

Modelo Discreto de Computación Cuántica

Jesús García López de Lacalle

Grupo de Investigación en Información y
Computación Cuántica (GIICC)

Escuela Técnica Superior de Ingeniería de Sistemas Informáticos

Universidad Politécnica de Madrid

Modelo Discreto de Computación Cuántica

1. Modelo de computación cuántica
2. Estados cuánticos discretos
3. Puertas cuánticas discretas
4. Conclusiones

1. Modelo de computación cuántica

Representación de la información (estados cuánticos)

bit	qubit
0	$ 0\rangle$
1	$ 1\rangle$
— — —	$a_0 0\rangle + a_1 1\rangle$

$$a_0, a_1 \in \mathbb{C}$$

$$|a_0|^2 + |a_1|^2 = 1$$

Ejemplos:

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad \frac{|0\rangle - i|1\rangle}{\sqrt{2}}, \quad \frac{\sqrt{3}|0\rangle + |1\rangle}{2}$$

Notación (por comodidad escribiremos los estados cuánticos sin normalizar):

$$|0\rangle + |1\rangle, \quad |0\rangle - i|1\rangle, \quad \sqrt{3}|0\rangle + |1\rangle$$

1. Modelo de computación cuántica

Representación de la información (estados cuánticos)

2-bit	2-qubit
00	$ 00\rangle$
01	$ 01\rangle$
10	$ 10\rangle$
11	$ 11\rangle$
— — —	$a_0 00\rangle + \dots + a_3 11\rangle$

$$a_0, \dots, a_3 \in \mathbb{C}$$

$$|a_0|^2 + \dots + |a_3|^2 = 1$$

Ejemplos:

$$|00\rangle + |11\rangle, \quad (1 - i)|00\rangle - (1 + i)|11\rangle, \quad |00\rangle + i|01\rangle + 2|10\rangle - 3i|11\rangle$$

Base de computación:

$$n = \text{núm. qubits}$$

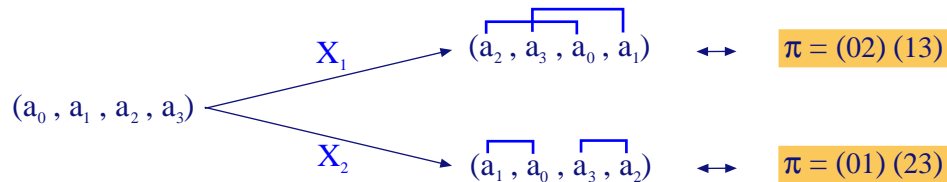
$$N = 2^n = \text{dimensión}$$

$$\left[|00\rangle, |01\rangle, |10\rangle, |11\rangle \right]$$

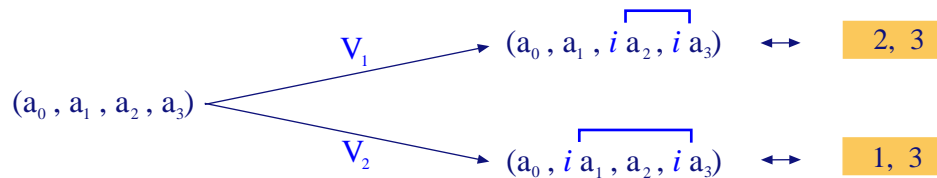
1. Modelo de computación cuántica

Transformación de la información (puertas cuánticas)

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}: \quad \begin{array}{|l} X|0\rangle = |1\rangle \\ X|1\rangle = |0\rangle \end{array} \quad \begin{array}{|l} X_j|*0*\rangle = |*1*\rangle \\ X_j|*1*\rangle = |*0*\rangle \end{array}$$



$$V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}: \quad \begin{array}{|l} V|0\rangle = |0\rangle \\ V|1\rangle = i|1\rangle \end{array} \quad \begin{array}{|l} V_j|*0*\rangle = |*0*\rangle \\ V_j|*1*\rangle = i|*1*\rangle \end{array}$$



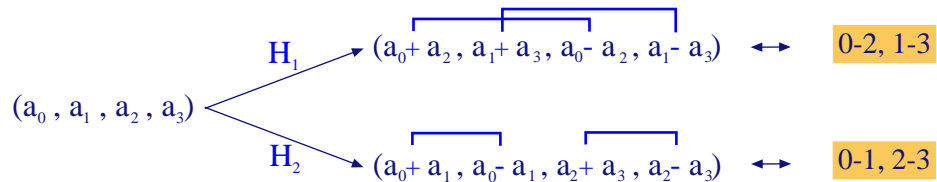
1. Modelo de computación cuántica

Transformación de la información (puertas cuánticas)

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

$$\begin{aligned} H|0\rangle &= |0\rangle + |1\rangle \\ H|1\rangle &= |0\rangle - |1\rangle \end{aligned}$$

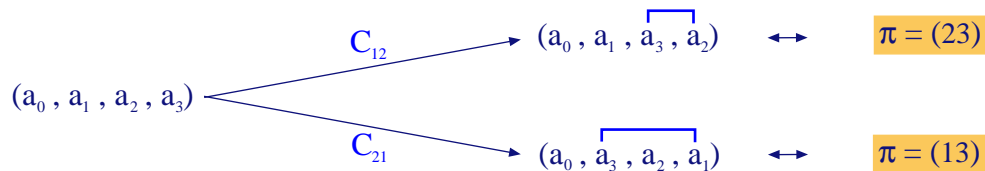
$$\begin{aligned} H_j|*0*\rangle &= |*0*\rangle + |*1*\rangle \\ H_j|*1*\rangle &= |*0*\rangle - |*1*\rangle \end{aligned}$$



$$C = \begin{pmatrix} I & \\ & X \end{pmatrix}:$$

$$\begin{aligned} C|0x\rangle &= |0x\rangle \\ C|1x\rangle &= |1\bar{x}\rangle \end{aligned}$$

$$\begin{aligned} C_{jk}|*0*x*\rangle &= |*0*x*\rangle \\ C_{jk}|*1*x*\rangle &= |*1*\bar{x}*\rangle \end{aligned}$$

