UNIVERSIDAD DE VALLADOLID

INSTITUTO DE INVESTIGACIÓN EN MATEMÁTICAS

24 de octubre de 2013

El abecé de la computación cuántica

JUANJO RUÉ[1] Y SEBASTIAN XAMBÓ[2]

[1] INSTITUT FÜR MATHEMATIK, FREIE UNIVERSITÄT BERLIN

[2] FME Y FIB / MA2

UNIVERSITAT POLITÈCNICA DE CATALUNYA

ÍNDICE

PRELIMINARES

Computación clásica

Números binarios (Leibnitz, Boole, Shannon,…)

$\boldsymbol{B} = \{0,1\}$ (*bits*). $1 + 1 = 0$

$33_{(10} = \ 100001_{(2} = 2^5 + 2^0$

► *Toda información se puede representar por una cadena de bits.*

Textos

$'A' \rightarrow 65_{(10} = 1000001, \ldots, 'z' \rightarrow \ 122_{(10} = 1111010$, … (ascii-7)

(otros códigos: ascii-8, Unicode, utf-8, utf-16, …)

Sonido

44100 valores de presión por segundo, expresados en 16 bits (p. ej.).

1s de música (sin comprimir) $\simeq$ 88 Kb

Bach

Imagen

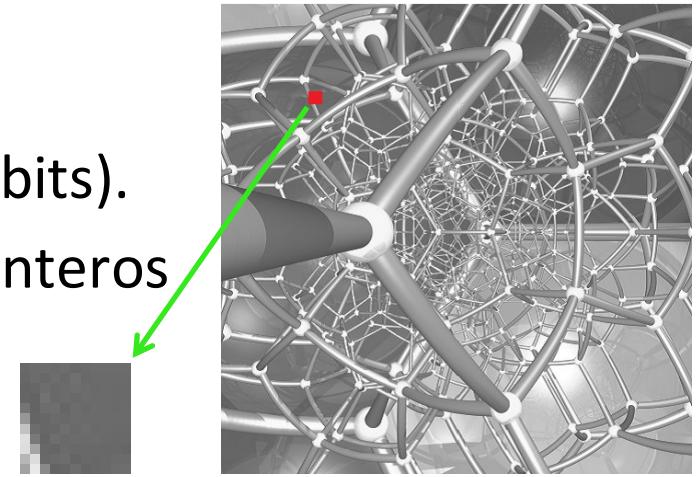
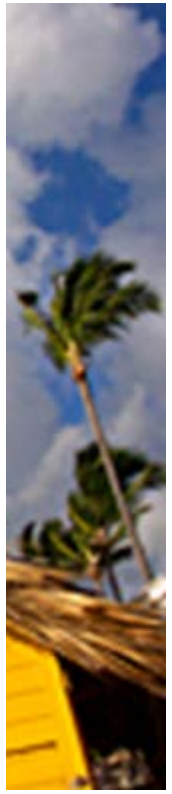


Figura 256 × 256 píxeles, 256 niveles de gris (8 bits). (matriz cuadrada X de orden 256 con valores enteros entre 0 y 255, $\simeq$ 65536 Kb). Por ejemplo:

X(100:110,100:110) =

105	108	109	107	109	104	106	108	108	108	108
103	108	104	109	105	112	105	107	107	107	107
101	103	109	105	107	110	108	106	107	106	106
102	100	114	105	107	105	108	107	107	106	106
116	100	109	110	102	108	105	108	107	106	107
150	101	103	107	105	108	107	107	107	107	107
194	109	103	104	110	106	109	106	107	106	106
223	121	101	110	106	108	107	108	106	105	105
221	165	104	102	107	105	105	105	104	105	102
182	220	105	107	109	101	105	104	105	107	107
162	233	137	100	102	109	101	104	105	109	110



Una computación clásica es una aplicación

$f: \boldsymbol{B}^n \to \boldsymbol{B}^m$ (tipo $n \to m$).

El número de computaciones de tipo $n \to m$ es $(2^m)^{2^n}$.

Por ejemplo: $\#\{8 \to 8\} = 256^{256}$ (617 cifras decimales).

$1 \to 1$				
x	f_1	f_2	f_3	f_4
0	0	1	0	1
1	0	0	1	1
	0	$\bar{x}$	x	**1**

$2 \to 1$																	
x	y	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	1	0	0	0	1	1	1	0	0	0	1	1	1	0	1
1	0	0	0	1	0	0	1	0	0	1	1	0	1	1	0	1	1
0	1	0	0	0	1	0	0	1	0	1	0	1	1	0	1	1	1
1	1	0	0	0	0	1	0	0	1	0	1	1	0	1	1	1	1
		0	$\bar{x}\bar{y}$	$x\bar{y}$	$\bar{x}y$	xy	$\bar{y}$	$\bar{x}$	$\overline{+}$	$+$	x	y	$\overline{xy}$	$\overline{\bar{x}y}$	$\overline{x\bar{y}}$	$\overline{\bar{x}\bar{y}}$	$\overline{\mathbf{0}}$
										XOR			NAND			V	**1**

$$+(x,y) = x\bar{y} \vee \bar{x}y = \overline{\overline{x\bar{y}}\;\overline{\bar{x}y}}\,, \quad \overline{+}(x,y) = \overline{x\bar{y}}\;\overline{\bar{x}y}$$

Ley de Morgan

► *Toda computación se puede resolver en una secuencia de operaciones booleanas.*

Ejemplo. Consideremos la computación

$$f: \boldsymbol{B}^3 \to \boldsymbol{B},$$

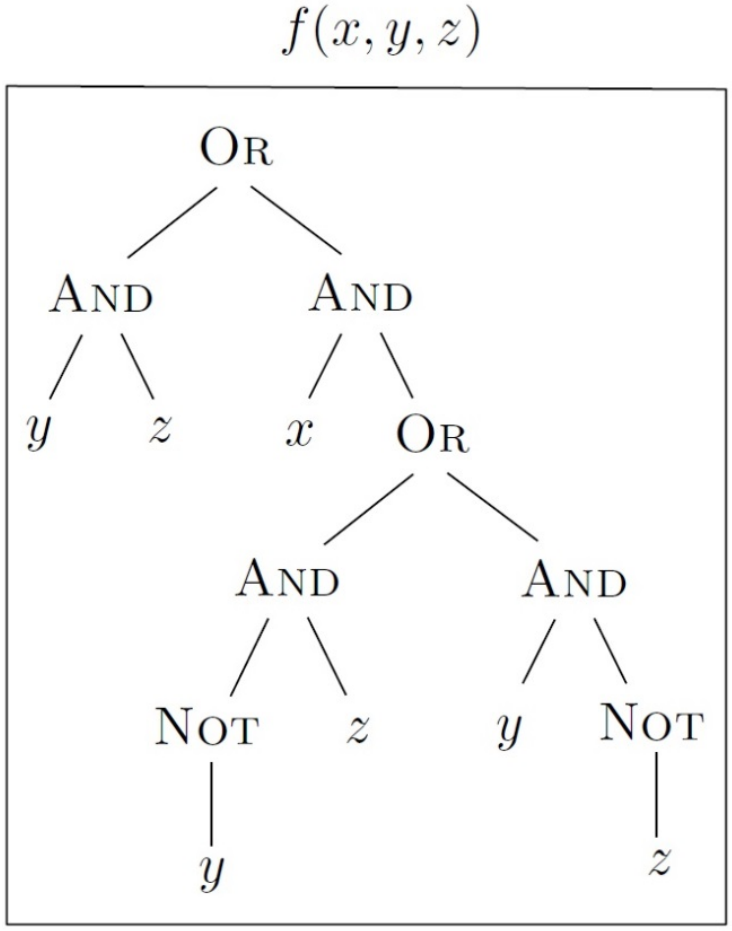
$$\mathbf{111}, 011, 101, 110 \mapsto 1$$

$$\mathbf{000}, 100, 010, 001 \mapsto 0$$

(descodificador del código [1,3] de repetición). Entonces

$$f(xyz) = xyz \vee \bar{x}yz \vee x\bar{y}z \vee xy\bar{z}$$

$$= yz \vee x(\bar{y}z \vee y\bar{z})$$



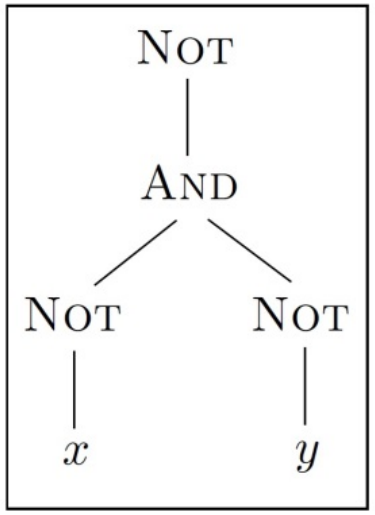
- *Toda computación se puede resolver en una secuencia de puertas lógicas elementales:*

$$\text{NOT}[j](b_1, \ldots, b_n) = \bar{b}_j$$

$$\text{NAND}[j,k]\,(b_1, \ldots, b_n) = \overline{b_j \cdot b_k} = \bar{b}_j \vee \bar{b}_k$$

- *Toda computación se puede incrustar en una computación de tipo $n \to n$ reversible (biyectiva).*

$\text{OR}(x, y)$



Ejemplo.

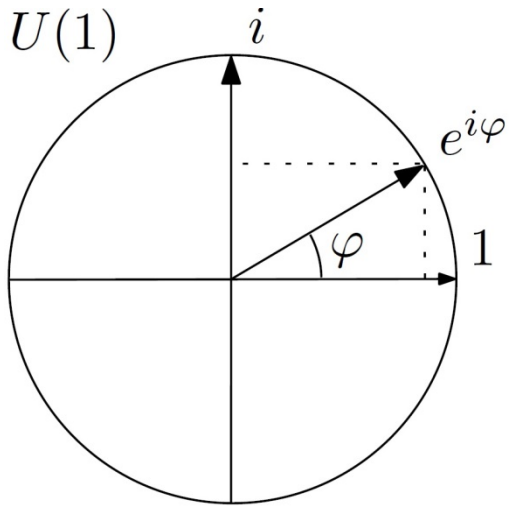
x	00	01	10	11
AND	0	0	0	1

x	**00**0	**01**0	**10**0	**11**0	001	011	101	111
AND	00**0**	01**0**	10**0**	11**1**	001	011	101	111

$$\text{AND}(x, y, z) = (x, y, xy) \text{ if } z = 0,$$
$$= (x, y, z) \text{ if } z = 1.$$

Notaciones

$\mathbb{R}$, $\mathbb{C}$



Si $\xi = a + bi \in \mathbb{C}$, $\bar{\xi} = a - bi$ es el *conjugado* de ξ.

- $\bar{\xi}\xi = (a - bi)(a + bi) = a^2 + b^2 = |\xi|^2$,
  siendo $|\xi| = \sqrt{a^2 + b^2}$ el *módulo* de ξ.
- Los números complejos de módulo 1 tienen la forma (Euler)

  $e^{i\varphi} = \cos\varphi + i \sin\varphi$, $\varphi \in \mathbb{R}$ (*factores de fase*, o *fasores*).

  Forman un grupo con el producto (el grupo $U(1) = S^1$):

  $e^{i\varphi} \cdot e^{i\varphi'} = e^{i(\varphi+\varphi')}$.

