Cómputo Cuántico

formulado como Algebra Tensorial

Guillermo Morales-Luna

Departamento de Computación
Centro de Investigación y Estudios Avanzados del IPN

XLIII Congreso Nacional de la Sociedad Matemática Mexicana

1. Productos de vectores y espacios
2. Elementos básicos de Cómputo Cuántico
   - qubits y quregistros
   - Compuertas cuánticas
   - Observables
   - Principio de Heisenberg
3. Estados entrelazados
   - Desigualdad de Bell
   - Paradoja EPR
   - Codificación superdensa
4. Problemas intratables
5. Construcción de computadoras cuánticas
6. Criptografía

Productos de vectores y espacios

U, V: dos espacios vectoriales sobre $\mathbb{C}$.

$\mathcal{L}(U, V)$: espacio de transformaciones lineales de U en V.

$U^* = \mathcal{L}(U, \mathbb{C})$: Dual de U.

Si $u^* \in U^*$ escribimos, para cada $u \in U$, $\langle u^* | u \rangle := u^*(u)$.

$\langle \cdot | \cdot \rangle : U^* \times U \to \mathbb{C}$ es una transformación bilineal.

El producto tensorial de U con V es $U \otimes V = \mathcal{L}(V^*, U)$.

Propiedad

$U \times V$ se identifica con un subconjunto de $U \otimes V$.

En efecto, sea $\Phi : U \times V \to U \otimes V$ tal que $\forall (u,v) \in U \times V$, $\Phi(u,v) \in \mathcal{L}(V^*, U)$ es $\Phi(u,v) : w^* \mapsto \langle w^* | v \rangle \, u$.

Φ es bilineal.

$\Phi(u_1,v_1) = \Phi(u_2,v_2)$ ssi existe $k \in \mathbb{C}$: $(u_1,v_1) = (ku_2, k^{-1}v_2)$. Esta es una relación de equivalencia $\equiv_0$ en $U \times V$. El espacio cociente $(U \times V)/\equiv_0$ se identifica con un subespacio de $U \otimes V$.

La aplicación $\Phi(u,v) \in \mathcal{L}(V^*, U)$ se denota como $u \otimes v = \Phi(u,v)$ y se dice ser el producto tensorial del vector u con el vector v.

Propiedad

Si $\dim U = m$ *y* $\dim V = n$ *entonces* $\dim(U \otimes V) = mn$.

Si $\dim V = n$, entonces también $\dim V^* = n$, y $\dim(\mathcal{L}(V^*, U)) = nm$.
Así pues, si $U = \mathbb{C}^m$ y $V = \mathbb{C}^n$ entonces $U \otimes V = \mathbb{C}^{mn}$.

Propiedad

Si $B_U = \{u_0, u_1, \ldots, u_{m-1}\}$ *es una base de* U *y* $B_V = \{v_0, v_1, \ldots, v_{n-1}\}$ *lo es de* V *entonces* $\left(u_i \otimes v_j\right)_{i<m, j<n}$ *es una base de* $U \otimes V$, *donde, para cada* i, j, $u_i \otimes v_j$ *es* $w^* = \sum_{k=0}^{n-1} w_k v_k^* \mapsto w_j u_i$. *Es la base producto.*

Si U_1, U_2, V_1, V_2 e.e. v.v. y $K : U_1 \to U_2$ y $L : V_1 \to V_2$ son lineales, las duales $K^* : U_2^* \to U_1^*$ y $L^* : V_2^* \to V_1^*$ están definidas mediante

$$\begin{aligned} \langle K^*(u_2^*)|u_1\rangle &= \langle u_2|K(u_1)\rangle \\ \langle L^*(v_2^*)|v_1\rangle &= \langle v_2|L(v_1)\rangle \end{aligned}$$

Definamos $K \otimes L : U_1 \otimes V_1 \to U_2 \otimes V_2$,

$$(K \otimes L)(u_1 \otimes v_1) = K(u_1) \otimes L(v_1).$$

qubits y quregistros

$\mathbb{C}^{m\times n}$ el espacio de matrices de orden $m \times n$ con entradas en $\mathbb{C}$.

Para $M = \left(m_{ij}\right)_{i,j} \in \mathbb{C}^{m\times n}$ su transpuesta hermitiana es $M^H = \left(m_{ji}^H\right)_{ji} \in \mathbb{C}^{n\times m}$.

$M = \left(m_{ij}\right)_{i,j} \in \mathbb{C}^{m\times n}$ es unitaria si $M^H M = \mathbf{1}_{nn}$: identidad de orden $n \times n$.

Conjunto de estados de un sistema físico cerrado: subconjunto consistente de los vectores columnas unitarias en $\mathbb{C}^{m\times 1}$

$$E_m = \{\mathbf{v} \in \mathbb{C}^m | 1 = \mathbf{v}^H\mathbf{v} =: \langle \mathbf{v}|\mathbf{v}\rangle\}.$$

m: grado de libertad del sistema.

Todo vector de la base canónica $\left(\mathbf{e}_j = \left(\delta_{ij}\right)_{i<m}\right)_{j<m}$ es un estado.

Postulado de Medición: Si el estado actual es $\mathbf{v} = (v_{i1})_{i<m}$ entonces, para cada $i < m$, con probabilidad $|v_{i1}|^2$ se realiza lo siguiente: *Se emite la respuesta* i *y se transita al estado* $\mathbf{e}_i$; es decir este último será el estado actual en el paso siguiente.