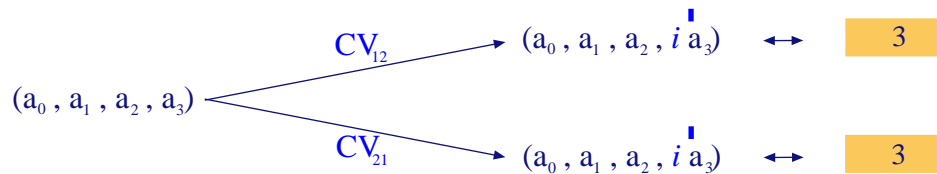


1. Modelo de computación cuántica

Transformación de la información (puertas cuánticas)

$$CV = \begin{pmatrix} I & \\ & V \end{pmatrix}:$$

$CV 0x\rangle = 0x\rangle$	$CV_{jk} *0*x*\rangle = *0*x*\rangle$
$CV x0\rangle = x0\rangle$	$CV_{jk} *x*0*\rangle = *x*0*\rangle$
$CV 11\rangle = i 11\rangle$	$CV_{jk} *1*1*\rangle = i *1*1*\rangle$

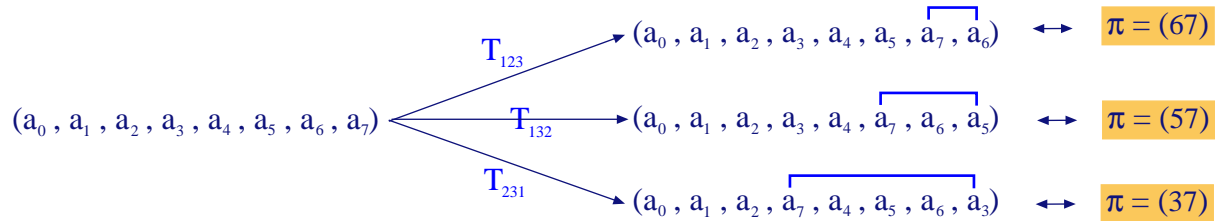


$$T = \begin{pmatrix} I & \\ & C \end{pmatrix}:$$

$T 0xy\rangle = 0xy\rangle$	$T_{jkl} *0*x*y*\rangle = *0*x*y*\rangle$
$T x0y\rangle = x0y\rangle$	$T_{jkl} *x*0*y*\rangle = *x*0*y*\rangle$
$T 11x\rangle = 11\bar{x}\rangle$	$T_{jkl} *1*1*x*\rangle = *1*1*\bar{x}*\rangle$

1. Modelo de computación cuántica

Transformación de la información (puertas cuánticas)



$TV:$	$TV 0xy\rangle = 0xy\rangle$	$TV_{jkl} *0*x*y*\rangle = *0*x*y*\rangle$
	$TV x0y\rangle = x0y\rangle$	$TV_{jkl} *x*0*y*\rangle = *x*0*y*\rangle$
	$TV xy0\rangle = xy0\rangle$	$TV_{jkl} *x*y*0*\rangle = *x*y*0*\rangle$
	$TV 111\rangle = i 111\rangle$	$TV_{jkl} *1*1*1*\rangle = i *1*1*1*\rangle$

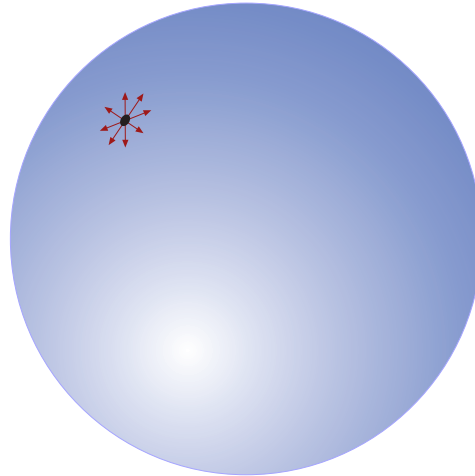
$$TV = \begin{pmatrix} I & \\ & CV \end{pmatrix}: (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7) \xrightarrow{TV_{123}} (a_0, a_1, a_2, a_3, a_4, a_5, a_6, i a_7) \leftrightarrow 7$$

1. Modelo de computación cuántica

Transformación de la información (puertas cuánticas)

Propiedades:

1. Las puertas de un qubit junto con C forman un conjunto universal.
2. Las puertas X , C y T generan el grupo S_N .
3. El modelo es continuo y esto dificulta el control de la propagación de errores.



2. Estados cuánticos discretos

Conjunto discreto de estados cuánticos \mathcal{E}

Definición 1. \mathcal{E} es el menor conjunto que verifica las siguientes propiedades:

1. La base de computación está contenida en \mathcal{E} .
2. El conjunto \mathcal{E} es invariante para las puertas H , V , CV y TV .

Propiedades:

1. El conjunto \mathcal{E} es invariante para las puertas Z , CZ y TZ .

$$Z = V^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad CZ = \begin{pmatrix} I & \\ & Z \end{pmatrix}, \quad TZ = \begin{pmatrix} I & \\ & CZ \end{pmatrix}$$

2. El conjunto \mathcal{E} es invariante para las puertas X , C y T .

$$X = HZH, \quad C = H_2 CZ H_2, \quad T = H_3 TZ H_3$$

2. Estados cuánticos discretos

Caracterización del conjunto \mathcal{E}

Teorema 1. El estado $\psi \in \mathcal{E}$ si y solo si existe $k \in \mathbb{N}$ tal que:

1.
$$\psi = \frac{1}{(\sqrt{2})^k} (x_0 + iy_0, x_1 + iy_1, \dots, x_{N-1} + iy_{N-1})$$

