{\mathrm{k}} \langle \mathrm{v_j}, \mathrm{w_k}| \mathrm{f_{1,2}} |\mathrm{v_j}, \mathrm{w_k}\rangle \right) = \mathrm{trf_{1,2}} = 1$$

5.6. Canales cuánticos

Hemos visto que la evolución de un sistema cuántico aislado inicialmente en un estado puro está regido por la ecuación de Schrödinger , es decir, es unitaria. En el formalismo de los operadores de densidad $\frac{\partial}{\partial t} f(t) = \frac{1}{i\hbar}[\mathcal{H}, f(t)]$. Si $\mathcal{H}$ no depende del tiempo, se puede ver fácilmente que $f(t) = \mathcal{U} f_0 \mathcal{U}^*$ donde $\mathcal{U}$ es unitaria.

¿Qué pasa cuando $\mathcal{U}$ actúa conjuntamente sobre un sistema que nos interesa (porque conlleva información asequible) y un entono de este sistema sobre el cual no podemos actuar de ninguna manera? Por ejemplo:



donde f es el estado inicial del sistema y $|e\rangle$ el estado inicial del entorno supuesto puro.

$\{|v_i\rangle\}$ base $\perp^{mal}$ para el sistema considerado $\{|w_k\rangle\}$ base para el entorno.

$$f \otimes |e \times e| = \sum_{ij} f_{ij} |v_i\rangle \langle v_j| \otimes |e \times e|$$

$$\Rightarrow f' = \sum_{ij} f_{ij} (\mathbb{1}_f \otimes \mathbb{1}_f) \mathcal{U} \left(|v_i\rangle \langle v_j| \otimes |e \times e| \right) \mathcal{U}^* (\mathbb{1}_f \otimes \mathbb{1}_f)$$

$$\Rightarrow f'_{SE} = \sum_{lj} f_{lj} \sum_{k_1 k_2} |v_{k_1}, w_{k_2}\rangle \langle v_{l_1}, w_{k_2}| \mathcal{U} |v_i, e\rangle \langle v_j, e| \mathcal{U}^* \sum_{l_1 l_2} |v_{l_1}, w_{l_2}\rangle \langle v_{l_1}, w_{l_2}| =$$

$$\sum_{i,j} \sum_{k_1 k_2} \sum_{l_1 l_2} f_{ij} \langle v_{k_1}, v_{k_2}| \mathcal{U} |v_i, e\rangle \langle v_j, e| \mathcal{U}^* |v_{l_1}, w_{l_2}\rangle |v_{k_1}, w_{k_2}\rangle \langle v_{l_1}, w_{l_2}|$$

No tenemos acceso a todo el estado f'_{SE}, sino sólo a la restricción al subsistema $\mathcal{S}$. Tomando la traza parcial

$$S'_{\mathcal{S}} = \sum_{i,j} \sum_{k_1 l_1} \sum_{k_2} \langle v_{k_1}, w_{k_2}| \mathcal{U} |v_i, e\rangle \langle v_j, e| \mathcal{U}^* |v_{l_1}, w_{k_2}\rangle |v_{k_1} \times v_{l_1}|$$

Definimos el siguiente operador lineal:

$$M_{k_2} : V_{\mathcal{S}} \to V_{\mathcal{S}}; |v_i\rangle \to \sum_{k_1} \langle v_{k_1}, w_{k_2}| \mathcal{U} |v_i, e\rangle |v_{k_1}\rangle \text{ donde } \forall k_2 = 1, \ldots, dimV_e$$

Con estos operadores se puede explicar $f'_{\mathcal{S}} = \sum_{i,j} f_{ij} \sum_{k_2} M_{k_2} |v_i\rangle \langle v_j| M^*_{k_2} \Rightarrow f'_{\mathcal{S}} = \sum_{k_2} M_{k_2} f M^*_{k_2}$. Se puede demostrar, usando la unitariedad de $\mathcal{U}$, que $\sum_{k_2} M^*_{k_2} M_{k_2} = \mathbb{1}_f$.

En resumen, el efecto de cualquier unitaria que actúa conjuntamente sobre "SE" se puede modelizar por un conjunto de operadores $\{M_{k_2}\}$ satisfaciendo $f'_{\mathcal{S}} = \sum_{k_2} M_{k_2} f M^*_{k_2}$ y $\sum_{k_2} M^*_{k_2} M_{k_2} = \mathbb{1}_f$. (Sin demostración) Inversamente, $\forall$ conjunto $\{M_{k_2}\}$ que cumple con $f'_{\mathcal{S}} = \sum_{k_2} M_{k_2} f M^*_{k_2}$, $\sum_{k_2} M^*_{k_2} M_{k_2} = \mathbb{1}_f$. Se puede asociar un entorno E y una unitaria $\mathcal{U}_{SE}$ y un estado inicial tal que $M_{k_2} : V_{\mathcal{S}} \to V_{\mathcal{S}}; |v_i\rangle \to \sum_{k_1} \langle v_{k_1}, w_{k_2}| \mathcal{U} |v_i, e\rangle |v_{k_1}\rangle$ donde $\forall k_2 = 1, \ldots, dimV_e$ se cumpla.