- Si $\xi \in \mathbb{C} - \{0\}$, existe un único $\varphi \in [0,2\pi)$, el *argumento* de ξ, tal que

  $\xi = |\xi| e^{i\varphi}$ (*forma polar* de ξ).

Espacio Hermítico

Es un *espacio vectorial* ***complejo*** E dotado de un producto escalar $\langle \boldsymbol{x}|\boldsymbol{y}\rangle$ tal que

1. $\langle \boldsymbol{x}|\xi\boldsymbol{y}+\xi'\boldsymbol{y}'\rangle = \xi\langle \boldsymbol{x}|\boldsymbol{y}\rangle + \xi'\langle \boldsymbol{x}|\boldsymbol{y}'\rangle, \xi, \xi' \in \mathbb{C}$
2. $\langle \boldsymbol{x}|\boldsymbol{y}\rangle = \overline{\langle \boldsymbol{y}|\boldsymbol{x}\rangle}$

   $\Rightarrow \langle \xi\boldsymbol{x}+\xi'\boldsymbol{x}'|\boldsymbol{y}\rangle = \bar{\xi}\langle \boldsymbol{x}|\boldsymbol{y}\rangle + \bar{\xi}'\langle \boldsymbol{x}'|\boldsymbol{y}\rangle;$

   $\langle \boldsymbol{x}|\boldsymbol{x}\rangle \in \mathbb{R}$
3. $\langle \boldsymbol{x}|\boldsymbol{x}\rangle \geq 0$, con igualdad si y sólo si $\boldsymbol{x} = 0$.

La *norma* $|\boldsymbol{x}|$ de un vector $\boldsymbol{x} \in E$ se define como $\sqrt{\langle \boldsymbol{x}|\boldsymbol{x}\rangle}$. Así, pues,

$|\boldsymbol{x}| > 0$ si $\boldsymbol{x} \neq 0$ y $|\boldsymbol{0}| = 0$.

► Si $\xi \in \mathbb{C}$ y $\boldsymbol{x} \in E$, entonces $|\xi\boldsymbol{x}| = |\xi||\boldsymbol{x}|$.

En efecto, $|\xi\boldsymbol{x}|^2 = \langle \xi\boldsymbol{x}|\xi\boldsymbol{x}\rangle = \bar{\xi}\xi\langle \boldsymbol{x}|\boldsymbol{x}\rangle = |\xi|^2|\boldsymbol{x}|^2$. □

Cuando $|\boldsymbol{x}| = 1$, decimos que $\boldsymbol{x}$ es *unitario*.

► Si $\boldsymbol{x} \in E - \{0\}$, y ponemos $\hat{\boldsymbol{x}} = \boldsymbol{x}/|\boldsymbol{x}|$, entonces $\hat{\boldsymbol{x}}$ es unitario. □

Ejemplo. $\mathbb{C}^n$, con el producto escalar

$$\langle \boldsymbol{\xi} | \boldsymbol{\eta} \rangle = \bar{\xi}_1 \eta_1 + \cdots + \bar{\xi}_n \eta_n \, .$$

En este caso,

$$|\boldsymbol{\xi}|^2 = \bar{\xi}_1 \xi_1 + \cdots + \bar{\xi}_n \xi_n = |\xi_1|^2 + \cdots + |\xi_n|^2 .$$

$\mathbb{C}^2$ (espacio de *espinores*) tiene un papel destacado en lo que sigue.

El *adjunto* de un operador lineal $A: E \to E$ es el operador $A^\dagger: E \to E$ definido por $\langle \boldsymbol{x} | A^\dagger \boldsymbol{y} \rangle = \langle A\boldsymbol{x} | \boldsymbol{y} \rangle$. Si $A^\dagger = A$, decimos que es *autoadjunto*. Un operador lineal $U: E \to E$ es *unitario* si $\langle U\boldsymbol{x} | U\boldsymbol{y} \rangle = \langle \boldsymbol{x} | \boldsymbol{y} \rangle$ ($\Leftrightarrow U^\dagger U = Id$).

► Si $F \subseteq E$ es un subespacio vectorial y $\boldsymbol{x} \in E$, existe un único vector $\boldsymbol{x}' \in F$ tal que $\boldsymbol{x}'' = \boldsymbol{x} - \boldsymbol{x}' \in F^\perp$, es decir, $\langle \boldsymbol{x}'' | \boldsymbol{y} \rangle = 0$ para todo $\boldsymbol{y} \in F$. El vector $\boldsymbol{x}'$ (denotado $\pi_F(\boldsymbol{x})$) se llama *proyección ortogonal de* $\boldsymbol{x}$ *en* F.

► El operador $\pi_F: E \to E$ es autoadjunto.

PRESENTACIÓN AXIOMÁTICA DE LA FÍSICA CUÁNTICA

Q1 (*q*-Estados). ► Un sistema cuántico Σ queda caracterizado por un *espacio vectorial hermítico* E. Los vectores $\boldsymbol{x} \in E - \{0\}$ representan *estados* (puros) de Σ. Dos vectores $\boldsymbol{x}, \boldsymbol{y} \in E - \{0\}$ representan el mismo estado si y sólo si existe $\xi \in \mathbb{C}$ tal que $\boldsymbol{y} = \xi \boldsymbol{x}$. □

Nota. Para los sistemas requeridos en este abecé de la computación cuántica, podemos suponer (y supondremos) que E es de dimensión finita.

En términos matemáticos, el espacio de estados de Σ es el *espacio proyectivo* asociado a E, $\mathbf{P}E$, y el estado (punto) correspondiente a $\boldsymbol{x}$ se suele denotar $[\boldsymbol{x}]$. En física se suele denotar $|\boldsymbol{x}\rangle$ (*notación "ket" de Dirac*).

► Si $\boldsymbol{x} \in E - \{0\}$, $|\boldsymbol{x}\rangle = |\widehat{\boldsymbol{x}}\rangle$. Es decir, todo estado se puede representar por un vector unitario $\boldsymbol{u} = \widehat{\boldsymbol{x}}$.

► Dos vectores unitarios $\boldsymbol{u}$ y $\boldsymbol{u}'$ representan el mismo estado si y sólo si

$\boldsymbol{u}' = e^{i\varphi}\boldsymbol{u}$ para algún $\varphi \in \mathbb{R}$.

Superposición cuántica

Si $\boldsymbol{u}, \boldsymbol{u}' \in E - \{0\}$, el estado

$$|\xi\boldsymbol{u} + \xi'\boldsymbol{u}'\rangle$$

se suele denotar (¡abuso de notación!)

$$\xi|\boldsymbol{u}\rangle + \xi'|\boldsymbol{u}'\rangle$$

y se dice que es superposición de $|\boldsymbol{u}\rangle$ y $|\boldsymbol{u}'\rangle$ (con coeficientes ξ y ξ').

Por ejemplo, si $\boldsymbol{u}_j$ $(j = 0, \dots, n-1)$ es la base estándar de $\mathbb{C}^n$, y $\boldsymbol{\xi} \in \mathbb{C}^n$, podemos poner

$$\begin{aligned} |\boldsymbol{\xi}\rangle &= |\xi_0\boldsymbol{u}_0 + \cdots + \xi_{n-1}\boldsymbol{u}_{n-1}\rangle \\ &= \xi_0|\boldsymbol{u}_0\rangle + \cdots + \xi_{n-1}|\boldsymbol{u}_{n-1}\rangle \\ &= \xi_0|0\rangle + \cdots + \xi_{n-1}|n-1\rangle \end{aligned}$$

(usualmente se escribe $|j\rangle$ en lugar de $|\boldsymbol{u}_j\rangle$).

Q2 (*q*-Observables)

- Un *q-observable de* Σ es un conjunto de pares

  $A = \{a_j, E_j\}, j = 1, \dots, r$, tales que:

  Los a_j son números reales distintos (valores del observable); y

  Los E_j son subespacios vectoriales de E, 2 a 2 ortogonales, con

  $E = \bigoplus_j E_j$. □

Una *observación* o *medida de* A, cuando el estado de Σ es $|\boldsymbol{u}\rangle$, consiste en

(i) seleccionar un valor a_j con probabilidad $p_j = \left|\pi_{E_j}\boldsymbol{u}\right|^2$, y

(ii) cambiar el estado $|\boldsymbol{u}\rangle$ de Σ al estado $|\pi_{E_j}\boldsymbol{u}\rangle$).

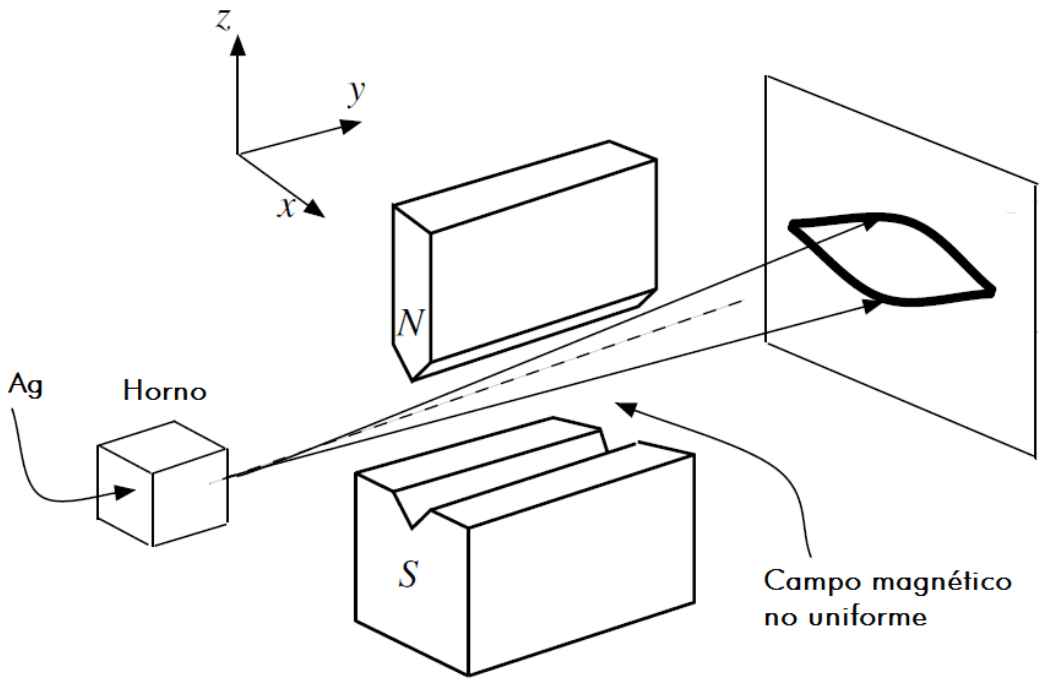
En particular, si $\boldsymbol{u} \in E_j$, entonces la observación suministra a_j con probabilidad 1 y Σ permanece en el estado $|\boldsymbol{u}\rangle$.