2. Las coordenadas son enteras:

$$x_0, y_0, x_1, y_1, \dots, x_{N-1}, y_{N-1} \in \mathbb{Z}$$

3. Se verifica la ecuación diofántica

$$x_0^2 + y_0^2 + x_1^2 + y_1^2 + \dots + x_{N-1}^2 + y_{N-1}^2 = 2^k$$

Si k es mínimo entonces decimos que el estado pertenece al nivel k :

$$\psi \in \mathcal{L}_k$$

2. Estados cuánticos discretos

Estados reducibles

Definición. Decimos que $\psi = (a_0, a_1, \dots, a_{N-1})$ es **reducible** si verifica que

$$\left. \begin{array}{l} \operatorname{Re}(a_{2k}) \equiv \operatorname{Re}(a_{2k+1}) \pmod{2} \\ \operatorname{Im}(a_{2k}) \equiv \operatorname{Im}(a_{2k+1}) \pmod{2} \end{array} \right\} \text{ para todo } 0 \leq k \leq N/2$$

Propiedad. Sea ψ un estado de \mathcal{L}_k . Entonces

$$\psi \text{ es reducible si y solo si } H_n \psi \in \mathcal{L}_{k-1}$$

Ejemplos:

$$(3, 1 + 2i, i, -i) \in \mathcal{L}_4 \rightarrow (4 + 2i, 2 - 2i, 0, 2i) = (2 + i, 1 - i, 0, i) \in \mathcal{L}_3$$

$$(3, 2 + i, i, -i) \in \mathcal{L}_4 \rightarrow (5 + i, 1 - i, 0, 2i) \in \mathcal{L}_5$$

2. Estados cuánticos discretos

La demostración (teorema 1) de que $\bigcup_{k=0}^{\infty} \mathcal{L}_k \subseteq \mathcal{E}$ es constructiva

Nivel 2	(1 + i , 0 , 0 , -1 + i)	$X_2 C_{21} X_2$
	(0 , 0 , 1 + i , -1 + i)	H_2
-----	(0 , 0 , 2i , 2)	simplificar
Nivel 1	(0 , 0 , i , 1)	X_2
	(0 , 0 , 1 , i)	$C V_{12}$
	(0 , 0 , 1 , -1)	H_2
-----	(0 , 0 , 0 , 2)	simplificar
Nivel 0	(0 , 0 , 0 , 1)	

2. Estados cuánticos discretos

Demostración del teorema 1

Propiedades. Sea $\psi \in \mathcal{L}_k$, con $k > 0$:

- a) El número de componentes impares (reales o imaginarias) de ψ es par.
- b) El número de coordenadas (p, i) o (i, p) de ψ es par.

Demostración. Sea $\psi \in \mathcal{L}_k$, con $k > 0$. Convertir ψ en reducible del siguiente modo:

- a) Transformar todas las coordenadas (i, p) en (p, i) .
- b) Reordenar las coordenadas de modo que las posiciones $2k$ y $2k + 1$ ($k > 0$) sean

$$(p, i) - (p, i), \quad (p, p) - (p, p) \quad \text{ó} \quad (i, i) - (i, i)$$

- c) Si las coordenadas 0 y 1 tienen una de las configuraciones anteriores ψ es reducible:

$$H_n \psi \in \mathcal{L}_{k-1}$$

2. Estados cuánticos discretos

Demostración del teorema 1

d) Si la configuración de las coordenadas $\mathbf{0}$ y $\mathbf{1}$ es $(\mathbf{p}, \mathbf{p}) - (\mathbf{i}, \mathbf{i})$, consideramos

$$\mathbf{R} = \tilde{\mathbf{V}} \mathbf{H}_n \tilde{\mathbf{V}} \mathbf{H}_n \quad \text{donde} \quad \begin{cases} \tilde{\mathbf{V}}|0 \cdots 01\rangle = i|0 \cdots 01\rangle \\ \tilde{\mathbf{V}}|x_0 \cdots x_n\rangle = |x_0 \cdots x_n\rangle \quad \text{e. o. c.} \end{cases}$$

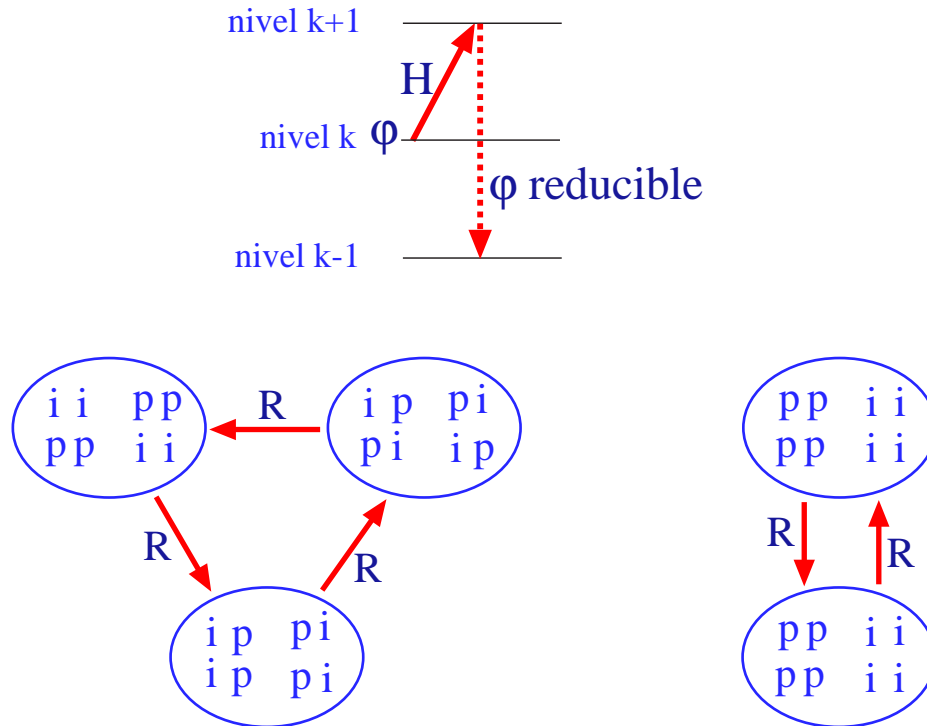
\mathbf{R} modifica exclusivamente las coordenadas $\mathbf{0}$ y $\mathbf{1}$ del siguiente modo:

$$\begin{aligned} \begin{pmatrix} x_0 + iy_0 \\ x_1 + iy_1 \end{pmatrix} &\Rightarrow \frac{1}{2} \begin{pmatrix} (x_0 - y_0 + x_1 + y_1) + i(x_0 + y_0 - x_1 + y_1) \\ (x_0 - y_0 - x_1 - y_1) + i(x_0 + y_0 + x_1 - y_1) \end{pmatrix} \\ &= \begin{pmatrix} (x'_0 - y'_0 + x'_1 + y'_1 + 1) + i(x'_0 + y'_0 - x'_1 + y'_1) \\ (x'_0 - y'_0 - x'_1 - y'_1 - 1) + i(x'_0 + y'_0 + x'_1 - y'_1) \end{pmatrix} \end{aligned}$$

