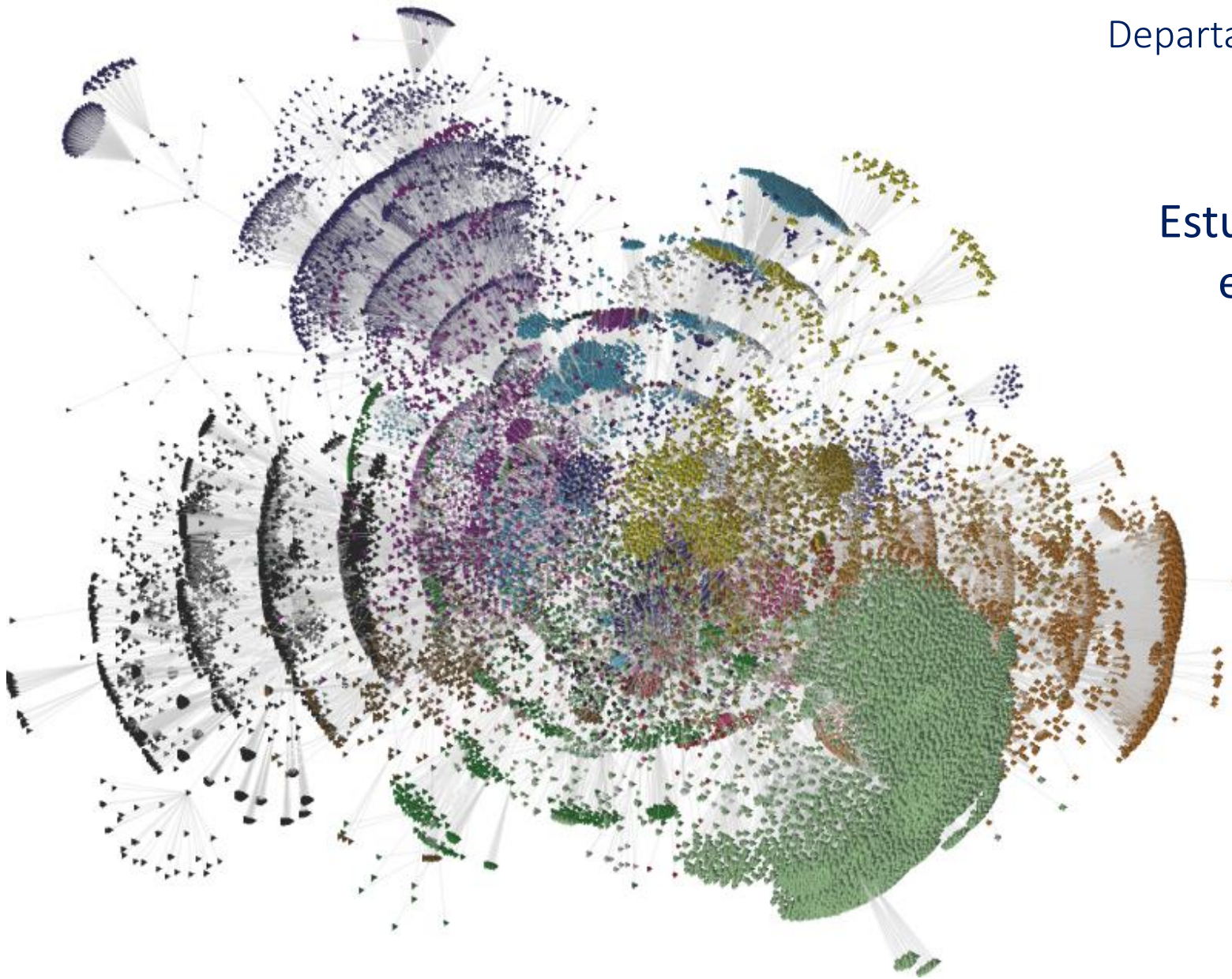


Departamento de Matemática Aplicada a las TIC
ETSI de Sistemas Informáticos – UPM