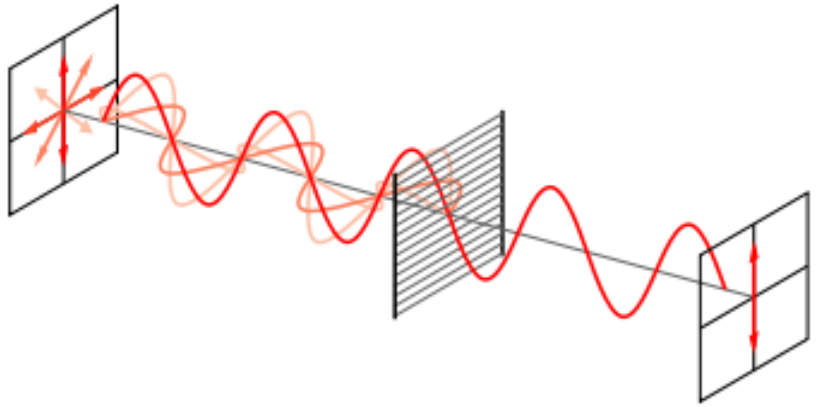
Nota. $\sum_j p_j = \sum_j \left|\pi_{E_j}\boldsymbol{u}\right|^2 = \left|\sum_j \pi_{E_j}\boldsymbol{u}\right|^2 = |\boldsymbol{u}|^2 = 1.$

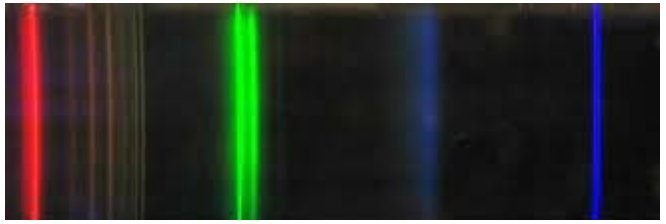
► A cada observable A se le pueden asignar el operador autoadjunto $\hat{A} = \sum_j a_j P_{E_j}$. Recíprocamente (teorema de representación espectral), todo operador autoadjunto $\hat{A} : E \to E$ da lugar a un observable formado con sus valores propios distintos a_j y los correspondientes subespacios $E_j = E_{a_j}$ de vectores propios. □

En lo que sigue no distinguiremos entre las dos representaciones.

Ejemplo (Eventualidades). Si F es a subespacio de E, la proyección ortogonal $P_F: E \to F$ es un observable con valores 1 y 0: $E_1 = F, E_0 = F^{\perp}$. Los observables de esta forma se denominan *eventualidades*. También son importantes los observables de la forma $\{\{1, F\}, \{-1, F^{\perp}\}\}$, o $P_F - P_{F^{\perp}}$.







Izquierda:*Experimento de Stern-Gerlach (1922).*

Derecha, arriba: *Polarización de la luz.* Abajo: *Espectro del* He

Q3 (Dinámica unitaria)

►Si Σ está en un ambiente no-reactivo (i.e., el ambiente no es afectado por Σ) en el intervalo temporal $[0, t]$, existe un operator unitario

$$U_t : E \to E$$

tal que $\boldsymbol{u}_t = U_t \boldsymbol{u}_0$ representa el estado de Σ en el instante t si $\boldsymbol{u}_0 \in E$ representa el estado de Σ en el instante $t = 0$. □

Si $U_t = e^{-iHt}$, siendo H un observable, decimos que la evolución es *hamiltoniana*, y que H es el *hamiltoniano* del sistema.

Nota. $U_t U_t^{\dagger} = e^{-iHt}\left(e^{-iHt}\right)^{\dagger} = e^{-iHt} e^{+iH^{\dagger}t} = Id.$

Q4 (Entrelazamiento)

►Si Σ' es un segundo sistema cuántico, y E' es el espacio que lo caracteriza, entonces $E \otimes E'$ es el espacio que caracteriza el sistema compuesto $\Sigma * \Sigma'$. □

De los estados de la forma $|\boldsymbol{u} \otimes \boldsymbol{u}'\rangle = |\boldsymbol{u}\rangle|\boldsymbol{u}'\rangle$ se dice que son *estados compuestos*. Los otros estados de $\Sigma * \Sigma'$ son *estados entrelazados* (*entangled*). Por ejemplo, si $|\boldsymbol{u}_0\rangle$ y $|\boldsymbol{u}_1\rangle$ son estados ortogonales de Σ, y $|\boldsymbol{u}'_0\rangle$ y $|\boldsymbol{u}'_1\rangle$ estados ortogonales de Σ', entonces

$$|\boldsymbol{u}_0 \otimes \boldsymbol{u}'_0 + \boldsymbol{u}_1 \otimes \boldsymbol{u}'_1\rangle = |\boldsymbol{u}_0\rangle|\boldsymbol{u}'_0\rangle + |\boldsymbol{u}_1\rangle|\boldsymbol{u}'_1\rangle$$

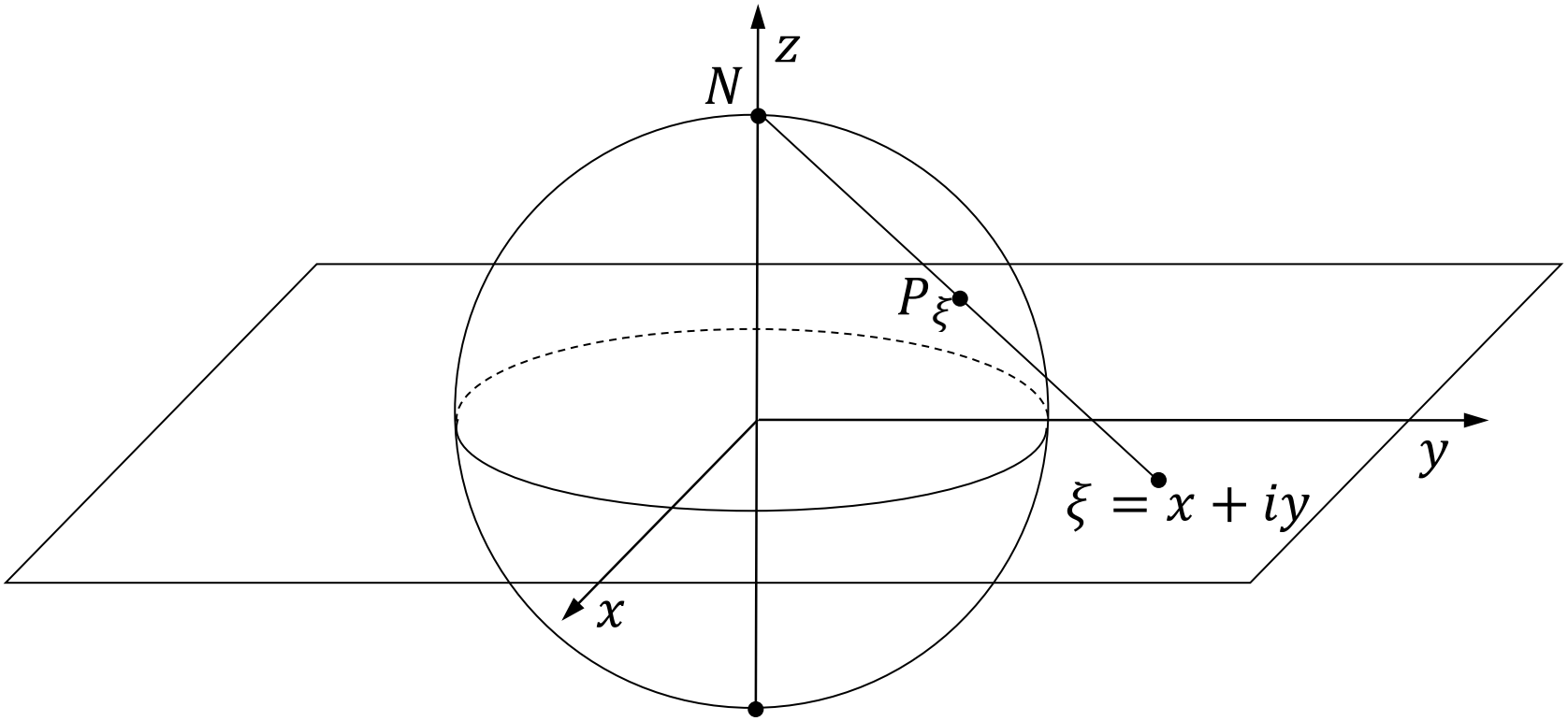
es un estado entrelazado.

q-bits (qubits)

Los estados de una partícula de espín ½ (sistema $\Sigma^{(1)}$) se pueden pensar como los puntos de una esfera S^2 de radio 1 (en unidades apropiadas).

► *El espacio asociado a este sistema* (**Q1**) *es* $\boldsymbol{H}^{(1)} = \mathbb{C}^2$ (*espinores*).

Este hecho se puede argumentar como sigue.



- Identifiquemos $\xi = x + iy \in \mathbb{C}$ con el punto $(x, y, 0) \in \mathbb{R}^3$ y consideremos el punto $P = P_\xi$ de

$$S^2 = \{(x, y, z) \in \mathbb{R}^3 | x^2 + y^2 + z^2 = 1\}$$

obtenido por proyección estereográfica desde $N = (0,0,1)$:

$$P = \left(\frac{2x}{x^2+y^2+1}, \frac{2y}{x^2+y^2+1}, \frac{x^2+y^2-1}{x^2+y^2+1}\right).$$

Poniendo $P_\infty = N$, se tiene una biyección entre $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ y S^2.

La aplicación inversa viene dada por

$$(x, y, z) \mapsto \frac{x}{1-z} + i\frac{y}{1-z}.$$

Si ponemos $x + iy = \sqrt{x^2 + y^2}e^{i\varphi} = \sqrt{1 - z^2}e^{i\varphi}$, entonces

$$\frac{x}{1-z} + i\frac{y}{1-z} = \sqrt{\frac{1+z}{1-z}}e^{i\varphi} = e^{i\varphi}\cot\frac{\theta}{2} \ (\theta = \widehat{PN}).$$

- Por otra parte también tenemos $\hat{\mathbb{C}} \simeq \mathbf{P}\mathbb{C}^2 = \mathbf{P}^1_{\mathbb{C}}$, pues cualquier $(\xi_0, \xi_1) \in \mathbb{C}^2$ es proporcional a un único vector de la forma $(1, \xi)$ cuando $\xi_0 \neq 0$ $(\xi = \xi_1/\xi_0)$, y a $(0,1)$ si $\xi_0 = 0$, con lo cual tenemos una aplicación

$$\hat{\mathbb{C}} \to \mathbf{P}^1_{\mathbb{C}}\,,\ \xi \mapsto |(1,\xi)\rangle = |0\rangle + \xi|1\rangle, \quad \infty \mapsto |(0,1)\rangle = |1\rangle.$$