Por tanto, $\mathbf{R}\psi$ es reducible: $\mathbf{H}_n \mathbf{R}\psi \in \mathcal{L}_{k-1}$

2. Estados cuánticos discretos

Propiedades de H_n y de R



3. Puertas cuánticas discretas

Conjunto discreto de puertas cuánticas \mathcal{P}

Definición 2. Una puerta cuántica $P \in \mathcal{P}$ si y solo si para todo $\psi \in \mathcal{E}$ se verifica

$$P\psi \in \mathcal{E}$$

Por ejemplo:

$$\frac{1}{(\sqrt{2})^6} \begin{pmatrix} 7 + 2i & -2 - 2i & 1 - i & i \\ 3 & 6 + 4i & 1 + i & -i \\ -1 - i & -1 + i & 7 + i & -1 + 3i \\ 0 & 1 - i & -1 + 3i & 6 + 4i \end{pmatrix} \in \mathcal{P}$$

Caracterización.

$P \in \mathcal{P}$ si y solo si sus columnas son estados discretos de niveles con la misma paridad.

Propiedad. El conjunto \mathcal{P} es un grupo multiplicativo.

3. Puertas cuánticas discretas

Conjunto universal de puertas cuánticas discretas

Nota. C junto con las puertas cuánticas discretas de un qubit no lo es.

$$\text{Núm. sol. } \{x_0^2 + y_0^2 + x_1^2 + y_1^2 = 2^k\} = 24 \quad \text{para todo } k > 0$$

Conjetura. Las puertas cuánticas discretas de dos qubits forman un conjunto universal.

Teorema 2:

Toda puerta discreta de dos qubits es producto de puertas H , V , CV y TV .

Corolario de la conjetura. El modelo propuesto tiene un conjunto universal finito:

$$H, V, CV, TV$$

3. Puertas cuánticas discretas

Ilustración del teorema 2

$$\begin{pmatrix} 7 + 2i & -2 - 2i & 1 - i & i \\ 3 & 6 + 4i & 1 + i & -i \\ -1 - i & -1 + i & 7 + i & -1 + 3i \\ 0 & 1 - i & -1 + 3i & 6 + 4i \end{pmatrix} \in \mathcal{P}_6$$

$$\Downarrow R_f^*$$

$$\begin{pmatrix} 7 + 2i & -2 - 2i & 1 - i & i \\ 3 & 6 + 4i & 1 + i & -i \\ -i & -1 - i & 4 + 6i & 3 \\ -i & -1 + i & 2 + 2i & -7 + 2i \end{pmatrix} \in \mathcal{P}_6$$

$$\Downarrow H_2$$

$$\begin{pmatrix} 5 + i & 2 + i & 1 & 0 \\ 2 + i & -4 - 3i & -i & i \\ -i & -1 & 3 + 4i & -2 + i \\ 0 & -i & 1 + 2i & 5 - i \end{pmatrix} \in \mathcal{P}_5$$

3. Puertas cuánticas discretas

Ilustración del teorema 2

$$\begin{pmatrix} 5+i & 2+i & 1 & 0 \\ 2+i & -4-3i & -i & i \\ -i & -1 & 3+4i & -2+i \\ 0 & -i & 1+2i & 5-i \end{pmatrix} \in \mathcal{P}_5$$

$$\Downarrow (24)_f, (24)_c$$

$$\begin{pmatrix} 5+i & 0 & 1 & 2+i \\ 0 & 5-i & 1+2i & -i \\ -i & -2+i & 3+4i & -1 \\ 2+i & i & -i & -4-3i \end{pmatrix} \in \mathcal{P}_5$$

$$\Downarrow R_c^2$$

$$\begin{pmatrix} 2+3i & 2+3i & 1 & 2+i \\ -2+3i & 2-3i & 1+2i & -i \\ 1-2i & i & 3+4i & -1 \\ i & 1+2i & -i & -4-3i \end{pmatrix} \in \mathcal{P}_5$$

3. Puertas cuánticas discretas

Ilustración del teorema 2

$$\begin{pmatrix} 2 + 3i & 2 + 3i & 1 & 2 + i \\ -2 + 3i & 2 - 3i & 1 + 2i & -i \\ 1 - 2i & i & 3 + 4i & -1 \\ i & 1 + 2i & -i & -4 - 3i \end{pmatrix} \in \mathcal{P}_5$$

$$\Downarrow V_{12}$$

$$\begin{pmatrix} 2 + 3i & 2 + 3i & 1 & 2 + i \\ -2 + 3i & 2 - 3i & 1 + 2i & -i \\ 1 - 2i & i & 3 + 4i & -1 \\ -1 & -2 + i & 1 & 3 - 4i \end{pmatrix} \in \mathcal{P}_5$$

$$\Downarrow H_2$$

$$\begin{pmatrix} 3i & 2 & 1 + i & 1 \\ 2 & 3i & -i & 1 + i \\ -i & -1 + i & 2 + 2i & 1 - 2i \\ 1 - i & 1 & 1 + 2i & -2 + 2i \end{pmatrix} \in \mathcal{P}_4$$