Ejemplo para un qubit

$f \to f' = p_0 f + p_x \sigma^x f \sigma^x + p_y \sigma^y f \sigma^y + p_z \sigma^z f \sigma^z$ donde $p_0, p_x, p_y, p_z \geq 0$ y $p_0 + p_x + p_y + p_z = 1$. En el caso $p_x = p_y = p_z = p$ se puede ver que este canal actúa como $f \to f' = (1-p) f + p\frac{\mathbb{1}}{2}$

Ejercicio

Calcula las trazas parciales para los siguientes estados:

- $|\eta_A \times \eta_A| \otimes |\eta_B \times \eta_B|$
  $f_1 = \sum_l |\eta_A\rangle \langle \eta_A| \langle w_l|\eta_B\rangle \langle \eta_B|w_l\rangle = |\eta_A\rangle \langle \eta_A| \underbrace{\sum_l \langle \eta_B|w_l\rangle \langle w_l|\eta_B\rangle}_{\langle \eta_B|\mathbb{1}|\eta_B\rangle = 1} = |\eta_A \times \eta_A|$

- $\sum_\alpha P_\alpha |\psi_A^\alpha \times \psi_A^\alpha| \otimes |\psi_B^\alpha \times \psi_B^\alpha|$
- $|\phi^+\rangle \langle\phi^+|$
- $|\psi^- \times \psi^-|$
- $|GHZ^+ \times GHZ^+|$

Anexos

7.7. Álgebra lineal

7.7.1. Cálculos de $cos\left(\theta-\frac{\pi}{2}\right)$ y $sin\left(\theta-\frac{\pi}{2}\right)$

$\mathbf{cos}\left(\theta-\frac{\pi}{2}\right)$

$$\begin{aligned} cos\left(\theta-\frac{\pi}{2}\right) &= \frac{1}{2}\left(e^{i(\theta-\frac{\pi}{2})}+e^{-i(\theta-\frac{\pi}{2})}\right)=\frac{1}{2}\left(-ie^{i\theta}+ie^{-i\theta}\right)= \\ &= \frac{1}{2}\left(-ie^{i\theta}+ie^{-i\theta}\right)=\frac{-i}{2}\left(e^{i\theta}-e^{-i\theta}\right)=\frac{1}{2i}\left(e^{i\theta}-e^{-i\theta}\right)= \\ &= sin\left(\theta\right) \end{aligned}$$

$\mathbf{sin}\left(\theta-\frac{\pi}{2}\right)$

$$sin\left(\theta-\frac{\pi}{2}\right)=-sin\left(\frac{\pi}{2}-\theta\right)=-cos\left(\theta\right)$$

7.8. Sistema de partículas

$$\left[\frac{1}{\sqrt{2}}\langle 0,0|+\frac{1}{\sqrt{2}}\langle 1,1|\right]\left[\frac{1}{\sqrt{2}}|0,0\rangle+\frac{1}{\sqrt{2}}|1,1\rangle\right]=\textstyle\sum_{i,j=0}^{1}\left(\frac{1}{\sqrt{2}}\right)^2\underbrace{\langle i,i|j,j\rangle}_{\delta_{ij}}=$$

$$=\frac{1}{2}\underbrace{\delta_{00}}_{1}+\frac{1}{2}\underbrace{\delta_{11}}_{1}+\frac{1}{2}\underbrace{\delta_{01}}_{0}+\frac{1}{2}\underbrace{\delta_{10}}_{0}=1$$

7.9. Código a 9 qubits

7.9.1. Cálculo de $|GHZ\rangle$

$$\sigma_1^x\sigma_2^x\sigma_3^x \left|GHZ^+\right\rangle_{123} = \frac{1}{\sqrt{2}}(\underbrace{\sigma_1^x\sigma_2^x\sigma_3^x \left|000\right\rangle}_{|111\rangle} + \underbrace{\sigma_1^x\sigma_2^x\sigma_3^x \left|111\right\rangle}_{|000\rangle}) = + \left|GHZ^+\right\rangle_{123}$$

De manera análoga:

$$\sigma_1^x\sigma_2^x\sigma_3^x \left|GHZ^-\right\rangle_{123} = \frac{1}{\sqrt{2}}(\underbrace{\sigma_1^x\sigma_2^x\sigma_3^x \left|000\right\rangle}_{|111\rangle} - \underbrace{\sigma_1^x\sigma_2^x\sigma_3^x \left|111\right\rangle}_{|000\rangle}) = - \left|GHZ^-\right\rangle_{123}$$

7.9.2. Cálculo de σ

$$\sigma^z\sigma^x + \sigma^x\sigma^z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} =$$
$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

7.10. Traza de un operador x

$$\mathrm{tr}\times = \sum_{\mathrm{i}} \langle \mathrm{v_i}| \times |\mathrm{v_i}\rangle$$

$$\times = \mathbb{1} \times \mathbb{1} = \sum_i |v_i \times v_i| \times \sum_j |v_j \times v_j| = \sum_{i,j} \langle v_i| \times |v_j\rangle \, |v_i\rangle \, \langle v_j|$$

Bibliografía

[1] M. A. Nielsen and I. Chuang, “Quantum computation and quantum information,” 2002.

[2] A. Y. Kitaev, A. Shen, M. N. Vyalyi, and M. N. Vyalyi, *Classical and quantum computation.* No. 47, American Mathematical Soc., 2002.

[3] J. Preskill, “Course information for physics 219/computer science 219 quantum computation (formerly physics 229),” 2021.

Índice de siglas

a. a. auto-adjunto. 26, 30

BV base vectorial. 16–20

BVs bases vectoriales. 15

CC Computación Cuántica. 1

EV espacio vectorial. 10–15, 17, 24–27, 32–35, 40, 44, 47, 57, 68, 71

EVs espacios vectoriales. 10

QFT Transformada cuántica de Fourier. 47, 49, 54, 55

SBV subbase vectorial. 17

SEV subespacio vectorial. 13, 14, 18, 26, 27, 57, 70

SEVs subespacios vectoriales. 13, 14

TF Transformada de Fourier. 47

Markel Álvarez Martínez

markelal@ucm.es

Mayo 2022

Últ. actualización 6 de abril de 2022