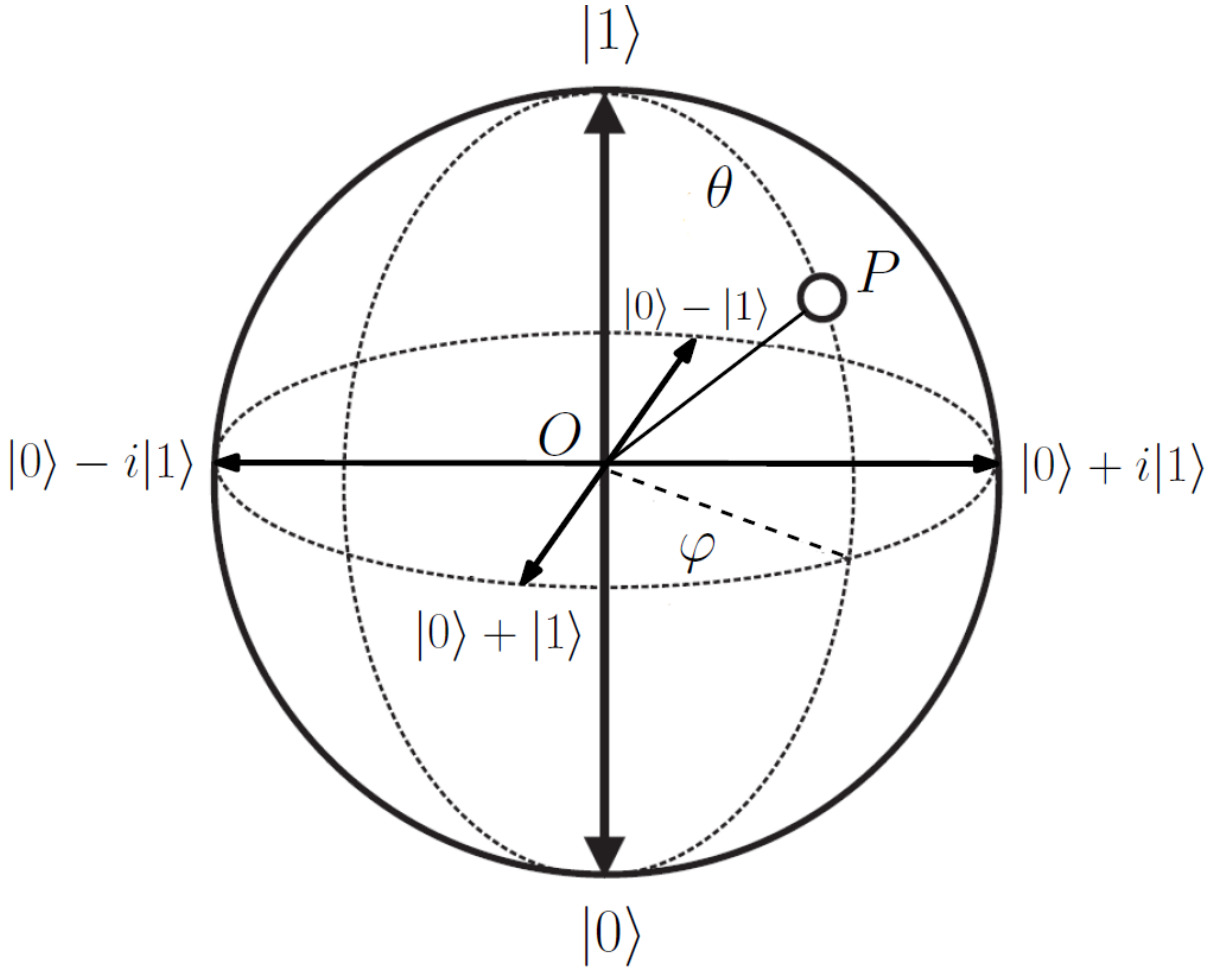
La aplicación inversa es la aplicación dada por

$$|(\xi_0, \xi_1)\rangle = \xi_0|0\rangle + \xi_1|1\rangle = \mapsto \begin{cases} \xi_1/\xi_0 \text{ si } \xi_0 \neq 0 \\ \infty \text{ si } \xi_0 = 0 \end{cases}$$

Finalmente, la identificación $S^2 \simeq \hat{\mathbb{C}} \simeq \mathbf{P}^1_{\mathbb{C}}$ queda descrita por las relaciones:

$$(x, y, z) \mapsto |0\rangle + \left(\frac{x}{1-z} + i\frac{y}{1-z}\right)|1\rangle = |0\rangle + e^{i\varphi}\cot\frac{\theta}{2}|1\rangle$$
$$= \sin\frac{\theta}{2}|0\rangle + e^{i\varphi}\cos\frac{\theta}{2}|1\rangle\ ,\ \text{si } z \neq 1;$$
$$N = (0,0,1) \mapsto |1\rangle.$$

Comentario. La esfera S^2, con la estructura de $\mathbf{P}^1_{\mathbb{C}}$, se conoce como la *esfera de Riemann.* En la literatura sobre computación cuántica se suele llamar *esfera de Bloch.*



$$\boldsymbol{p} = e^{-i\varphi/2}\sin(\tfrac{\theta}{2})|0\rangle + e^{i\varphi/2}\cos(\tfrac{\theta}{2})|1\rangle$$

► *En $\mathbb{C}^2$, dos puntos antipodades de S^2 son ortogonales.*

Hemos visto que el punto $P = (x, y, z) \in S^2$, considerado como un estado (punto de $\mathbf{P}^1_{\mathbb{C}}$), es representado por el vector

$$\boldsymbol{p} = (s, \xi c),\ s = \sin\theta/2,\ c = \cos\theta/2,\ \xi = e^{i\varphi}.$$

La misma regla nos da que el punto antípoda $P^* = (-x, -y, -z)$ es representado por el vector $\boldsymbol{p}^\perp = (c, -\xi s)$, y $\langle \boldsymbol{p} | \boldsymbol{p}^\perp \rangle = sc - sc = 0$. □

Comentario. El observable $\pi_{\boldsymbol{p}} - \pi_{\boldsymbol{p}^\perp}$ nos indica que la probabilidad de hallar que el espín es $|\boldsymbol{p}\rangle$, cuando el estado de $\Sigma^{(1)}$ es $|\boldsymbol{p}'\rangle$, es

$$\left|\pi_{\boldsymbol{p}}(\boldsymbol{p}')\right|^2 = |\langle \boldsymbol{p}' | \boldsymbol{p} \rangle|^2 = \cos^2\frac{\alpha}{2}$$

siendo $\cos\alpha = P \cdot P'$ (es decir, $\cos^2\frac{\alpha}{2} = \frac{1+\cos\alpha}{2} = \frac{1+xx'+yy'+zz'}{2}$). Estas afirmaciones se comprueban sin dificultad con simples cálculos.

q-Registros

Por el axioma **Q4** el espacio $\boldsymbol{H}^{(n)} \simeq \boldsymbol{H}^{(1)} \bigotimes \cdots \bigotimes \boldsymbol{H}^{(1)} \simeq \mathbb{C}^{2^n}$ es el espacio asociado al sistema $\Sigma^{(n)} = \Sigma^{(1)} * \cdots * \Sigma^{(1)}$ (n términos) compuesto de n sistemas $\Sigma^{(1)}$. Diremos que $\Sigma^{(n)}$ es un *q-registro* de orden n.

Por el axioma **Q3**, la evolución temporal de $\Sigma^{(n)}$ viene dada por una matriz unitaria de orden 2^n.

Juan Ignacio Cirac. Físico español (Manresa, 1965) que trabaja en Alemania. Líder mundial en el campo de la **información cuántica y sus aplicaciones**. …

http://www.arbolmat.com/juan-ignacio-cirac/

COMPUTACIÓN CUÁNTICA EN TÉRMINOS MATEMÁTICOS

- n número entero positivo (número de *bits* o *q-bits*)
- j número entero positivo en $0 \cdot\cdot (2^n - 1)$
- $j_1 j_2 \cdots j_{n-1} j_n$ expresión binaria de j

  $(j = j_1 2^{n-1} + \cdots + j_{n-1} 2 + j_n)$
- $\boldsymbol{H}^{(n)} = \mathbb{C}^{2^n}$: espacio de *q-vectores* de orden n .

  Son vectores complejos $\boldsymbol{a} = \sum_j a_j \boldsymbol{u}_j = \sum_j a_j \, |j\rangle$ (notación de Dirac) de 2^n componentes:

$$\boldsymbol{a} \equiv \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{2^n-1} \end{bmatrix};\ \boldsymbol{u}_0 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = |0\rangle, \boldsymbol{u}_1 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} = |1\rangle, \boldsymbol{u}_{2^n-1} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} = |2^n - 1\rangle$$

- Si $\boldsymbol{b} = \sum_j b_j \, |j\rangle$ es otro q-vector, y $c \in \mathbb{C}$,

  $\boldsymbol{a} + \boldsymbol{b} = \sum_j \big(a_j + b_j\big) \, |j\rangle$, $c\boldsymbol{a} = \sum_j c a_j \, |j\rangle$, $\langle \boldsymbol{a} | \boldsymbol{b} \rangle = \sum_j \bar{a}_j b_j$.

  $\langle j | k \rangle = \delta_{jk}$ ($|0\rangle$, $|1\rangle$, …, $|2^n - 1\rangle$ es una *base ortonormal*)

Ejemplo $(n = 1)$

$$\boldsymbol{a} = a_0|0\rangle + a_1|1\rangle \equiv \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = a_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + a_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Ejemplo $(n = 2)$

$$\begin{aligned} \boldsymbol{a} &= a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle \\ &= a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \\ &\equiv \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix} = a_{00} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + a_{01} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + a_{10} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + a_{11} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \end{aligned}$$

Proposición

$$|j_1 j_2\rangle = |j_1\rangle \otimes |j_2\rangle \equiv |j_1\rangle|j_2\rangle, \text{ donde } \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{bmatrix}.$$

Corolario. $\boldsymbol{H}^{(2)} \simeq \boldsymbol{H}^{(1)} \otimes \boldsymbol{H}^{(1)}$.

Demostración

$$|0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} = |00\rangle$$

$$|0\rangle \otimes |1\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} = |01\rangle$$

$$|1\rangle \otimes |0\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} = |10\rangle$$

$$|1\rangle \otimes |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix} = |11\rangle$$

En general, $\boldsymbol{H}^{(n)} \otimes \boldsymbol{H}^{(n')} = \boldsymbol{H}^{(n+n')}$, con

$$\left(\sum_j a_j |j\rangle\right) \otimes \left(\sum_{j'} a_{j'} |j'\rangle\right) = \sum_{j,j'} a_j a_{j'} \, |j 2^{n'} + j'\rangle$$

$$= \sum_{j,j'} a_j a_{j'} \, |jj'\rangle \, .$$

En particular se tiene

$$\boldsymbol{H}^{(n)} \simeq \boldsymbol{H}^{(1)} \otimes \cdots \otimes \boldsymbol{H}^{(1)}$$

$$|j_1 \cdots j_{n-1} j_n\rangle = |j_1\rangle \otimes \cdots \otimes |j_{n-1}\rangle \otimes |j_n\rangle$$

$$\equiv |j_1\rangle \cdots |j_{n-1}\rangle |j_n\rangle$$

Concatenación de las expresiones binarias de j y j'.

q-Computaciones

Si $U = [u_{jk}]$ es una matriz, su *traspuesta* es $U^T = [u_{kj}]$ y su *adjunta*

$$U^\dagger = [\bar{u}_{kj}] = \overline{U^T}.$$

Una *q-computación de orden n* es una matriz

$$U = [u_{jk}]_{0 \le j,k < 2^n}, \; u_{jk} \in \mathbb{C}, \text{ tal que } UU^\dagger = I_{2^n}$$

(esto es, U es una *matriz unitaria* de dimensión 2^n: $U \in \boldsymbol{U}(2^n) = \boldsymbol{U}^{(n)}$).

- Si $U, V \in \boldsymbol{U}^{(n)}$, $VU \in \boldsymbol{U}^{(n)}$ y $U^{-1} = U^\dagger$. En otras palabras,

  Identidad. $I_{2^n} \in \boldsymbol{U}^{(n)}$**.**

  Composición. *La composición de dos q-computaciones de orden* n *es una q-computación de orden* n; y

  Reversibilidad. *La inversa de una q-computación de orden* n *es una q-computación de orden* n.