3. Puertas cuánticas discretas

Demostración del teorema 2

Definiciones. Sea $P = (a_{ij}) \in \mathcal{P}$ una puerta discreta de dos qubits. Decimos que:

a) P es de **nivel k** , $P \in \mathcal{P}_k$, si para todo $0 \leq i \leq 3$ verifica

$$\sum_{j=0}^3 |a_{ij}|^2 = 2^k$$

b) P es **f-estándar** si para todo $0 \leq i \leq 3$ y $0 \leq j \leq 1$ se verifica

$$\operatorname{Re}(a_{i,2j}) + \operatorname{Im}(a_{i,2j}) + \operatorname{Re}(a_{i,2j+1}) + \operatorname{Im}(a_{i,2j+1}) = 0 \pmod{2}$$

c) P es **c-estándar** si para todo $0 \leq i \leq 1$ y $0 \leq j \leq 3$ se verifica

$$\operatorname{Re}(a_{2i,j}) + \operatorname{Im}(a_{2i,j}) + \operatorname{Re}(a_{2i+1,j}) + \operatorname{Im}(a_{2i+1,j}) = 0 \pmod{2}$$

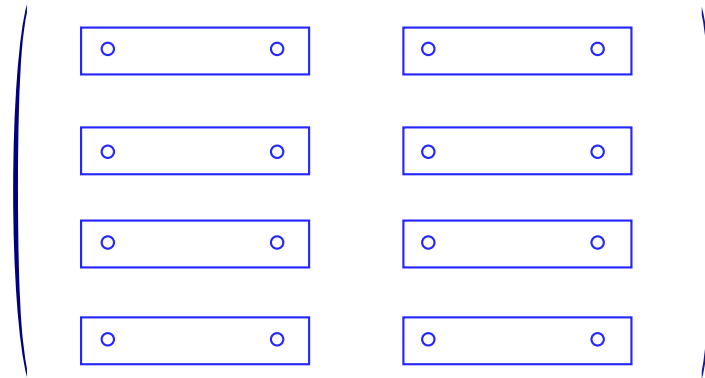
d) P es **estándar** si es f-estándar y es c-estándar.

3. Puertas cuánticas discretas

Demostración del teorema 2

Definiciones. Sea $P = (a_{ij}) \in \mathcal{P}$ una puerta discreta de dos qubits. Decimos que:

- e) P es **reducible** si sus vectores columna lo son: $H_2 P \in \mathcal{P}_{k-1}$
- f) P es **semi-reducible** si la submatriz formada por las filas 3 y 4 lo es.
- g) La **paridad** del elemento a_{ij} es $\text{Re}(a_{ij}) + \text{Im}(a_{ij}) \pmod{2}$.



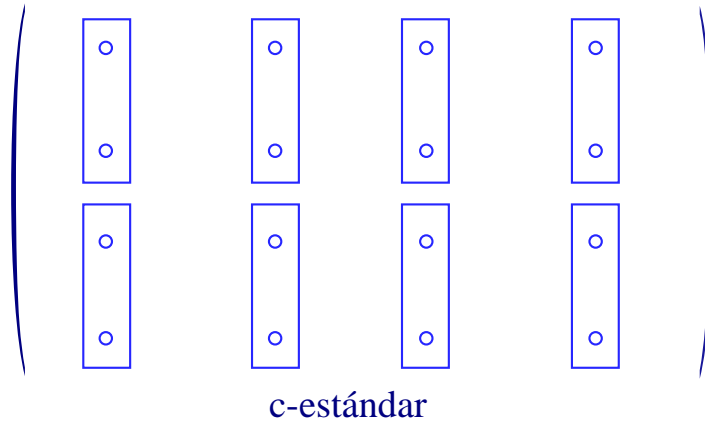
f-estándar

3. Puertas cuánticas discretas

Demostración del teorema 2

Definiciones. Sea $P = (a_{ij}) \in \mathcal{P}$ una puerta discreta de dos qubits. Decimos que:

- e) P es **reducible** si sus vectores columna lo son: $H_2 P \in \mathcal{P}_{k-1}$
- f) P es **semi-reducible** si la submatriz formada por las filas 2 y 3 lo es.
- g) La **paridad** del elemento a_{ij} es $\text{Re}(a_{ij}) + \text{Im}(a_{ij}) \pmod{2}$.

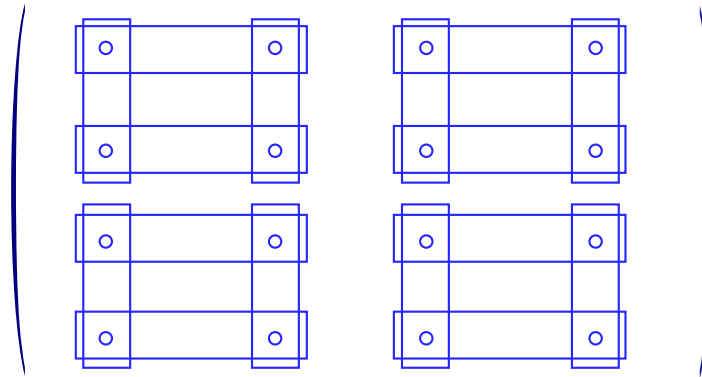


3. Puertas cuánticas discretas

Demostración del teorema 2

Definiciones. Sea $P = (a_{ij}) \in \mathcal{P}$ una puerta discreta de dos qubits. Decimos que:

- e) P es **reducible** si sus vectores columna lo son: $H_2 P \in \mathcal{P}_{k-1}$
- f) P es **semi-reducible** si la submatriz formada por las filas 2 y 3 lo es.
- g) La **paridad** del elemento a_{ij} es $\text{Re}(a_{ij}) + \text{Im}(a_{ij}) \pmod{2}$.