Estudio de la complejidad de estados en Computación Cuántica discreta

Rafael Martín-Cuevas R.
Doctorando Industrial Accenture - UPM

26 de abril de 2018



Contenidos

Introducción

Bits vs Qubits

Estados cuánticos

Puertas lógicas cuánticas

Computación Cuántica discreta

Descripción del modelo

Conjunto de puertas considerado

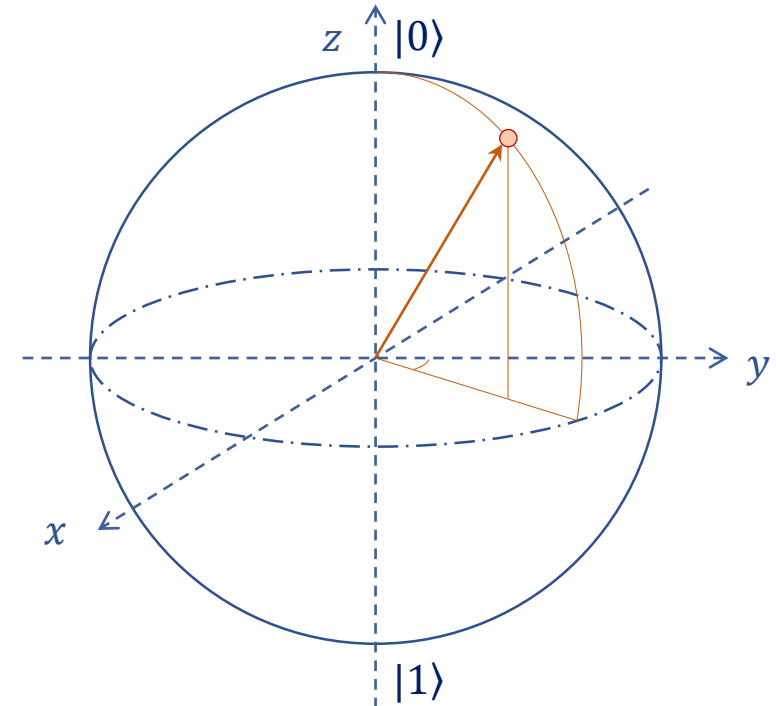
Algoritmo de generalización de puertas de 1 qubit