Un *q-input* para una q-computación U es un vector $\boldsymbol{a} \in \boldsymbol{H}^{(n)}$ tal que $\langle \boldsymbol{a}|\boldsymbol{a}\rangle = 1$ (vector unitario).

Ejemplo: $\boldsymbol{h}^{(n)} = (|0\rangle + |1\rangle + \cdots + |2^n - 1\rangle)/\sqrt{2^n}$

El *q-output* de una q-computación U es el vector (unitario) $\boldsymbol{b} = U\boldsymbol{a}$.

Ejemplo. Si $U \in \boldsymbol{U}^{(n)}$ y $U' \in \boldsymbol{U}^{(n')}$ entonces $U \otimes U' : \boldsymbol{U}^{(n+n')}$, donde

$$(U \otimes U')(|j\rangle|j'\rangle) \mapsto U|j\rangle\, U'|j'\rangle\,.$$

Similarmente, si $U \in \boldsymbol{U}^{(1)}$, entonces $U^{\otimes n} \in \boldsymbol{U}^{(n)}$, donde

$$U^{\otimes n}|j\rangle = U|j_1\rangle\, U|j_2\rangle \cdots\ U|j_n\rangle.$$

Ejemplo (*q*-computación asociada a una computación clásica). Dada una *computación clásica de orden n*, $f : \boldsymbol{B}^n \to \boldsymbol{B}^n$ ($\boldsymbol{B} = \{0,1\}$), podemos definir una aplicación lineal $U_f : \boldsymbol{H}^{(n)} \to \boldsymbol{H}^{(n)}$ por $U_f|j\rangle = |f(j)\rangle$. Si f es reversible, entonces U_f es una q-computación. Diremos que U_f es la q-computación correspondiente a la computación clásica reversible f.

Ejemplos $(n = 1)$***.*** Una q-computación de orden 1 es una matriz $U \in \boldsymbol{U}^{(1)}$, i.e., una matriz de la forma

$$U = e^{i\alpha}\begin{bmatrix} u_0 & u_1 \\ -\bar{u}_1 & \bar{u}_0 \end{bmatrix},\ \alpha \in \mathbb{R},\ u_0, u_1 \in \mathbb{C}, u_0\bar{u}_0 + u_1\bar{u}_1 = 1.$$

$$U\begin{bmatrix} a_0 \\ b_0 \end{bmatrix} = e^{i\alpha}\begin{bmatrix} u_0a_0 + u_1a_1 \\ -\bar{u}_1a_0 + \bar{u}_0a_1 \end{bmatrix}$$

Nota. Es fácil comprobar que $e^{i\alpha}\begin{bmatrix} u_0 & u_1 \\ -\bar{u}_1 & \bar{u}_0 \end{bmatrix}$ es unitaria y no es difícil ver toda matriz unitaria de orden 2 tiene esta forma.

Comentario. Las únicas computaciones clásicas reversibles $1 \to 1$ son la identidad $(b \mapsto b)$ y la negación $(b \mapsto 1 + b)$.

Casos especiales: a) Matrices Pauli

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \sigma_z = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\Rrightarrow X|0\rangle = |1\rangle,\ X|1\rangle = |0\rangle \qquad \boxed{X = NOT = N}$$

Nota. Las matrices de Pauli son auto-adjuntas y $X^2 = Y^2 = Z^2 = I_2$.

b) Matriz de Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad \begin{cases} |0\rangle \mapsto (|0\rangle + |1\rangle)/\sqrt{2} \\ |1\rangle \mapsto (|0\rangle - |1\rangle)/\sqrt{2} \end{cases}$$

Pondremos HADAMARD$[n] \equiv H^{\otimes n}$: $|j_1 \cdots j_n\rangle \mapsto H|j_1\rangle \cdots H|j_n\rangle$

c) Matrices de desplazamiento de fase (phase shift)

$$S_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix} = e^{i\alpha/2} \begin{bmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{bmatrix}$$

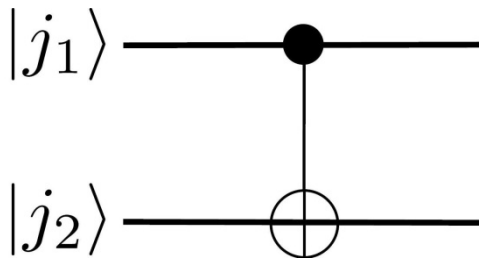
En particular, $S = S_{\pi/2} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ y $T = S_{\pi/4} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Ejemplos $(n = 2)$

Sea $U \in \boldsymbol{U}^{(1)}$. Definimos $C_{12}(U) \in \boldsymbol{U}^{(2)}$ como sigue:

$C_{12}(U)|0j_2\rangle = |0j_2\rangle$, $C_{12}(U)|1j_2\rangle = |1\rangle U|j_2\rangle$. Si $= \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$, entonces

$$C_{12}(U) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$



En particular ponemos $C_{12} = C_{12}(N)$:

$C_{12}|0j_2\rangle = |0j_2\rangle$, $C_{12}|1j_2\rangle = |1\rangle|1 + j_2\rangle$:

$$C_{01} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

No cambia el segundo bit o lo niega según que el primer bit sea 0 o 1. Es una *negación conditional* (CONTROLLED-NOT=CNOT)

$C_{21}(U)$ se define de manera análoga. Por ejemplo,

$$C_{21} = C_{21}(N) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$C_{21}(\alpha) = C_{21}(S_\alpha) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\alpha} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Ejemplo (*Teorema de no-clonación*). No existe ninguna *q*-computación *U* de orden 2 que satisfaga $U(|b\rangle|0\rangle) = |b\rangle|b\rangle$ para cualquier $|b\rangle \in \boldsymbol{H}^{(1)}$.

En efecto, consideremos $|h\rangle = \rho(|b\rangle + |b'\rangle)$, $b' = 1 + b$, $\rho = 1/\sqrt{2}$; el cálculo siguiente indica que la existencia de U lleva a una contradicción:

$$U(|h\rangle|0\rangle) = \begin{cases} |h\rangle|h\rangle = \rho^2(|b\rangle|b\rangle + |b\rangle|b'\rangle + |b'\rangle|b\rangle + |b'\rangle|b'\rangle) \\ \rho U(|b\rangle|0\rangle + |b'\rangle|0\rangle) = \rho(|b\rangle|b\rangle + |b'\rangle|b'\rangle). \end{cases}$$

q-Observaciones (o medidas)

$\boldsymbol{a} \in \boldsymbol{H}^{(n)}$ un vector unitario (*q-estado* actual).

$L = \{l_1, \dots, l_r\} \subseteq \{1, \dots, n\}$.

Si $M = m_1 m_2 \cdots m_r$ es un vector binario de orden r, sea $E_M \subseteq \boldsymbol{H}^{(n)}$ el subespacio generado por los $|j\rangle$ tales que $j_L = M$, $j_L = j_{l_1} j_{l_2} \cdots j_{l_r}$. Entonces el conjunto de pares $\{M, E_M\}$, $M \in \boldsymbol{B}^r$, es un observable A_L.

Una *q-observación* de los *q*-bits de las posiciones L es una *q*-observación de A_L, que denotaremos $M_L(\boldsymbol{a})$. Dado que $\boldsymbol{a}_L^M := \sum_{j_L = M} a_j |j\rangle = \pi_{E_M} \boldsymbol{a}$, $M_L(\boldsymbol{a})$ queda definida por dos efectos: (***i***) Selección de un $M \in \boldsymbol{B}^r$ con probabilidad $p_M = \left|\boldsymbol{a}_L^M\right|^2$ y, (***ii***) si M es el resultado obtenido, el *q*-estado $\boldsymbol{a}$ se cambia por el *q*-estado $|\boldsymbol{a}_L^M\rangle$.

Los vectores $\boldsymbol{a}_L^M$ serán denominados *colapsos de* $M_L(\boldsymbol{a})$.[N1]

Ejemplos. Consideremos el caso $n = 3$. En la observación del q-bit 3, $M_3(\boldsymbol{a})$, hay dos valores posibles, 0 y 1, sus colapsos son

$$\boldsymbol{a}_3^0 = \sum_{j_1 j_2} a_{j_1 j_2 0} |j_1 j_2 0\rangle \text{ y } \boldsymbol{a}_3^1 = \sum_{j_1 j_2} a_{j_1 j_2 1} |j_1 j_2 1\rangle \ (\boldsymbol{a} = \boldsymbol{a}_3^0 + \boldsymbol{a}_3^1)$$

y sus probabilidades $p_0 = \left|\boldsymbol{a}_3^0\right|^2$ y $p_1 = \left|\boldsymbol{a}_3^1\right|^2$.

Similarmente, para $M_{13}(\boldsymbol{a})$ se tienen cuatro resultados posibles y los correspondientes colapsos son

$$\boldsymbol{a}_{13}^{rs} = a_{r0s}|r0s\rangle + a_{r1s}|r1s\rangle \ (r, s \in \boldsymbol{B}),$$

con probabilidades

$$p_{rs} = |\boldsymbol{a}_{13}^{rs}|^2.$$

Nótese que $\boldsymbol{a} = \boldsymbol{a}_{13}^{00} + \boldsymbol{a}_{13}^{10} + \boldsymbol{a}_{13}^{01} + \boldsymbol{a}_{13}^{11} = \sum_{r,s} \boldsymbol{a}_{13}^{rs}$.

Ejemplo. En el caso de medir todos los q-bits, $M_{\{1,\ldots,n\}}(\boldsymbol{a})$, los valores posibles son los 2^n números $m \in \boldsymbol{B}^n$, los colapsos son los vectores $a_m|m\rangle$ y la probabilidad del resultado m es $p_m = |a_m|^2$.

q-Procedimientos

Un *q-procedimiento* es una secuencia de acciones, cada una de las cuales es o una *q*-computación o una *q*-observación, que se aplican sucesivamente al *q*-estado, inicialmente $|0 \ldots 0\rangle$.

Puesto que los *q*-procedimientos se diseñan para producir resultados, usualmente la última acción es una *q*-observación.

Comentarios. Siendo las *q*-observaciones procesos aleatorios, en general los *q*-procedimientos son *probabilísticos.* Esto conlleva que se ha de comprobar si el resultado suministrado satisface las condiciones requeridas y repetir el *q*-procedimiento mientras no las cumpla.

En algunos casos puede ser *exacto*, en el sentido que la probabilidad del resultado es 1.

q-Procedimientos elementales

0. ***q-Memoria***

   Para el *q-estado* $\boldsymbol{a}$. Input: $I(\boldsymbol{a})$. Por defecto, $|0 \ldots 0\rangle$.

1. ***Rotaciones de un q-bit***, $R_l(U)$, $U \in \boldsymbol{U}^{(1)}$ (*puertas* U)

   $R_2(U)|011\rangle = |0\rangle\, U|1\rangle\, |1\rangle$.

2. ***Negaciones controladas*** $N_{r,s}$ (*puertas* CNOT)

   $$|\cdots 1_r \cdots 0_s \cdots\rangle \mapsto |\cdots 1_r \cdots 1_s \cdots\rangle$$
   $$|\cdots 1_r \cdots 1_s \cdots\rangle \mapsto |\cdots 1_r \cdots 0_s \cdots\rangle$$

3. $M_L(\boldsymbol{a})$

   Suministra un $M \in B^r$ con probabilidad $p_M = |\boldsymbol{a}_L^M|^2$ y pone la *q*-memoria en el *q*-estado $\boldsymbol{u}(\boldsymbol{a}_L^M)$.

q-Algoritmos

Un *q-algoritmo es* un *q*-procedimiento formado únicamente con *q*-procedimientos elementales. La *complejidad* de un *q*-algoritmo es el número de *q*-procedimientos (elementales) que lo componen.