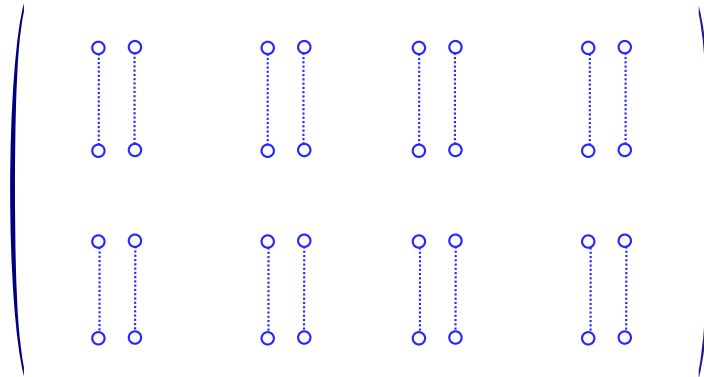
estándar

3. Puertas cuánticas discretas

Demostración del teorema 2

Definiciones. Sea $P = (a_{ij}) \in \mathcal{P}$ una puerta discreta de dos qubits. Decimos que:

- e) P es **reducible** si sus vectores columna lo son: $H_2 P \in \mathcal{P}_{k-1}$
- f) P es **semi-reducible** si la submatriz formada por las filas 2 y 3 lo es.
- g) La **paridad** del elemento a_{ij} es $\text{Re}(a_{ij}) + \text{Im}(a_{ij}) \pmod{2}$.



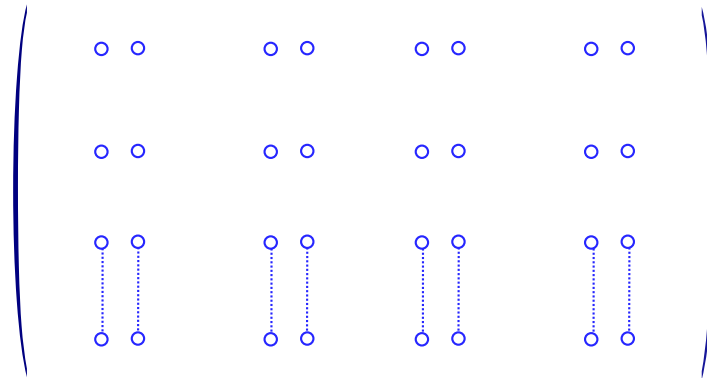
reducible

3. Puertas cuánticas discretas

Demostración del teorema 2

Definiciones. Sea $P = (a_{ij}) \in \mathcal{P}$ una puerta discreta de dos qubits. Decimos que:

- e) P es **reducible** si sus vectores columna lo son: $H_2 P \in \mathcal{P}_{k-1}$
- f) P es **semi-reducible** si la submatriz formada por las filas 2 y 3 lo es.
- g) La **paridad** del elemento a_{ij} es $\text{Re}(a_{ij}) + \text{Im}(a_{ij}) \pmod{2}$.



semi-reducible

3. Puertas cuánticas discretas

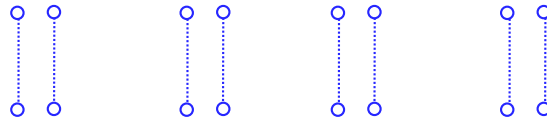
Demostración del teorema 2

Propiedades. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits. Entonces se cumple que:

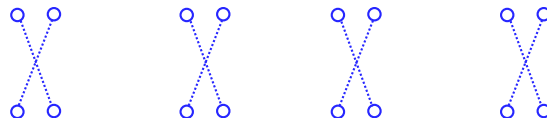
a) En toda fila (columna) de P el número de componentes impares es par.

$$\sum_{j(i)=0}^3 \text{Re}^2(a_{ij}) + \text{Im}^2(a_{ij}) = 2^k$$

b) En todo par de filas el núm. de coincidencias de comp. impares es par.



c) En todo par de filas el núm. de coincidencias cruzadas de comp. impares es par.



3. Puertas cuánticas discretas

Demostración del teorema 2

Propiedades. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits. Entonces se cumple que:

d) P se puede transformar en f-estándar (c-estándar), reordenando columnas (filas).

Demostración:

Si en cada fila todos los elementos tienen la misma paridad: \checkmark

Si hay una fila con configuración (p, p, i, i) , reordenando filas si es preciso:

Basta probar que no puede existir otra con configuración (p, i, p, i) :

fila 1	p	p	i	i				
fila 2	p	i	p	i				
coincidencias	0	2	0	1	0	1	0	1
coinc. cruz.	0	2	0	1	0	1	1	0

Y todas las combinaciones contradicen la propiedad (b) o (c): \checkmark

3. Puertas cuánticas discretas

Demostración del teorema 2

Propiedades. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits. Entonces se cumple que:

- e) P se puede transformar en estándar, reordenando filas y columnas.
- f) En toda fila de P el núm. de coordenadas impares es par.

Es una forma de reescribir la propiedad (a).

- g) En número de filas con configuración (i, i, i, i) es par.

$$\begin{pmatrix} i & i & i & i \\ i & i & i & i \\ i & i & i & i \end{pmatrix}$$

3. Puertas cuánticas discretas

Demostración del teorema 2

Propiedades. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits. Entonces se cumple que:

- e) P se puede transformar en estándar, reordenando filas y columnas.
- f) En toda fila de P el núm. de coordenadas impares es par.

Es una forma de reescribir la propiedad (a).

- g) En número de filas con configuración (i, i, i, i) es par.

$$\begin{pmatrix} i & i & i & i \\ i & i & i & i \\ i & i & i & i \\ i & i & i & i \end{pmatrix}$$

3. Puertas cuánticas discretas

Demostración del teorema 2

Propiedades. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits. Entonces se cumple que:

- e) P se puede transformar en estándar, reordenando filas y columnas.
- f) En toda fila de P el núm. de coordenadas impares es par.

Es una forma de reescribir la propiedad (a).

- g) En número de filas con configuración (i, i, i, i) es par.

$$\begin{pmatrix} i & & & \\ & i & & \\ & & i & \\ & & & i \end{pmatrix}$$

3. Puertas cuánticas discretas

Demostración del teorema 2

Propiedades. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits. Entonces se cumple que:

- e) P se puede transformar en estándar, reordenando filas y columnas.
- f) En toda fila de P el núm. de coordenadas impares es par.

Es una forma de reescribir la propiedad (a).