Se realiza al final de todo algoritmo cuántico. Se arriba así a un estado final.

Para $m = 2$, la base canónica consta de $\mathbf{e}_0 = [1 \;\; 0]^T$ y $\mathbf{e}_1 = [0 \;\; 1]^T$.
Para $z_0, z_1 \in \mathbb{C}$ con $|z_0|^2 + |z_1|^2 = 1$, $z_0\mathbf{e}_0 + z_1\mathbf{e}_1$ es un qubit.
$\mathbf{e}_0$ "es" el valor de verdad falso, o cero, y $\mathbf{e}_1$ verdadero, o uno.
Para cada $n > 1$: $\mathbb{H}_n = \mathbb{H}_{n-1} \otimes \mathbb{H}_1$.
$\dim(\mathbb{H}_n) = 2^n$ y una base es $B_{\mathbb{H}_n} = (\mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0})_{\varepsilon_{n-1},\ldots,\varepsilon_1,\varepsilon_0 \in \{0,1\}}$:

$$|\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0\rangle := \mathbf{e}_{\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0} = \mathbf{e}_{\varepsilon_{n-1}} \otimes \cdots \otimes \mathbf{e}_{\varepsilon_1} \otimes \mathbf{e}_{\varepsilon_0} =: |\varepsilon_{n-1}\rangle \cdots |\varepsilon_1\rangle\,|\varepsilon_0\rangle \tag{1}$$

Cada $i \in [\![0, 2^n - 1]\!]$ en binario es $i = (\varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0)_2$.

$$[\![0, 2^n - 1]\!] \approx \{0,1\}^n \;\;,\;\; i \leftrightarrow \varepsilon = \varepsilon_{n-1}\cdots\varepsilon_1\varepsilon_0.$$

Si $\mathbf{z} \in E_{2^n}$ (esfera unitaria euclidiana en $\mathbb{H}_n$) entonces $\sum_{\varepsilon\in\{0,1\}^n} z_\varepsilon \mathbf{e}_\varepsilon$ es un estado correspondiente a una palabra de información de longitud n, y es también la concatenación de n qubits.

Compuertas cuánticas

Si $U \in \mathbb{C}^{m\times m}$ es unitaria, entonces determina una transformación ortogonal $\mathbb{C}^m \to \mathbb{C}^m$: $\mathbf{v} \mapsto U\mathbf{v}$.

Su restricción a la esfera unitaria transforma estados en estados: $U|_{E_m} : E_m \to E_m$.

U es una compuerta cuántica.

Algoritmo cuántico

Un algoritmo cuántico es la composición de un número finito de compuertas cuánticas seguida de una medición.

$n = 1$: Compuertas básicas

Identidad. $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. $I : \mathbb{H}_1 \to \mathbb{H}_1$ es el operador identidad.

Rotación. Sea $t \in [-\pi, \pi]$ un ángulo y sea

$$Rot_t = \begin{bmatrix} \cos(t) & -\text{sen}(t) \\ \text{sen}(t) & \cos(t) \end{bmatrix}.$$

Rot_t es unitaria y tiene como efecto rotar un ángulo t en sentido antihorario.

Negación. $N = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Se tiene $N : \begin{bmatrix} z_0 \\ z_1 \end{bmatrix} \mapsto \begin{bmatrix} z_1 \\ z_0 \end{bmatrix}$. N es unitaria y tiene como función permutar señales, es de hecho "una reflexión a lo largo de la diagonal principal".

Hadamard. $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Se tiene

$$H : \begin{bmatrix} z_0 \\ z_1 \end{bmatrix} \mapsto \frac{1}{\sqrt{2}} \begin{bmatrix} z_0 + z_1 \\ z_0 - z_1 \end{bmatrix}.$$ H es unitaria.

$n = 2$: Compuertas básicas

Negación controlada. Sea $C : \mathbb{H}_2 \to \mathbb{H}_2$ la transformación lineal que sobre los vectores básicos actúa $\mathbf{e}_x \otimes \mathbf{e}_y \mapsto \mathbf{e}_x \otimes \mathbf{e}_{x \oplus y}$. Esta transformación se llama negación controlada debido a que en su salida, el segundo qubit es la negación del primero sólo si en la entrada el segundo qubit "estaba prendido". Esto puede verse como que el segundo qubit de entrada sirve de "control" para aplicar el operador de negación al primero, el cual hace las veces de "argumento".

Reversos. $R_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, es tal que $R_2(\mathbf{e}_i \otimes \mathbf{e}_j) = \mathbf{e}_j \otimes \mathbf{e}_i$.