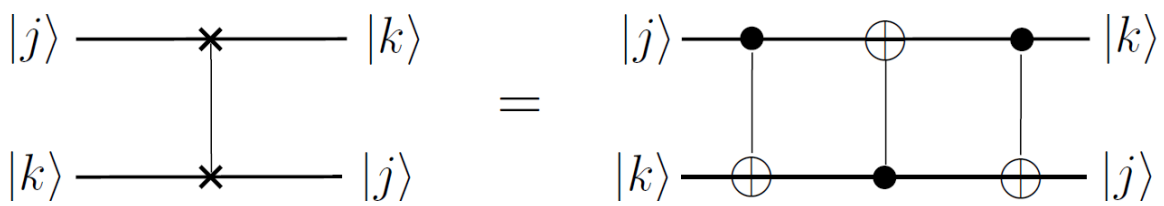
De un *q*-algoritmo se dice que es *interno* si no contiene *q*-observaciones.

Un *q*-algoritmo es *exacto* si la probabilidad de su *output* es 1, y *probabilista* en otro caso.

Ejemplo (Trasposición de 2 *q*-bits)

SWAP$[j,k]$

$C_{j,k}, C_{k,j}, C_{j,k}$.



Comentario. SWAP es interno y su complejidad es 3.

Teorema (Universalidad de las *q*-puertas U y CNOT)

Toda q-computación se puede realizar mediante un q-algoritmo interno.

Diremos que un *q-algoritmo* es *restringido* si las operaciones $R_l(U)$ que aparecen sólo usan $U \in \{H, S, T\}$, siendo

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},\ S = S_{\pi/2} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix},\ T = S_{\pi/4} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}.$$

Teorema (Universalidad aproximada de las *q*-puertas H, S, T y CNOT)

Toda q-computación se puede realizar, con tanta aproximación como deseemos, mediante un q-algoritmo interno restringido.

La idea básica de la demostración es que toda $U \in \boldsymbol{U}^{(1)}$ se puede aproximar, con cualquier precisión que deseemos, por un producto cuyos factores son matrices de $\{H, S, T\}$.

Comentario. Todo algoritmo clásico se puede traducir de manera sencilla en un *q*-algoritmo con la misma complejidad.

COMPUTADORES CUÁNTICOS

De las observaciones precedentes se sigue que para ejecutar q-programas de orden n en un soporte físico basta disponer de un registro cuántico $\Sigma^{(n)}$ e "implementaciones" de las operaciones

$M_L(\boldsymbol{a})$

$C_l(U)$ [con $U = H$, $S = S_{\pi/2}, T = S_{\pi/4}$ en el caso restringido]

$C_{j,k}$

Un *computador cuántico* (de orden n) es un registro cuántico $\Sigma^{(n)}$ dotado de capacidad para efectuar tales operaciones. Un computador de esta naturaleza permite realizar (o aproximar tanto como queramos) cualquier q-computación.

ALGUNOS EJEMPLOS DE *Q-ALGORITMOS*

QFT

La *transformada de Fourier discreta de* $\boldsymbol{H}^{(n)}$ es el operador lineal

$$F\colon \boldsymbol{H}^{(n)} \to \boldsymbol{H}^{(n)}\ ,\ F|j\rangle = \frac{1}{\sqrt{2^n}}\sum_k \xi^{jk}|k\rangle\ ,$$

siendo $\xi = \xi_n = e^{2\pi i/2^n} = e^{\pi i/2^{n-1}}$. En forma matricial,

$$F = \rho^n \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \xi & \cdots & \xi^m \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \xi^m & \cdots & \xi^{m^2} \end{bmatrix},\ \ \rho = 1/\sqrt{2},\ m = 2^n - 1.$$

Proposición. $F \in \boldsymbol{U}^{(n)}$**.**

Demostración:

$$\langle\, F|j\rangle \mid F|j'\rangle\,\rangle = \frac{1}{2^n}\sum_k \xi^{(j'-j)k} = \begin{cases} 1 & \text{Si } j' = j \\ 0 & \text{Si } j' \neq j \end{cases}\ ,$$

ya que, si $l \neq 0$, $\sum_{k=0}^{2^n-1} \xi^{lk} = \left(\left(\xi^l\right)^{2^n} - 1\right)/(\xi^l - 1)\ = 0.$

QFT[N2]

FOR $l \in \{1, \dots, n\}$

$R_l(H)$

FOR $s \in \{1, \dots, n-l\}$

$C_{l+s,l}(S_{\pi/2^s})$

FOR $l \in \{1, \dots, \lfloor n/2 \rfloor\}$

SWAP$[l, n-l+1]$.

Teorema. QFT computa F.[N3] Su complejidad es $O(n^2)$.

Nota. La clásica transformada de Fourier rápida, para vectores de dimensión 2^n, tiene complejidad $O(n2^n)$.

Ejemplos. *a*) $n = 1$. En este caso $\xi = e^{\pi i} = -1$, $F = \rho \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H$, que coincide con el valor suministrado por QFT.

b) $n = 2$. Tenemos $\xi = e^{\pi i/2} = i$ y por tanto

$$\begin{aligned} F|j_1 j_2\rangle &= \rho^2 \sum_{k_1,k_2} i^{(j_1 2 + j_2)(k_1 2 + k_2)} |k_1\rangle|k_2\rangle \\ &= \rho^2 \sum_{k_1,k_2} i^{2j_1k_2 + 2j_2k_1 + j_2k_2} |k_1\rangle|k_2\rangle \\ &= \rho^2 \sum_{k_1,k_2} (-1)^{j_1k_2} (-1)^{j_2k_1} i^{j_2k_2} |k_1\rangle|k_2\rangle \\ &= \rho^2 \Big(\sum_{k_1} (-1)^{j_2k_1} |k_1\rangle\Big)\Big(\sum_{k_2} (-1)^{j_1k_2} i^{j_2k_2} |k_2\rangle\Big) \\ &= \rho^2 \big(|0\rangle + (-1)^{j_2}|1\rangle\big)\big(|0\rangle + (-1)^{j_1} i^{j_2}|1\rangle\big). \end{aligned}$$

Por otra parte, QFT equivale a la secuencia

$$R_1(H), R_{1,2}, R_2(H), \text{SWAP}[1,2],$$

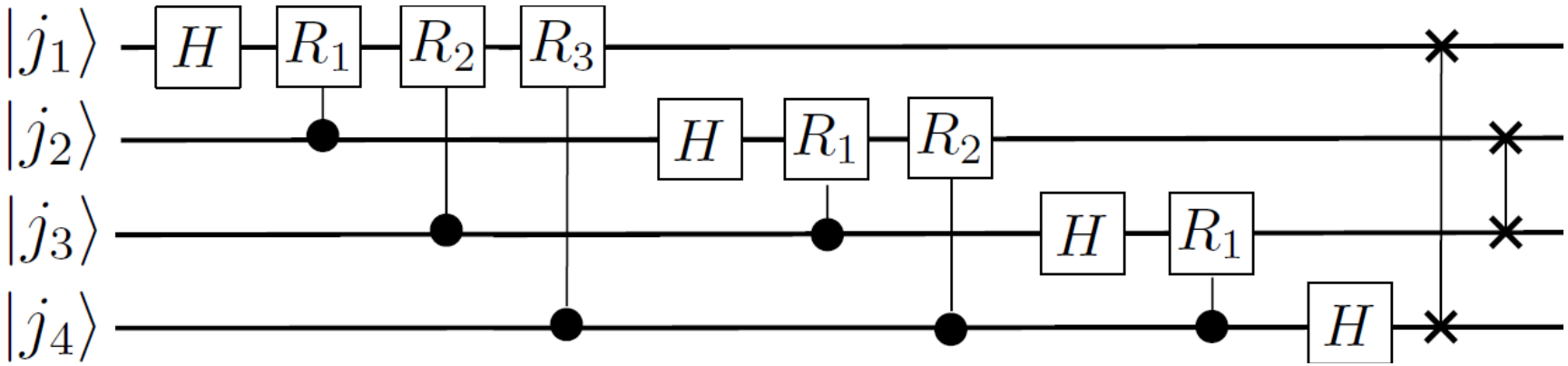
la cual transforma $|j_1 j_2\rangle = |j_1\rangle|j_2\rangle$ como sigue:

$$|j_1\rangle|j_2\rangle \mapsto \rho\big(|0\rangle + (-1)^{j_1}|1\rangle\big)|j_2\rangle \mapsto \rho\big(|0\rangle + (-1)^{j_1} i^{j_2}|1\rangle\big)|j_2\rangle$$

$$\mapsto \rho\big(|0\rangle + (-1)^{j_1} i^{j_2}|1\rangle\big)\,\rho\big(|0\rangle + (-1)^{j_2}|1\rangle\big)$$

$$\mapsto \rho^2\big(|0\rangle + (-1)^{j_2}|1\rangle\big)\big(|0\rangle + (-1)^{j_1} i^{j_2}|1\rangle\big).$$

El siguiente diagrama es una representación gráfica de la QFT de orden 4:



Generador aleatorio de números en el intervalo $0 \cdot\cdot (2^n - 1)$ con distribución uniforme

RANDOM

$$I\left(\boldsymbol{h}^{(n)}\right) = H^{\otimes n}|0 \ldots 0\rangle$$

$$M\left(\boldsymbol{h}^{(n)}\right)$$ N4

Nótese que $\left\langle j \middle| \boldsymbol{h}^{(n)} \right\rangle^2 = 1/2^n$.

Comentario. $H^{\otimes n}|0 \ldots 0\rangle = H|0\rangle \cdots H|0\rangle = \frac{1}{\sqrt{2^n}} \prod_1^n (|0\rangle + |1\rangle)$

$$= \frac{1}{\sqrt{2^n}} \sum_{j_1,\ldots,j_n} |j_1\rangle \cdots |j_n\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_j |j\rangle = \boldsymbol{h}^{(n)}.$$

q-algoritmo de Deutsch

Sea $f: \boldsymbol{B}^n \to \boldsymbol{B}$ una aplicación, y supongamos que sabemos que es o bien *constante* o bien *equilibrada* (esto significa que los conjuntos $f^{-1}(0)$ y $f^{-1}(1)$ tienen el mismo cardinal). El *Problema de Deutsch* consiste en decidir cuál de las dos posibilidades es la que realmente se da.

Comentario. En el procedimiento clásico pueden ser necesarios hasta $2^{n-1}+1$ pasos para la decisión (complejidad exponencial).

El *q*-algoritmo de Deutsch es *exacto* y su complejidad es *lineal*:

DEUTSCH$[f]$ N5	
$\|\boldsymbol{a}\rangle = N_{n+1}\|0 \dots 0\rangle\|0\rangle$ $\|\boldsymbol{a}\rangle =$HADAMARD$\|\boldsymbol{a}\rangle$ $\|\boldsymbol{a}\rangle = U_{\tilde{f}}\|\boldsymbol{a}\rangle$	$\|\boldsymbol{a}\rangle =$HADAMARD$[n]\ \|\boldsymbol{a}\rangle$ $M = M_{\{1,\dots,n\}}\|\boldsymbol{a}\rangle$ IF $M = 0$ THEN Constante ELSE Equilibrada.