- g) En número de filas con configuración (i, i, i, i) es par.

$$\begin{pmatrix} i & i & i & i \\ i & i & p & p \\ p & p & i & i \end{pmatrix}$$

3. Puertas cuánticas discretas

Demostración del teorema 2

Propiedades. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits. Entonces se cumple que:

- e) P se puede transformar en estándar, reordenando filas y columnas.
- f) En toda fila de P el núm. de coordenadas impares es par.

Es una forma de reescribir la propiedad (a).

- g) En número de filas con configuración (i, i, i, i) es par.

$$\begin{pmatrix} i & i & i & i \\ i & i & p & p \\ p & p & i & i \\ & i & i & \end{pmatrix}$$

3. Puertas cuánticas discretas

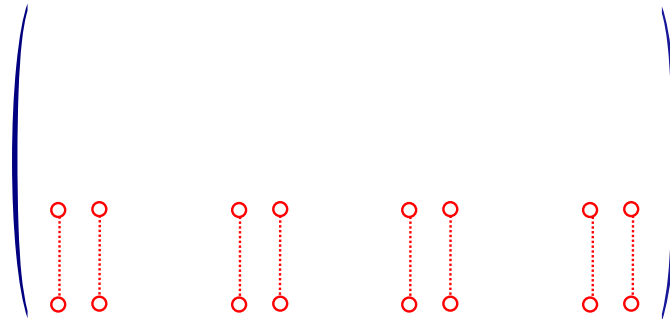
Demostración del teorema 2

Lema 1. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits semi-reducible. Entonces P se puede transformar en reducible.

Demostración.

P es c-estándar y se puede transformar en estándar manteniendo la semi-reducibilidad.

La submatriz generada por las filas 1 y 2 cumple las propiedades (a), (b), (c), (g) y (f).



3. Puertas cuánticas discretas

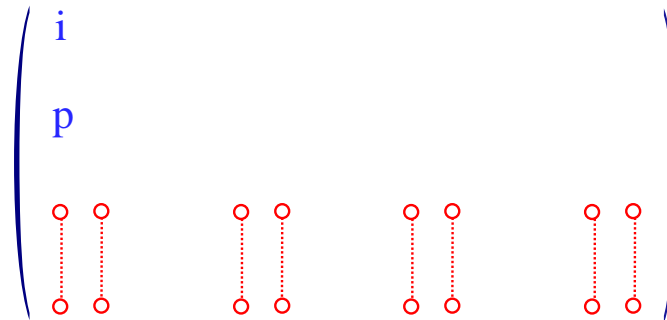
Demostración del teorema 2

Lema 1. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits semi-reducible. Entonces P se puede transformar en reducible.

Demostración.

P es c-estándar y se puede transformar en estándar manteniendo la semi-reducibilidad.

La submatriz generada por las filas 1 y 2 cumple las propiedades (a), (b), (c), (g) y (f).



3. Puertas cuánticas discretas

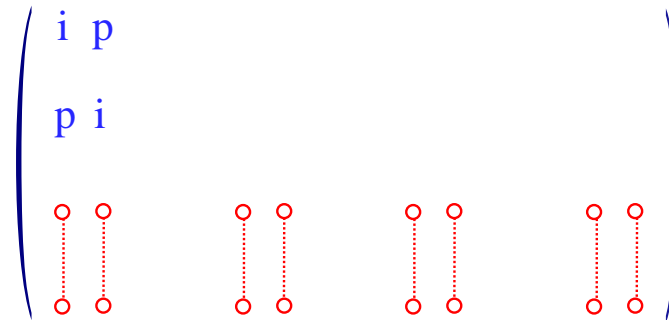
Demostración del teorema 2

Lema 1. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits semi-reducible. Entonces P se puede transformar en reducible.

Demostración.

P es c-estándar y se puede transformar en estándar manteniendo la semi-reducibilidad.

La submatriz generada por las filas 1 y 2 cumple las propiedades (a), (b), (c), (g) y (f).



3. Puertas cuánticas discretas

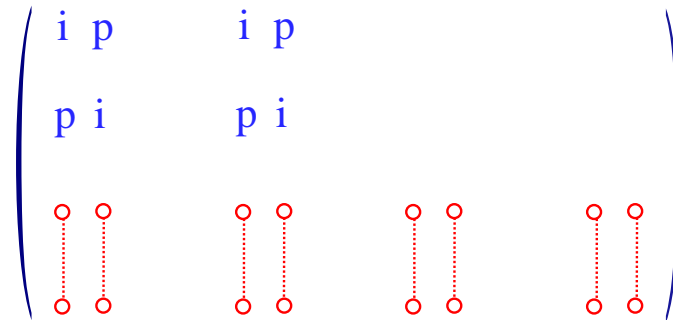
Demostración del teorema 2

Lema 1. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits semi-reducible. Entonces P se puede transformar en reducible.

Demostración.

P es c-estándar y se puede transformar en estándar manteniendo la semi-reducibilidad.

La submatriz generada por las filas 1 y 2 cumple las propiedades (a), (b), (c), (g) y (f).



3. Puertas cuánticas discretas

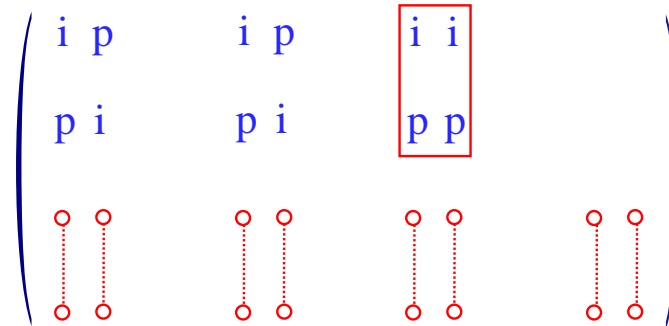
Demostración del teorema 2

Lema 1. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits semi-reducible. Entonces P se puede transformar en reducible.

Demostración.

P es c-estándar y se puede transformar en estándar manteniendo la semi-reducibilidad.

La submatriz generada por las filas 1 y 2 cumple las propiedades (a), (b), (c), (g) y (f).