Complejidad de estados cuánticos

Concepto de complejidad

Algoritmo de generación del árbol de estados

Estados de interés. Conjeturas

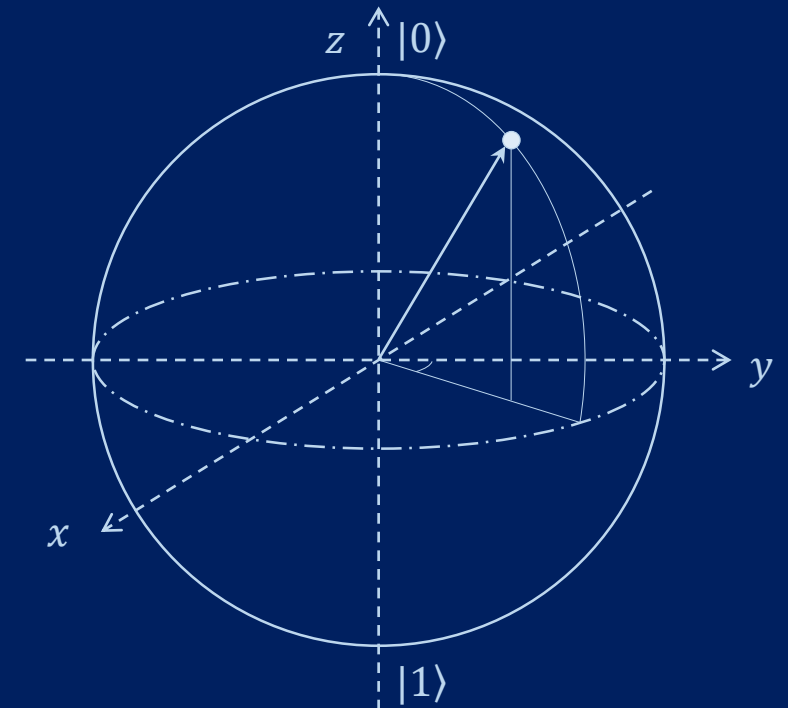


1 Introducción

Bits vs Qubits

Estados cuánticos

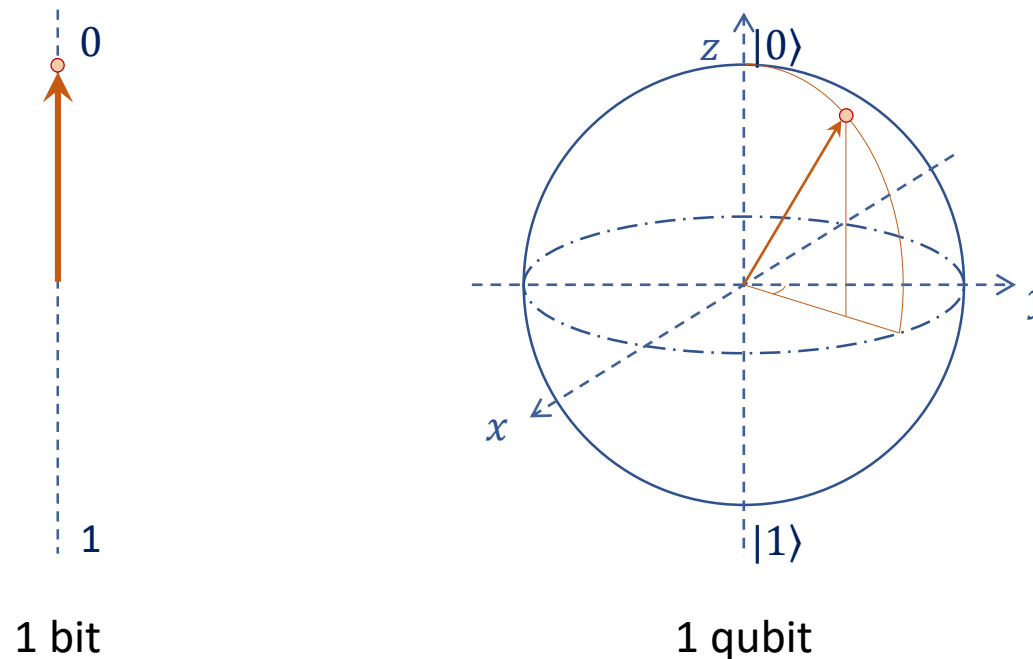
Puertas lógicas cuánticas



Introducción

Bits vs Qubits

Mientras que un bit solamente puede estar en los estados 0 ó 1, un qubit puede estar en uno de ellos o en una proporción de ambos a la vez (**principio de superposición**). Esta situación puede representarse con la **Esfera de Bloch**.

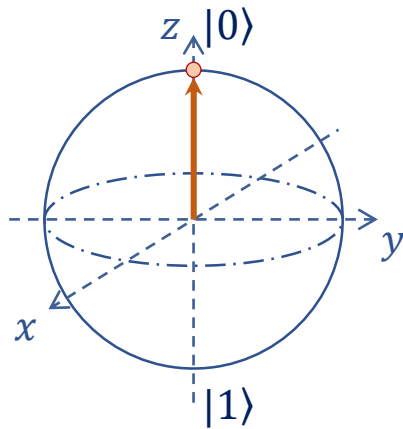


Al medir un estado cuántico, este **colapsa** a uno clásico, con una determinada probabilidad que depende de su “latitud”.

Introducción

Estados cuánticos

Usamos los estados clásicos como base computacional.

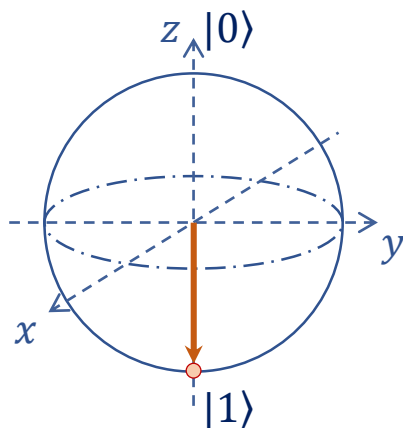


$$1 \cdot |0\rangle + 0 \cdot |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$



$$P(0) = 1^2 = 1 = 100\%$$

$$P(1) = 0^2 = 0 = 0\%$$



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



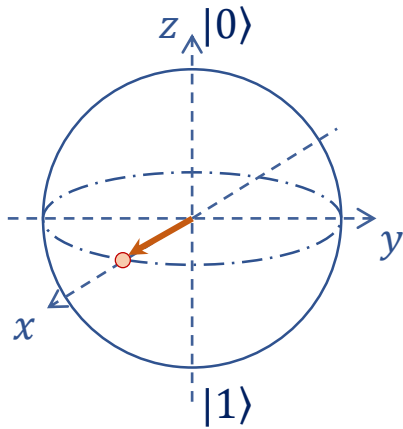
$$P(0) = 0^2 = 0 = 0\%$$

$$P(1) = 1^2 = 1 = 100\%$$

Introducción

Estados cuánticos

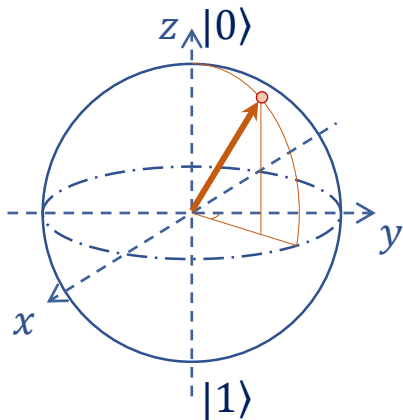
Un qubit puede estar en cualquier superposición lineal de sus dos estados básicos.