$U_{\tilde{f}}: \boldsymbol{H}^{(n)} \times \boldsymbol{H}^{(1)} \to \boldsymbol{H}^{(n)} \times \boldsymbol{H}^{(1)}$ por $|j\rangle|b\rangle \mapsto |j\rangle|b + f(j)\rangle$.

q-algoritmo de Grover

Supongamos que $f: \boldsymbol{B}^n \to \boldsymbol{B}$ es una aplicación, y que $f(j) = 0$ para todo j excepto para un valor desconocido $j = t$. Con un algoritmo clásico, la complejidad de hallar t es $O(2^n)$. El q-algoritmo de Grover halla t con una complejidad $O(\sqrt{2^n})$.

Si $U_{\tilde{f}}$ es la q-computación definida en el q-algoritmo de Deutsch y ponemos $G_0|j\rangle = \begin{cases} |0\rangle \text{ Si } j = 0 \\ -|j\rangle \text{ Si } j \neq 0 \end{cases}$ y $D = H^{\otimes n} G_0 H^{\otimes n}$, entonces

GROVER$[f]$ N6

$|\boldsymbol{a}\rangle = H^{\otimes(n+1)} N_{n+1}(|0 \ldots 0\rangle|0\rangle)$

// $|\boldsymbol{a}\rangle = \rho^{n+1}\left(\sum_j |j\rangle\right)(|0\rangle - |1\rangle)$

REPEAT $\left\lfloor \frac{\pi}{4}\sqrt{2^n} \right\rfloor$

$|\boldsymbol{a}\rangle = D\ U_{\tilde{f}}\ |\boldsymbol{a}\rangle$

$M_{\{1,\ldots,n\}}|\boldsymbol{a}\rangle$

***q*-algoritmo** KITAEV (Estimación de fase)

Dado un operador unitario U y un vector propio $|\boldsymbol{u}\rangle$ de U, este q-algoritmo halla una buena aproximación $\tilde{\varphi}$ de la fase φ del correspondiente valor propio $e^{2\pi i\varphi}$.

KITAEV$[U, \boldsymbol{u}]$ [N7]

0. $\rightarrow |\mathbf{0}_m\rangle|\boldsymbol{u}\rangle$
1. HADAMARD$[m]$ $\rightarrow |\boldsymbol{h}^{(m)}\rangle|\boldsymbol{u}\rangle$
2. for $l \in 1..m$ do
   $C_{m-l+1}(U^{2^{l-1}})$
3. $\mathrm{QFT}^{\dagger}[m]$
4. $M_{\{1,\ldots,m\}}$ $\rightarrow |\tilde{\varphi}\rangle|\boldsymbol{u}\rangle$

***q*-algoritmo** SHOR-FACTOR$[N]$ (1994)

Se basa en una idea clásica (recuadro) que se puede ilustrar con un ejemplo. Sea $N = 8689648673559693$.

Buscamos un número al azar en $1..N$:

x =random(N)→ 6981311236634346

y calculamos (si $d = \text{mcd}(x, N) > 1$, $d|N$)

$r = \text{ord}_N(x)$→ 1448274778685 7258

(r es el menor número entero positivo r tal que $a^r \equiv 1 \bmod N$; si r es impar, repetir el proceso). Ahora hallamos

$X = x^{r/2} - 1 \bmod N$ → 4310665528291 2388 y

$d = \text{mcd}(X, N)$→102205879

es un divisor. De hecho es un divisor primo y $N/d = 850210267$ también lo es: la factorización de N es $102205879 * 850210267$.

Como $x^r \equiv 1 \bmod N$, $x^r - 1$ es divisible por N. Siendo

$x^r - 1 = (x^{r/2} - 1)(x^{r/2} + 1)$

o $d = \text{mcd}\left(x^{r/2} - 1, N\right) > 1$

o $d = \text{mcd}\left(x^{r/2} + 1, N\right) > 1$.

Si $d < N$, d es un divisor de N.

En caso $d = N$, se repite el proceso.

En el q-algoritmo SHOR-FACTOR$[N]$ todo funciona como en el algoritmo anterior, excepto que $\mathrm{ord}_N(x)$, que es exponencial en el número n de bits de N ($n = \lceil \log_2 N \rceil$), se calcula con el q-algoritmo SHOR-ORDER (polinómico en n). A su vez, el elemento esencial de este algoritmo es el q-algoritmo de estimación de fase. [N8]

Peter W. Shor (1959).

Nevanlinna Prize (1998)

Gödel Prize (1999)

Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer

SIAM Journal of Computing **26** (1997), 1484-1509.

Ejemplo (Estados EPR). Un estado posible de un q-registro de orden 2 es

$$|\boldsymbol{a}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Tales estados son entrelazados y se llaman *estados EPR*. (Einstein, Podolsky, Rolfsen, 1935).

Supongamos que el primer q-bit está en A y el otro en B. Si A y B miden sucesivamente su q-bit, resulta que obtienen el mismo resultado:

En efecto, el estado $|\boldsymbol{a}\rangle$ colapsa en $|00\rangle$ o en $|11\rangle$ según que A mida 0 o 1, respectivamente (i.e., la proyección ortogonal normalizada de $|\boldsymbol{a}\rangle$ en el espacio $\{|0b\rangle\}$ es $|00\rangle$, y en el espacio $\{|1b\rangle\}$ es $|11\rangle$).

A	$\boldsymbol{a}_1^A$	B
0	$\|00\rangle$	0
1	$\|11\rangle$	1

Comentario. Esta situación desconcertó a sus descubridores, Einstein, Podolski y Rolfsen (y a cualquier desde entonces) por aparecer como '*acción fantasmal a distancia*' ('*spooky action at a distance*').

Teleportación

Las técnicas de computación cuántica permiten transferir el estado de un q-bit en A al mismo estado de un q-bit en B (el *estado* desaparece en A y aparece en B). He aquí un esbozo de del procedimiento.

- Sea $|\boldsymbol{u}\rangle = \alpha|0\rangle + \beta|1\rangle$ el estado (desconocido) de un q-bit en A que deseamos teleportar a B.
- Sea $|\boldsymbol{a}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ un estado EPR compartido por A y B.
- A aplica C_{12} al estado

  $|\boldsymbol{u}\rangle|\boldsymbol{a}\rangle = \frac{1}{\sqrt{2}}[\,\alpha|0\rangle\,(|00\rangle + |11\rangle)\; + \beta|1\rangle\,(|00\rangle + |11\rangle)]$, obteniendo

  $\frac{1}{\sqrt{2}}[\,\alpha|0\rangle\,(|00\rangle + |11\rangle)\; + \beta|1\rangle\,(|10\rangle + |01\rangle)]$.
- Seguidamente A aplica H al primer bit y obtiene

  $\frac{1}{2}[\,\alpha(|0\rangle + |1\rangle)\,(|00\rangle + |11\rangle)\; + \;\beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]$,

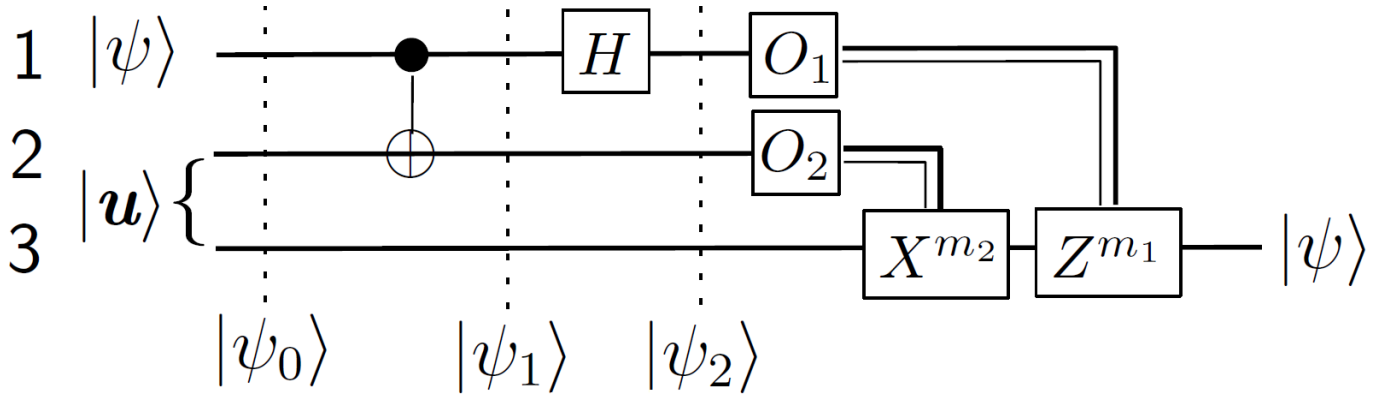
  que se puede escribir en la forma,

$$\frac{1}{2}\Big[\,|00\rangle\,(\alpha|0\rangle+\beta|1\rangle)+|01\rangle\,(\alpha|1\rangle+\beta|0\rangle)+\;\; |10\rangle\,(\alpha|0\rangle-\beta|1\rangle)\;+|11\rangle\,(\alpha|1\rangle-\beta|0\rangle)\,\Big]$$

- Ahora A mide los q-bits 1 y 2. La tabla que sigue muestra, para cada uno de los resultados posibles, el estado del q-bit en B:

Resultado	00	01	10	11
Estado B	$\alpha\|0\rangle+\beta\|1\rangle$	$\alpha\|1\rangle+\beta\|0\rangle$	$\alpha\|0\rangle-\beta\|1\rangle$	$\alpha\|1\rangle-\beta\|0\rangle$
Acción en B	I	X	Z	XZ

- Finalmente B puede reproducir el estado $|\boldsymbol{u}\rangle$ en su q-bit si conoce el resultado de la medición efectuada por A (00, 01, 10 o 11) sin más que aplicar las acciones I, X, Z o XZ, respectivamente.[N9]



COMENTARIOS FINALES

Paralelismo cuántico

Esta característica es la posibilidad de inicializar una q-computación en estados tales como $\boldsymbol{h}^{(n)} = (|0\rangle + |1\rangle + \cdots + |2^n - 1\rangle)/\sqrt{2^n}$:

- Este estado contiene (de hecho es una suma normalizada de) todos los números de n bits.
- Por tanto, cualquier operación del computador cuántico actúa sobre todos los números simultáneamente. Esto "explica" por qué un computador cuántico puede ser mucho más rápido que un computador clásico.
- En general, el éxito de los q-algoritmos (como el de factorización de Shor, por ejemplo) se basa en que, tras su ejecución, las amplitudes de los "números útiles" son grandes, al tiempo que las de los demás son pequeñas.

El problema de la decoherencia

Esta dificultad tiene su raíz en el hecho que las interacciones con el entorno pueden "perturbar" rápidamente los estados de $\Sigma^{(n)}$ ("entrelazamiento" incontrolado entre los estados del entorno y de $\Sigma^{(n)}$).

Tales dificultades en la ruta hacia la construcción de computadores cuánticos son de naturaleza física y tecnológica. La investigación de muchos laboratorios de todo el mundo está enfocada a estos problemas, con progresos continuos en muchas direcciones:

http://en.wikipedia.org/wiki/Timeline_of_quantum_computing

(se puede percibir una explosión de actividades en los últimos años, y muy especialmente desde 2006).