Transformaciones de Pauli

Las matrices de Pauli son

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad , \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2}$$

las cuales son hermitianas y unitarias, es decir, para $j = 0, 1, 2, 3$, $\sigma_j \sigma_j = \mathbf{1}_2$ es la matriz identidad de orden 2×2.
Las cuatro matrices de Pauli conforman una base de $\mathbb{C}^{2\times 2}$:

$$\forall A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \in \mathbb{C}^{2\times 2} \; \exists c_0, c_1, c_2, c_3 : \\ A = c_0\sigma_0 + c_1\sigma_1 + c_2\sigma_2 + c_3\sigma_3 \tag{3}$$

$$(c_0, c_1, c_2, c_3) = \tfrac{1}{2}\left((a_{00} + a_{11}), (a_{01} + a_{10}), i(a_{01} - a_{10}), (a_{00} - a_{11})\right).$$

Se tiene también que valen las siguientes relaciones, para $1 \leq j,k \leq 3$

$$\sigma_j\sigma_k + \sigma_k\sigma_j = 2\delta_{jk}\mathbf{1}_2 \quad (4)$$

$$\sigma_j\sigma_k = \delta_{jk}\mathbf{1}_2 + i\sum_{\ell=1}^{3}\varepsilon_{jk\ell}\sigma_\ell \quad (5)$$

donde en la última expresión,

$$\varepsilon_{jk\ell} \in \{-1,0,1\}\ ,\ |\varepsilon_{jk\ell}| = 1 \ \Leftrightarrow\ \{j,k,\ell\} = \{1,2,3\}$$

y además

$$\varepsilon_{jk\ell} = 1 \ \Leftrightarrow\ (j,k,\ell) \text{ es rotación horaria.}$$

Si $\mathbf{z} = z_0\mathbf{e}_0 + z_1\mathbf{e}_1$, con $|z_0|^2 + |z_1|^2 = 1$, entonces

- $\sigma_1\mathbf{z} = z_1\mathbf{e}_0 + z_0\mathbf{e}_1$ y $\sigma_2\mathbf{z} = -iz_1\mathbf{e}_0 + iz_0\mathbf{e}_1$ corresponden a errores de permutación de bits (bit-flip errors) en $\mathbf{z}$,
- $\sigma_3\mathbf{z} = z_0\mathbf{e}_0 - z_1\mathbf{e}_1$ es un error de fase de bit (phase-flip error) en $\mathbf{z}$.

Grupo de Pauli

El grupo que generan, junto con sus inversos aditivos, en el grupo de matrices unitarias consta de 16 elementos:

$$\sigma_0 = \pi_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \; ; \quad -\sigma_0 = \pi_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$i\,\sigma_0 = \pi_3 = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \; ; \quad -i\,\sigma_0 = \pi_4 = \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix}$$

$$\sigma_1 = \pi_5 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \; ; \quad -\sigma_1 = \pi_6 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

$$i\,\sigma_1 = \pi_7 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \; ; \quad -i\,\sigma_1 = \pi_8 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

$$\sigma_2 = \pi_9 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \; ; \quad -\sigma_2 = \pi_{10} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

$$i\,\sigma_2 = \pi_{11} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \; ; \quad -i\,\sigma_2 = \pi_{12} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_3 = \pi_{13} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \; ; \quad -\sigma_3 = \pi_{14} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$i\,\sigma_3 = \pi_{15} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \; ; \quad -i\,\sigma_3 = \pi_{16} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

Tabla de multiplicación del grupo de Pauli

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15
3	4	2	1	7	8	6	5	11	12	10	9	15	16	14	13
4	3	1	2	8	7	5	6	12	11	9	10	16	15	13	14
5	6	7	8	1	2	3	4	15	16	14	13	12	11	9	10
6	5	8	7	2	1	4	3	16	15	13	14	11	12	10	9
7	8	6	5	3	4	2	1	14	13	16	15	9	10	11	12
8	7	5	6	4	3	1	2	13	14	15	16	10	9	12	11
9	10	11	12	16	15	13	14	1	2	3	4	7	8	6	5
10	9	12	11	15	16	14	13	2	1	4	3	8	7	5	6
11	12	10	9	13	14	15	16	3	4	2	1	6	5	8	7
12	11	9	10	14	13	16	15	4	3	1	2	5	6	7	8
13	14	15	16	11	12	10	9	8	7	5	6	1	2	3	4
14	13	16	15	12	11	9	10	7	8	6	5	2	1	4	3
15	16	14	13	10	9	12	11	5	6	7	8	3	4	2	1
16	15	13	14	9	10	11	12	6	5	8	7	4	3	1	2

Mediciones de espines

Para cada $\mathbf{v} \in \mathbb{R}^3$, hagamos

$$V_{\mathbf{v}} = v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3 = \begin{pmatrix} v_3 & v_1 - i\,v_2 \\ v_1 + i\,v_2 & -v_3 \end{pmatrix}. \tag{6}$$

Toda vez que $\mathbf{v}$ sea un vector unitario, $V_{\mathbf{v}}$ se dice ser la medición de espín a lo largo de $\mathbf{v}$. Los valores propios de $V_{\mathbf{v}}$ son $-\|\mathbf{v}\|_2, \|\mathbf{v}\|_2$, es decir, son $-1, 1$ con correspondientes vectores propios

$$\mathbf{u}_{\mathbf{v}0} = \begin{bmatrix} v_3 - 1 \\ v_1 + i\,v_2 \end{bmatrix} \quad , \quad \mathbf{u}_{\mathbf{v}1} = \begin{bmatrix} v_3 + 1 \\ v_1 + i\,v_2 \end{bmatrix}.$$

Para cada $\mathbf{x} = [x_0 \;\; x_1]^T \in \mathbb{H}_1$ se tiene

$$\langle \mathbf{x} | V_{\mathbf{v}} \mathbf{x} \rangle = (2x_0x_1)\,v_1 + \left(x_0^2 - x_1^2\right) v_3$$

por lo que la esperanza de $V_{\mathbf{v}}$ en un estado $\mathbf{x}$ es una rotación que depende de $\mathbf{x}$.