3. Puertas cuánticas discretas

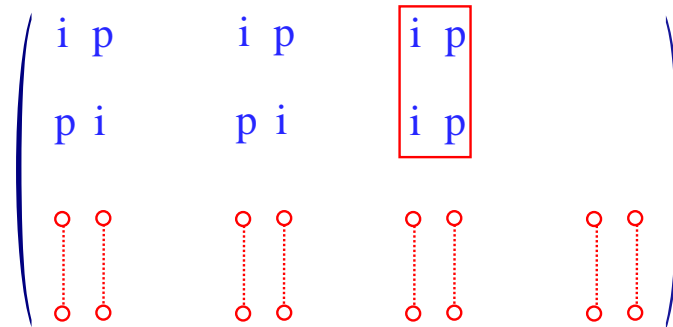
Demostración del teorema 2

Lema 1. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits semi-reducible. Entonces P se puede transformar en reducible.

Demostración.

P es c-estándar y se puede transformar en estándar manteniendo la semi-reducibilidad.

La submatriz generada por las filas 1 y 2 cumple las propiedades (a), (b), (c), (g) y (f).



3. Puertas cuánticas discretas

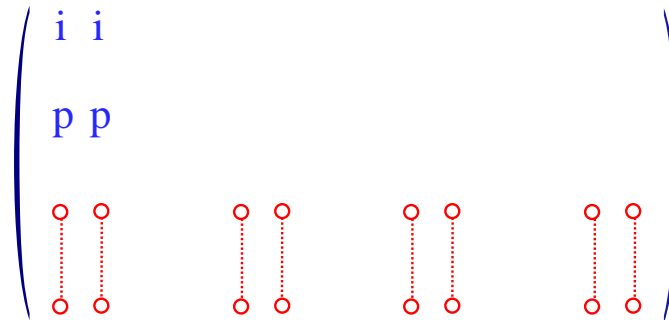
Demostración del teorema 2

Lema 1. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits semi-reducible. Entonces P se puede transformar en reducible.

Demostración.

P es c-estándar y se puede transformar en estándar manteniendo la semi-reducibilidad.

La submatriz generada por las filas 1 y 2 cumple las propiedades (a), (b), (c), (g) y (f).



3. Puertas cuánticas discretas

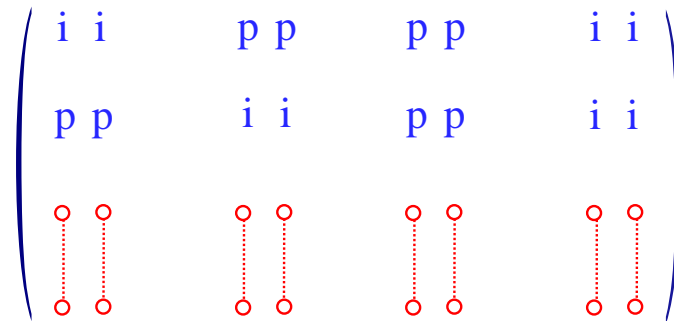
Demostración del teorema 2

Lema 1. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits semi-reducible. Entonces P se puede transformar en reducible.

Demostración.

P es c-estándar y se puede transformar en estándar manteniendo la semi-reducibilidad.

La submatriz generada por las filas 1 y 2 cumple las propiedades (a), (b), (c), (g) y (f).



3. Puertas cuánticas discretas

Demostración del teorema 2

Lema 1. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits semi-reducible. Entonces P se puede transformar en reducible.

Demostración.

Propiedades de la transformación R :

$$\left\{ \begin{array}{cc} i & i \\ p & p \end{array} \quad \begin{array}{cc} p & p \\ i & i \end{array} \right\} \Rightarrow \left\{ \begin{array}{cc} i & p \\ i & p \end{array} \quad \begin{array}{cc} p & i \\ p & i \end{array} \right\}$$

$$\left\{ \begin{array}{cc} p & p \\ p & p \end{array} \quad \begin{array}{cc} i & i \\ i & i \end{array} \right\} \Rightarrow \left\{ \begin{array}{cc} p & p \\ p & p \end{array} \quad \begin{array}{cc} i & i \\ i & i \end{array} \right\}$$

3. Puertas cuánticas discretas

Demostración del teorema 2

Lema 1. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits semi-reducible. Entonces P se puede transformar en reducible.

Demostración.

P es c-estándar y se puede transformar en estándar manteniendo la semi-reducibilidad.

La submatriz generada por las filas 1 y 2 cumple las propiedades (a), (b), (c), (g) y (f).

$$\left(\begin{array}{cc|cc|cc|cc} i & i & p & p & p & p & i & i \\ p & p & i & i & p & p & i & i \\ \hline \circ & \circ & \circ & \circ & \circ & \circ & \circ & \circ \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline \circ & \circ & \circ & \circ & \circ & \circ & \circ & \circ \end{array} \right)$$

Por tanto, RP es reducible.

3. Puertas cuánticas discretas

Demostración del teorema 2

Lema 1. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits semi-reducible. Entonces P se puede transformar en reducible.

Lema 2. Sea $P \in \mathcal{P}$ una puerta discreta de dos qubits. Entonces P se puede transformar en semi-reducible.

Demostración...

4. Conclusiones

Resumen de resultados

1. Se ha definido y caracterizado:
 - a) El conjunto de estados cuánticos discretos \mathcal{E} .
 - b) El conjunto de puertas cuánticas discretas \mathcal{P} .
2. Se han obtenido algoritmos para:
 - a) Construir estados cuánticos discretos.
 - b) Construir puertas cuánticas discretas de dos qubits.

4. Conclusiones

Problemas abiertos

1. Acotar (inferior y superiormente) el tamaño de \mathcal{L}_k .
2. Describir algoritmos para aproximar:
 - a) Estados cuánticos mediante estados cuánticos discretos.
 - b) Puertas cuánticas de un qubit mediante puertas cuánticas discretas de dos qubits.
3. Describir algoritmos eficientes de simulación de:
 - a) La computación cuántica discreta.
 - b) Las medidas de estados cuánticos discretos.
4. Probar la conjetura sobre la universalidad de las puertas discretas de dos qubits.

¡Gracias por su atención!