Véase también http://en.wikipedia.org/wiki/Quantum_computer para una descripción de más de una docena de líneas de investigación dirigidas a la realización de computadores cuánticos.

Referencias

Kaye, Phillip – Laflamme, Raymond – Mosca, Michele: *An introduction to quantum computing*. Oxford University Press, 2007.

Nielsen, M. A. – Chuang, I. L.: *Quantum computation and quantum information* Cambridge University Press, 2000.

Benatti, Fabio – Fannes, Mark – Floreanini, Roberto – Petritis, Dimitri (editors): Quantum information, computation and cryptography: An introductory survey of theory, technology and experiments. Lecture Notes in Physics 808. Springer, 2010. ix+350p.

***

Einstein, A. – Podolsky, B. – Rolfsen, N.: *Can a quantum-mechanical description of physical reality be considered complete? Phys. Rev.*, **47** (1935).

Feynman, Richard P.: Simulating physics with computers. *International Journal de Theoretical Physics*, 21(6/7):467-488, 1982.

Sudbery, Anthony: *Quantum mechanics and the particles of nature. An outline for mathematicians*. Cambridge University Press, 1986 (1st), 1988 (reprinted with corrections).

Pittenger, Arthur O.: *An Introduction to Quantum Computing Algorithms*. Progress in Computer Science and Applied Logic, Birkhäuser, 2000.

ALBER, Gernot — BETH, Thomas — HORODECKI, Michal — HORODECKI, Pawel — HORODECKI, Ryszard – RÖTTELER, Martin — WEINFURTER, Harald – WERNER, Reinhard – ZEILINGER, Anton: *Quantum information. An introduction to basic theory, concepts and experiments*. Tracts in Math Physics, 173. Springer-Verlag, 2001. xi+216p.

KITAEV, A. Yu. — SHEN, A. H. — VYALYI, M. N.: *Classical and quantum computation.* Graduate Studies in Mathematics, 47. American Mathematical Society, 2002. xiii+257.

SHOR, Peter W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484-1509, 2005.

PARTHASARATHY, K. R.: *Lecture notes on quantum computation, quantum error correcting codes and information theory.* Tata Institute de Fundamental Research, Narosa Publishing House, 2006 (distributed by the AMS).

MERMIN, N. David: *Quantum Computer Science: an introduction.* Cambridge University Press, 2007. ["known for the clarity and wit of his scientific writings"]

JAEGER, Gregg: *Quantum Information—An overview.* Springer, 2007.

BENENTI, Giuliano – CASATI, Giulio – STRINI, Giuliano: *Principles de quantum computación y information.* Volume I: *Basic concepts*. World Scientific, 2004. Volume II: *Basic tools and special topics*. World Scientific, 2007.

STOLZE, Joachim – SUTER, Dieter: *Quantum Computing: a Short Course from Theory to Experiment*. Second, updated y enlarged edition (paperback). Wiley-VCH, 2008.

JORDAN, Stephen P.: *Quantum Computation Beyond the Circuit Model.* Tesis MIT, 2008.

OLMSCHENK, S. — MATSUKEVICH, D. N. — MAUNZ, P. — HAYES, D. – DUAN, L.-M. – MONROE, C.: Quantum teleportation between distant matter Qbits. *Science*, 323 (23 Jan 2009).

KOLLMITZER, Christian – PIVK, Mario (eds.): *Applied Quantum Cryptography.* Lecture Notes on Physics 797. Springer 2010.

WEINBERG, Steven: *Lectures on quantum mechanics*. Cambridge University Press, 2013.

NOTAS

N1 (p. 35) Observemos que:

1) Los $M \in \boldsymbol{B}^r$ son los valores propios del operador (diagonal) A_L definido por $A_L|j\rangle = j_L|j\rangle$;

2) El espacio de vectores propios correspondiente a M es

$$\boldsymbol{H}_{L,M}^{(n)} = \text{espacio generado por } \{|j\rangle \mid j_L = M\};$$

3) $\boldsymbol{a}_L^M$ es la proyección ortogonal de $\boldsymbol{a}$ sobre $\boldsymbol{H}_{L,M}^{(n)}$.

Por tanto, una q-observación es un caso particular de la noción general de q-medida de un q-observable.

N2 (p. 42) La complejidad de QFT es $O(n^2)$. Si ponemos

$$R_{l,m} = C_{m,l}(S_{\pi/2^{m-l}}), m = l+1, \dots, n,$$

entonces QFT equivale a la siguiente sucesión de acciones:

$$R_1(H), R_{1,2}, \dots, R_{1,n},$$

$$R_2(H), R_{2,3}, \dots, R_{2,n},$$

$\cdots$,

$R_{n-1}(H), R_{n-1,n}$,

$R_n(H)$,

$\mathrm{SWAP}[1,n], \mathrm{SWAP}[2,n-1], \ldots, \mathrm{SWAP}[\nu,\nu']$,

donde $\nu = \lfloor n/2 \rfloor$ y $\nu' = \lceil n/2 \rceil + 1$.

Las trasposiciones finales invierten el orden de los q-bits:

$$|i_1 \cdots i_n\rangle \mapsto |i_n \cdots i_1\rangle.$$

N3 (p. 42) La demostración es un cálculo:

$$F|j\rangle = \rho^n \sum_{k=0}^{2^n-1} e^{\frac{2\pi ijk}{2^n}} |k\rangle$$

$$= \rho^n \sum_{k_1,\ldots,k_n \in B} e^{2\pi ij\left(\frac{k_1}{2^1}+\frac{k_2}{2^2}+\cdots+\frac{k_n}{2^n}\right)} |k_1 \cdots k_n\rangle$$

$$= \rho^n \sum_{k_1,\ldots,k_n \in B} \bigotimes_{l=1}^{n} e^{\frac{2\pi ijk_l}{2^l}} |k_l\rangle$$

$$= \rho^n \bigotimes_{l=1}^{n} (|0\rangle + e^{\frac{2\pi ij}{2^l}} |1\rangle) \, .$$

Pero $\frac{j}{2^l} = \frac{j_n}{2^l} + \frac{j_{n-1}}{2^{l-1}} + \cdots + \frac{j_{n-(l-1)}}{2}$ + número entero, con lo cual el l-ésimo factor del producto tensorial en la expresión es igual a

$$|0\rangle + e^{i\pi(j_n/2^{l-1})} \ldots e^{i\pi j_{n-(l-1)}}|1\rangle$$

En consecuencia

$$F|j\rangle = \rho^n\big(|0\rangle + e^{\pi i j_n}|1\rangle\big)\big(|0\rangle + e^{\pi i j_n/2} e^{\pi i j_{n-1}}|1\rangle\big)\cdots$$

$$= \big(|0\rangle + e^{\pi i j_n/2^{n-1}} \ldots e^{\pi i j_2/2} e^{\pi i j_1}\big).$$

Si escribimos este producto en orden inverso, con un ρ para cada factor, obtenemos

$$\rho\big(|0\rangle + e^{\pi i j_n/2^{n-1}} \ldots e^{\pi i j_2/2} e^{\pi i j_1}\big)\, \rho\big(|0\rangle + e^{\pi i j_n/2^{n-2}} \ldots e^{\pi i j_2}\big)\cdots$$

$$\rho\big(|0\rangle + e^{\pi i j_n/2} e^{\pi i j_{n-1}}|1\rangle\big)\, \rho\big(|0\rangle + e^{\pi i j_n}|1\rangle\big),$$

con lo cual el factor l-ésimo es igual a

$$\rho\left(|0\rangle + e^{\pi i j_n/2^{n-l}} \ldots e^{\pi i j_{l+1}/2} e^{\pi i j_l}|1\rangle\right) = R_{n-l} \cdots R_1 H|j_l\rangle$$

donde R_s significa, para el l-ésimo q-bit, $C_{l+s,l}(S_{\pi/2^s})$.

N4 (p. 45) La relación entre física cuántica y aleatoriedad es también objeto de trabajos teóricos y experimentales. Una muestra reciente:

> S. Pironio, A. **Acín**, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning , C. Monroe:
> *Random numbers certified by Bell's theorem.*
> Nature **464**, 15 April 2010.

N5 (p. 46) Veámoslo con más detenimiento. Consideremos un *q*-computador de orden $n+1$ y consideremos las acciones siguientes:

1. $|\boldsymbol{a}\rangle = N_{n+1}(|0\rangle \cdots |0\rangle|0\rangle) = |0\rangle \cdots |0\rangle|1\rangle$.

2. $|\boldsymbol{x}\rangle = H^{\otimes(n+1)}|\boldsymbol{a}\rangle = \rho^{n+1}\sum_{j=0}^{2^n-1}|j\rangle(|0\rangle - |1\rangle)$.

3. Definimos $U_{\tilde{f}}: \boldsymbol{H}^{(n)} \times \boldsymbol{H}^{(1)} \to \boldsymbol{H}^{(n)} \times \boldsymbol{H}^{(1)}$ por $|j\rangle|b\rangle \mapsto |j\rangle|b + f(j)\rangle$, esto es, el *q*-procedimiento correspondiente a $\tilde{f}(j,b) = \big(j, b + f(j)\big)$.

Sea $|\boldsymbol{y}\rangle = U_{\tilde{f}}|\boldsymbol{x}\rangle = \rho^{n+1}\sum_{j=0}^{2^n-1}|j\rangle(|f(j)\rangle - |1 + f(j)\rangle)$

$= \rho^{n+1}\big(\sum_{j=0}^{2^n-1}(-1)^{f(j)}|j\rangle\big)(|0\rangle - |1\rangle)$.

4. $|\boldsymbol{z}\rangle = \big(H^{\otimes n} \otimes I_2\big)|\boldsymbol{y}\rangle$. Después de algunos cálculos obtenemos que $|\boldsymbol{z}\rangle = \rho^{2n+1}\big(\sum_{j,k}(-1)^{j\cdot k + f(j)}|k\rangle\big)(|0\rangle - |1\rangle)$.

Sea $a_k = \rho^{2n+1} \sum_j (-1)^{j\cdot k + f(j)}$, el coeficiente de $|k\rangle(|0\rangle - |1\rangle)$. Si f es constante, $a_k = 0$ para $k \neq 0$ y $a_0 = (-1)^{f(0)}\rho$. Si f es equilibrada, entonces $a_0 = 0$. En consecuencia

$$|z\rangle = \begin{cases} a_0|0\rangle(|0\rangle - |1\rangle) & \text{Si } f \text{ es constante} \\ \sum_{k\neq 0} a_k|k\rangle(|0\rangle - |1\rangle) & \text{Si } f \text{ es equilibrada} \end{cases}$$

5. Observemos los n q-bits. Si f es constante, el resultado es 0 con probabilidad 1, y si f es equilibrada, entonces obtenemos un número $\neq 0$.

N6 (p. 47) Para la fundamentación de este algoritmo, que es bastante extensa, el lector puede consultar el artículo online

J. Rué, S. Xambó
Mathematical essentials of quantum computing

Para otras presentaciones, consúltese la Bibliografía.

N7 (p. 48) V. referencia **N6**.

N8 (p. 50) V. referencia **N6**.

N9 (p. 53) Recently this possibility has been demostrated with Yb atoms at a distance de 1m (Olmschenk et al. 2009). This opens great potential for quantum networks.