- Un estado $\sigma(\mathbf{z}) = \sum_{\varepsilon \in \{0,1\}^n} z_\varepsilon \mathbf{e}_\varepsilon \in \mathbb{H}_n$ está determinado por 2^n coordenadas.
- Si $U : \mathbb{H}_n \to \mathbb{H}_n$ es una compuerta cuántica, el estado $\sigma(U\mathbf{z})$ consta también de 2^n coordenadas.

Paralelismo intrínseco

Un cálculo que involucra un número exponencial de términos se hace en "un paso" de cómputo cuántico y así se acelera el proceso de corrida.

- Un estado es descomponible, o factorizable, si es de la forma $\mathbf{z}_1 \otimes \cdots \otimes \mathbf{z}_n = \sigma(\mathbf{z})$, con $\mathbf{z}_i \in \mathbb{H}_1$.

- Un estado que no es descomponible se dice ser entrelazado (entangled state).

Observables

$\mathbb{H}$: espacio de Hilbert de dimensión finita sobre $\mathbb{C}$

$E_{\mathbb{H}}$ su esfera unitaria.

Una transformación lineal $H : \mathbb{H} \to \mathbb{H}$ es autoadjunta si $\forall \mathbf{x}, \mathbf{y} \in \mathbb{H} \ \ \langle \mathbf{x} | H\mathbf{y} \rangle = \langle H\mathbf{x} | \mathbf{y} \rangle$, o equivalentemente, su matriz es hermitiana: $H^H = \overline{H}^T = H$.

Una transformación autoadjunta es un observable.

Si $U, V : \mathbb{H}_n \to \mathbb{H}_n$ es un observable, su suma $U + V$ siempre lo es, pero el producto UV lo será si, por ejemplo, U y V conmutan. Sin embargo $UV + VU$ e $i(UV - VU)$ siempre lo serán.

Para un observable $U : \mathbb{H}_n \to \mathbb{H}_n$ existe una base ON de $\mathbb{H}_n$ formada por vectores propios de U. Así, si $\lambda_0, \ldots, \lambda_{k-1}$ son los valores propios de U y $L_0, \ldots, L_k$ son los correspondientes espacios propios:

$$\mathbf{x} \in L_\kappa \implies U(\mathbf{x}) = \lambda_\kappa \mathbf{x}.$$

Por lo cual, U se representa como

$$U = \sum_{\kappa=0}^{k-1} \lambda_\kappa \pi_{L_\kappa},$$

donde para cada espacio $L < \mathbb{H}_n$, $\pi_L : \mathbb{H}_n \to L$ es la proyección ortogonal sobre L.

Si $\{\mathbf{v}_0, \ldots, \mathbf{v}_{m-1}\}$ es una base ON de L y $\mathbf{L}$ es la matriz que tiene a esos vectores como "vectores columnas" entonces $\pi_L = \mathbf{L} \cdot \mathbf{L}^H$. Ya que π_{L_κ} es una proyección ortogonal, para cada $\mathbf{x} \in \mathbb{H}_n$, $\langle \mathbf{x} - \pi_{L_\kappa}(\mathbf{x}) | \pi_{L_\kappa}(\mathbf{x}) \rangle = 0$, y

$$\langle \mathbf{x} | \pi_{L_\kappa}(\mathbf{x}) \rangle = \langle \pi_{L_\kappa}(\mathbf{x}) | \pi_{L_\kappa}(\mathbf{x}) \rangle = \| \pi_{L_\kappa}(\mathbf{x}) \|^2.$$

Principio de medición extendido

Para un observable U, al tomar una medición en un n-registro $\mathbf{x} \in \mathbb{H}_n$, se da como resultado uno de los valores propios λ_κ y se asume como estado actual la proyección normalizada $\frac{\pi_{L_\kappa}(\mathbf{x})}{\| \pi_{L_\kappa}(\mathbf{x}) \|}$. Además para cada valor propio λ_κ, la probabilidad que ése sea el resultado es

$$\Pr(\lambda_\kappa) = \langle \mathbf{x} | \pi_{L_\kappa}(\mathbf{x}) \rangle . \tag{7}$$

Observamos $\sum_{\kappa=0}^{k-1} \Pr(\lambda_\kappa) = \sum_{\kappa=0}^{k-1} \| \pi_{L_\kappa}(\mathbf{x}) \|^2 = \| \mathbf{x} \|^2 = 1.$

Para un observable H, sea $(\mathbf{f}_i)_i$ una base ortonormal de $\mathbb{H}$ consistente de eigenvectores de H. Entonces para cada $\mathbf{z} \in E_{\mathbb{H}}$, se puede expresar $\mathbf{z} = \sum_i a_i \mathbf{f}_i$, donde $\sum_i |a_i|^2 = 1$. Se tiene

$$\begin{aligned} \langle \mathbf{z} | H\mathbf{z} \rangle &= \left\langle \sum_i a_i \mathbf{f}_i | H \left(\sum_j a_j \mathbf{f}_j \right) \right\rangle \\ &= \left\langle \sum_i a_i \mathbf{f}_i | \sum_j a_j \lambda_j \mathbf{f}_j \right\rangle \\ &= \sum_i \lambda_i |a_i|^2 = E(\lambda_i) \end{aligned}$$

Así, $\langle \mathbf{z} | H\mathbf{z} \rangle$ es el valor observado promedio de la palabra $\mathbf{z}$ bajo H.

$$\triangle H : \mathbb{H} \to \mathbb{R}\ ,\ \mathbf{x} \mapsto \triangle H(\mathbf{x}) = \sqrt{\langle H^2\mathbf{x} | \mathbf{x} \rangle - \langle H\mathbf{x} | \mathbf{x} \rangle^2}.$$

$\triangle H(\mathbf{x})$ es la desviación estándar del observable H en el punto $\mathbf{x}$.

Principio de Heisenberg

Sean $H_1, H_2 : \mathbb{H} \to \mathbb{H}$ dos observables. Entonces $\forall \mathbf{x} \in \mathbb{H}$:

$$\langle H_2 \circ H_1 \mathbf{x} | \mathbf{x} \rangle \langle \mathbf{x} | H_2 \circ H_1 \mathbf{x} \rangle = \langle H_1 \circ H_2 \mathbf{x} | \mathbf{x} \rangle \langle \mathbf{x} | H_1 \circ H_2 \mathbf{x} \rangle = |\langle H_1 \mathbf{x} | H_2 \mathbf{x} \rangle|^2,$$

y de la desigualdad de Schwartz se tiene
$|\langle H_1 \mathbf{x} | H_2 \mathbf{x} \rangle|^2 \leq \|H_1 \mathbf{x}\|^2 \|H_2 \mathbf{x}\|^2$.

Desigualdad de Robertson-Schrödinger.

$$\frac{1}{4} |\langle (H_1 \circ H_2 - H_2 \circ H_1) \mathbf{x} | \mathbf{x} \rangle|^2 \leq \|H_1 \mathbf{x}\|^2 \|H_2 \mathbf{x}\|^2. \qquad (8)$$

Dos observables H_1, H_2 son compatibles si conmutan:
$H_1 \circ H_2 = H_2 \circ H_1$.
Su conmutador es $[H_1, H_2] = H_1 \circ H_2 - H_2 \circ H_1$.

Principio de Incertidumbre de Heisenberg

Para cualesquiera dos observables H_1, H_2 y para cualquier vector unitario $\mathbf{z} \in E_{\mathbb{H}}$,

$$\|\triangle H_1(\mathbf{z})\|^2 \|\triangle H_2(\mathbf{z})\|^2 \geq \frac{1}{4} \left|\langle \mathbf{z}| \left[H_1, H_2\right] \mathbf{z}\rangle\right|^2 . \tag{9}$$

Si los observables son incompatibles, entonces cada vez que H_1 sea medido con una mayor precisión, H_2 ha de ser medido con una menor precisión, y viceversa.

Desigualdad de Bell

Supongamos: Carola prepara dos partículas, una para Alicia, otra para Beto.

Alicia puede medir sobre su partícula una de dos propiedades, W y X, con valores ± 1: P_W, P_X. Selecciona aleatoriamente W o X.

Igualmente, Beto puede medir sobre su partícula una de dos propiedades, Y y Z, con valores ± 1: P_Y o P_Z. Selecciona aleatoriamente Y o Z.

Consideremos el valor

$$F = WY + XY + XZ - WZ. \tag{10}$$

Entonces $F = \pm 2$, y la mitad de las combinaciones da valores negativos:

W	X	Y	Z
-1	-1	1	-1
-1	-1	1	1
-1	1	-1	-1
-1	1	1	-1
1	-1	-1	1
1	-1	1	1
1	1	-1	-1
1	1	-1	1

$F = -2$

W	X	Y	Z
-1	-1	-1	-1
-1	-1	-1	1
-1	1	-1	1
-1	1	1	1
1	-1	-1	-1
1	-1	1	-1
1	1	1	-1
1	1	1	1

$F = 2$

Es evidente que la esperanza es $E(F) \leq 2$, y de su linealidad resulta la

Desigualdad de Bell

$$E(WY) + E(XY) + E(XZ) - E(WZ) \leq 2 \tag{11}$$

Desde un punto de vista clásico, se puede presuponer

realidad: los valores P_W, P_X, P_Y, P_Z son inherentes a las partículas, Alicia y Beto tan solo las descubren,

localidad: las mediciones de Alicia y Beto son independientes entre sí.

Paradoja EPR

En el experimento anterior, Carola prepara las partículas en el estado entrelazado $\mathbf{b}_3 = \frac{1}{\sqrt{2}}(\mathbf{e}_{01} - \mathbf{e}_{10})$. Supongamos observables:

$$\begin{aligned} W &= \sigma_3 & Y &= \tfrac{1}{\sqrt{2}}(\sigma_1 + \sigma_3) \\ X &= \sigma_1 & Z &= \tfrac{1}{\sqrt{2}}(\sigma_1 - \sigma_3) \end{aligned} \tag{12}$$

Entonces,

$$\frac{1}{\sqrt{2}} = E(WY) = E(XY) = E(XZ) = -E(WZ) \tag{13}$$

y $E(F) = \frac{4}{\sqrt{2}} = 2\sqrt{2}$, lo cual contradice (11).

Para evitar la paradoja, ¡¡es necesario rechazar los principios de realidad y de localidad!!

Codificación superdensa

En $\mathbb{H}_2 = \mathbb{H}_1 \otimes \mathbb{H}_1$, sea $\{\mathbf{e}_{00}, \mathbf{e}_{01}, \mathbf{e}_{10}, \mathbf{e}_{11}\}$ la base canónica y sea

$$\begin{aligned} \mathbf{b}_0 &= \frac{1}{\sqrt{2}}(\mathbf{e}_{00} + \mathbf{e}_{11}) & \mathbf{b}_1 &= \frac{1}{\sqrt{2}}(\mathbf{e}_{00} - \mathbf{e}_{11}) \\ \mathbf{b}_2 &= \frac{1}{\sqrt{2}}(\mathbf{e}_{01} + \mathbf{e}_{10}) & \mathbf{b}_3 &= \frac{1}{\sqrt{2}}(\mathbf{e}_{01} - \mathbf{e}_{10}) \end{aligned} \tag{14}$$

El conjunto $B = \{\mathbf{b}_0, \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$ es una base ortonormal de $\mathbb{H}_2$, llamada base de Bell.

Supongamos: Alicia quisiera transmitirle a Beto un par de bits clásicos, $\varepsilon = \varepsilon_1\varepsilon_0$, transmitiendo sólo un qubit.
Fijan inicialmente el estado entrelazado $\mathbf{x} = \mathbf{b}_0$.

1. Alicia calcula $\mathbf{y} = \mathbf{b}_\varepsilon$ como sigue:

$$\begin{aligned}
\varepsilon = 00 &\implies \mathbf{y} = (\mathbf{1}_1 \otimes \mathbf{1}_1)(\mathbf{x}) = \mathbf{b}_0 \\
\varepsilon = 01 &\implies \mathbf{y} = (\sigma_3 \otimes \mathbf{1}_1)(\mathbf{x}) = \mathbf{b}_1 \\
\varepsilon = 10 &\implies \mathbf{y} = (\sigma_1 \otimes \mathbf{1}_1)(\mathbf{x}) = \mathbf{b}_2 \\
\varepsilon = 11 &\implies \mathbf{y} = ((i\,\sigma_2 \otimes \mathbf{1}_1)(\mathbf{x}) = \mathbf{b}_3
\end{aligned}$$

2. Alicia le envía **y** a Beto.
3. Beto mide **y** respecto a la base de Bell,
4. y recupera $\varepsilon = \varepsilon_1\varepsilon_0$.

Teorema de Holevo

La cantidad de información recuperable de un registro de qubits está acotada superiormente por la entropía de von Neumann, la cual a su vez no excede a la entropía de Shannon, de hecho la iguala cuando los qubits son ortogonales a pares.

Este teorema excluye la posibilidad de que se pueda comunicar más de n bits (clásicos) de información al transmitir n qubits. Mas, mediante el uso de estados entrelazados es posible reducir la complejidad de la información cuántica.

Problemas intratables

Éstos son intratables con el enfoque clásico:

Factorización (Fact)

Dado un número entero, factorizarlo como un producto de números primos.

Logaritmos discretos (DLP)

Dado un grupo finito, un generador en él y un elemento cualquiera, encontrar el número de veces que hay que operar el generador consigo mismo para obtener el elemento cualquiera.

Búsquedas eficientes

Localizar un registro en una base de datos realizando un número de consultas sublineal respecto al tamaño de la base, digamos del orden de su raíz cuadrada.

Construcción de computadoras cuánticas

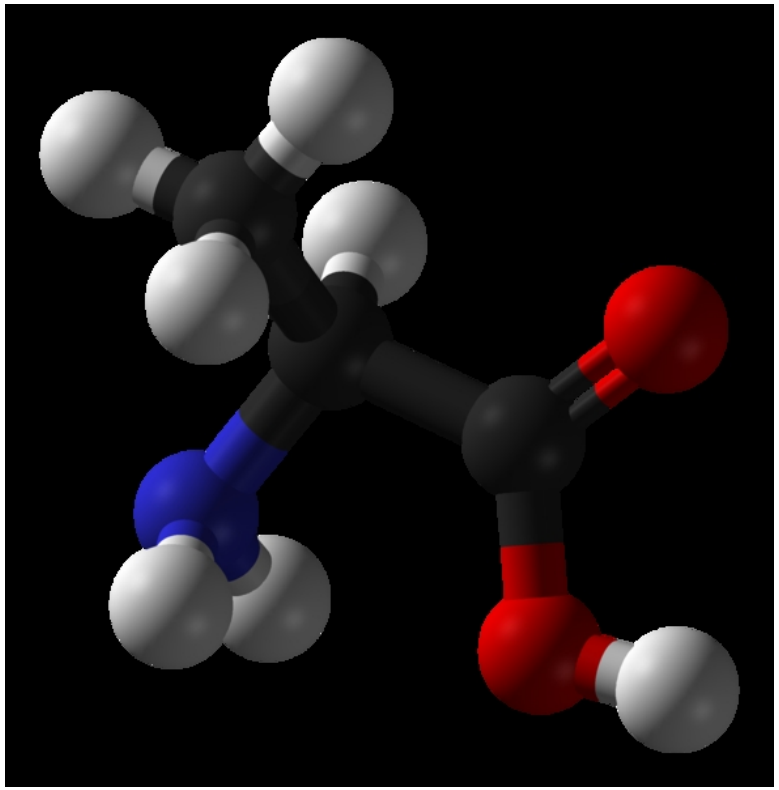
En cuanto a la implementación se tiene que cualquier sistema físico que realice la Computación Cuántica ha de cumplir con los criterios siguientes llamados de DiVicenzo:

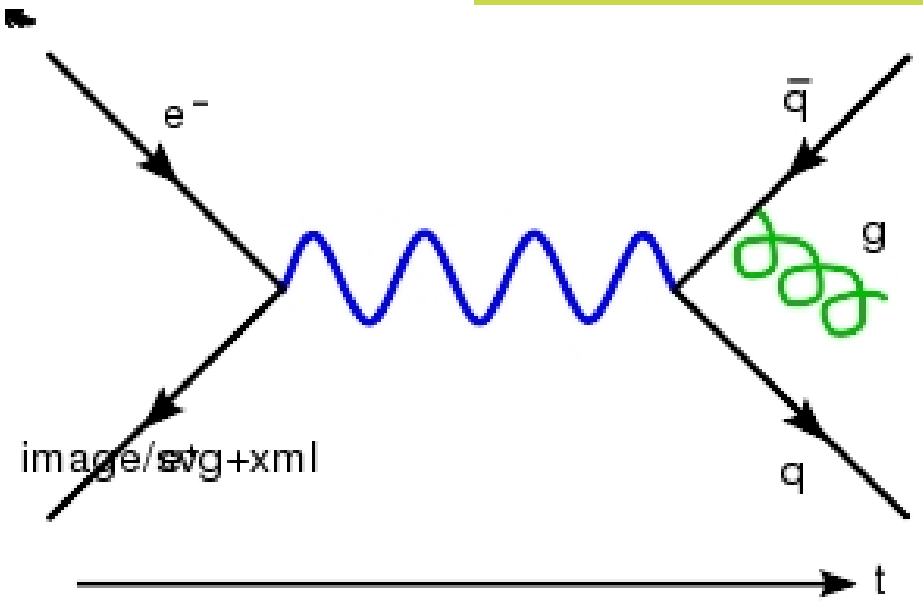
1. Tener caracterizada la noción de qubit y poder ensamblar varios de ellos
2. Contar con un conjunto de compuertas cuánticas primitivas que permitan realizar cualquier algoritmo
3. Poder inicializar una lista de qubits en estados puros determinados
4. Poder ejecutar la operación de toma de mediciones
5. Que los tiempos de decoherencia excedan los de aplicación de las compuertas cuánticas primitivas

The Mid-Level Quantum Computation Roadmap: Promise Criteria

QC Approach	The DiVincenzo Criteria							
	Quantum Computation						QC Networkability	
	#1	#2	#3	#4	#5		#6	#7
NMR								
Trapped Ion								
Neutral Atom								
Cavity QED								
Optical								
Solid State								
Superconducting								
Unique Qubits	This field is so diverse that it is not feasible to label the criteria with "Promise" symbols.							

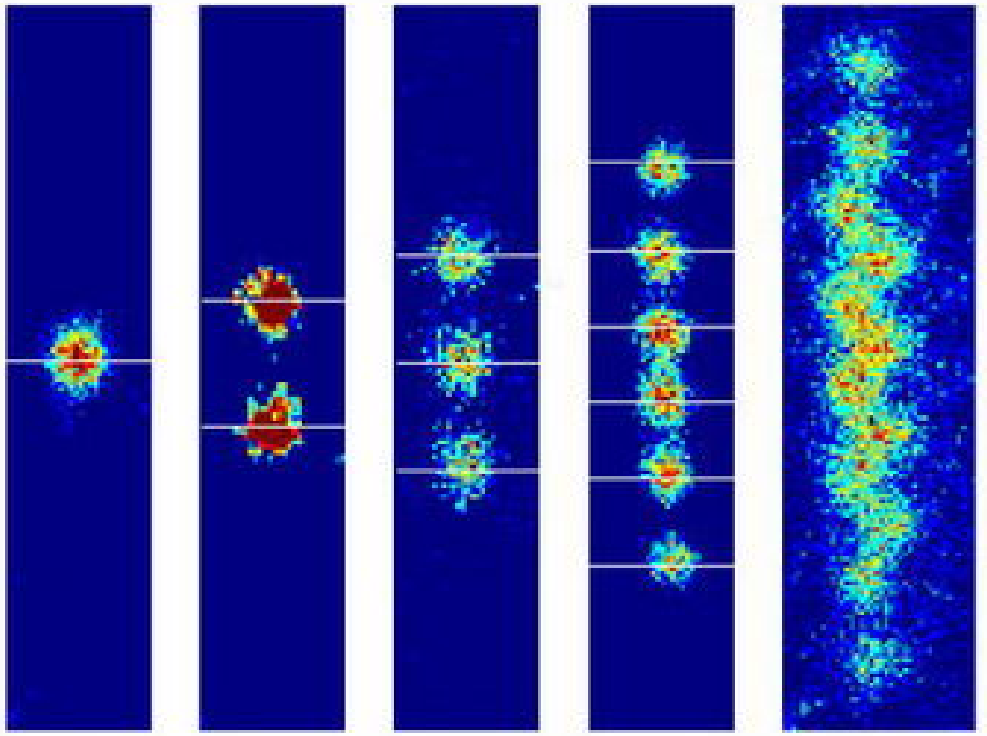
Resonancia nuclear magnética (Nuclear Magnetic Resonance (NMR)):
Un conjunto de moléculas en una solución líquida en el que siete *espines* en cada molécula hacen las veces de siete qubits. Con esto, se puede factorizar a 15 como el producto de 3 por 5. Sin embargo, no podría extenderse el modelo a más de 10 qubits.





Cavidad electrodinámica cuántica (Cavity Quantum Electro-Dynamics (Cavity QED)):
Interacción entre un qubit material (realizado como un átomo atrapado o sistema puntual semiconductor) y un campo cuantizado (un fotón) de un resonador de microondas. La dinámica coherente resulta de una *cavidad* para ampliar la frecuencia coherente de Rabi entre el átomo y el campo. El modelo convierte estados de qubits materiales y qubits de fotones y es apto para protocolos de 2-quregistros.
Ha sido utilizado en comunicaciones por el grupo del profesor catalán J.I. Cirac del Instituto Max Planck.

Trampas de iones (Ion Trap):
Se utiliza arreglos de trampas de iones interconectados por fotones o por iones que hacen las veces de cabezas lectoras para transmit información entre arreglos. Los qubits dados como iones se mueven en diferentes zonas de trampas sin decoherencia en tiempos adecuados para aplicar compuertas cuánticas. Las trampas pueden realizarse como sistemas micro-electro-mecánicos o mediante técnicas de nanofabricación.



Criptografía

El Cómputo Cuántico ha permitido diversos protocolos para el establecimiento de claves comunes. Una característica de ellos es que es incluso posible detectar la sola presencia de un intruso.
Sea $E^0 = \{\mathbf{e}_0^0, \mathbf{e}_1^0\} = \{|0\rangle, |1\rangle\}$ la base canónica de $\mathbb{H}_1$ y sea $H(E^0) = E^1 = \{\mathbf{e}_0^1, \mathbf{e}_1^1\} = \{H|0\rangle, H|1\rangle\}$ la base de $\mathbb{H}_1$ obtenida al aplicar la transformación de Hadamard a E^0. E^0 puede corresponder a un *spin* con polarización *vertical–horizontal*, $E^0 = \{\uparrow, \rightarrow\}$, y E^1 a un *spin* con polarización *oblicua*, *NO–NE*, $E^1 = \{\nwarrow, \nearrow\}$.
Dos partes, *Alicia* y *Beto*, han de establecer una cllave común.
Cuentan con dos canales de transmisión

Canal cuántico Transmite de manera unidireccional, digamos de Alicia hacia Beto.

Canal clásico Transmite de manera bidireccional.

Supongamos que la transmisión a través de los canales está libre de cualquier ruido.

Protocolo sobre el canal cuántico

1. Alicia genera dos sucesiones de bits $\delta = [\delta_i]_{i=1}^{N}$ y $\varepsilon = [\varepsilon_i]_{i=1}^{N}$. Transmite por el canal cuántico la sucesión de estados $S = \left[\mathbf{s}_i = \mathbf{e}_{\delta_i}^{\varepsilon_i}\right]_{i=1}^{N}$.
2. Beto genera una sucesión de bits $\eta = [\eta_i]_{i=1}^{N}$ y realiza una medición de cada qubit $\mathbf{s}_i$ respecto a la base E^{η_i} para obtener así una sucesión de bits $\zeta = [\zeta_i]_{i=1}^{N}$. Toda vez que $\varepsilon_i = \eta_i$, se va a tener que $\delta_i = \zeta_i$, por lo que puede esperarse que en casi $N/2$ entradas van a coincidir las sucesiones δ y ζ.

Protocolo sobre el canal clásico

1. Beto le envía su sucesión ζ a Alicia.
2. Alicia calcula el conjunto $J = \{i \leq N | \zeta_i = \varepsilon_i\}$ que corresponde a cuando Beto seleccionó la base correcta. Alicia le envía, de vuelta, J a Beto.
3. Necesariamente las restricciones de δ y de ζ a J, $\delta|_J$ y $\zeta|_J$, han de coincidir, $\forall j \in J$: $\delta_j = \zeta_j$, y por tanto esa sucesión, o una porción de ella, puede ser asumida como la llave en común. La única manera en la que δ y ζ podrían diferir sería mediante la intromisión de una tercera parte, Isabel.
4. Para revisar si acaso hubo una intromisión, Alicia y Beto intercambian porciones de sus respectivas sucesiones $\delta|_J$ y $\zeta|_J$. Cada vez que intercambian una porción, la suprimen de sus sucesiones. Si en alguna pareja de porciones intercambiadas aparece una discrepancia, se detecta la intromisión de Isabel. De otra manera, se puede confiar con una muy alta probabilidad que la llave en común ya ha sido establecida.

¿Preguntas? ¡Gracias!

Guillermo Morales-Luna
gmorales@cs.cinvestav.mx
http://delta.cs.cinvestav.mx/~gmorales