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



$$P(0) = \left(\frac{1}{\sqrt{2}}\right)^2 = 1/2 = 50\%$$
$$P(1) = \left(\frac{1}{\sqrt{2}}\right)^2 = 1/2 = 50\%$$



$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}; \quad |\alpha|^2 + |\beta|^2 = 1$$



$$P(0) = |\alpha|^2$$
$$P(1) = |\beta|^2$$

Introducción

Estados cuánticos

Si trabajamos con dos qubits ($n = 2$), encontramos cuatro estados clásicos posibles:

$$|\psi_0\rangle = |00\rangle$$

$$|\psi_1\rangle = |01\rangle$$

$$|\psi_2\rangle = |10\rangle$$

$$|\psi_3\rangle = |11\rangle$$



$$\alpha \cdot |00\rangle + \beta \cdot |01\rangle + \gamma \cdot |10\rangle + \delta \cdot |11\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$$
$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$



$$P(00) = |\alpha|^2$$

$$P(01) = |\beta|^2$$

$$P(10) = |\gamma|^2$$

$$P(11) = |\delta|^2$$

Introducción

Estados cuánticos

Si generalizamos para cualquier longitud n , necesitamos **vectores de longitud 2^n** :

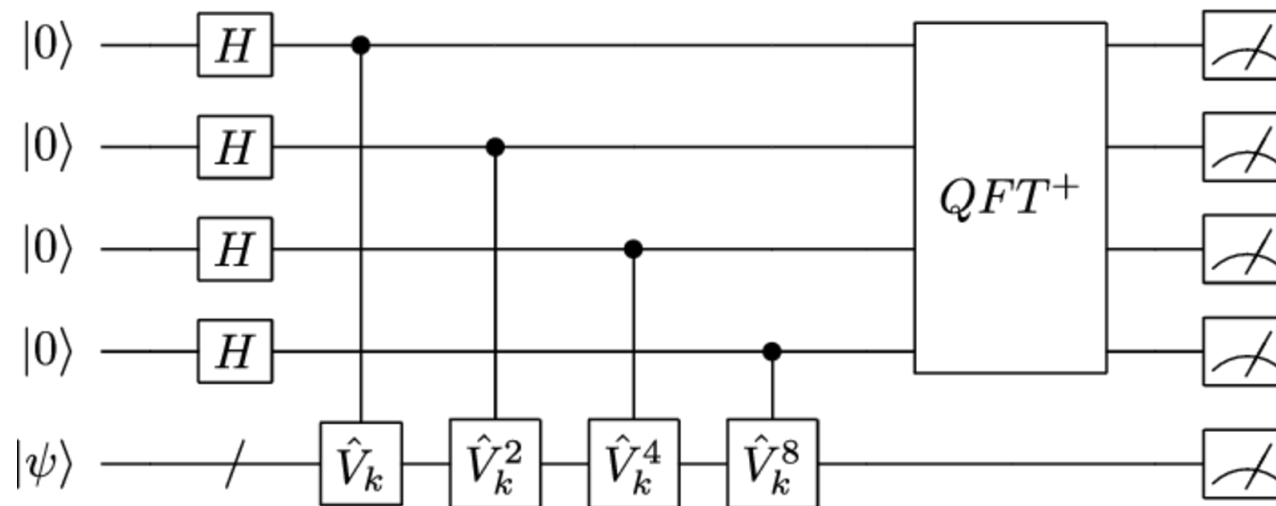
$$\begin{array}{l} |\psi_0\rangle \\ |\psi_1\rangle \\ \dots \\ |\psi_{2^n}\rangle \end{array} \quad \longrightarrow \quad \alpha_0 \cdot |\psi_0\rangle + \alpha_1 \cdot |\psi_1\rangle + \dots + \alpha_{2^n} \cdot |\psi_{2^n}\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \dots \\ \alpha_{2^n} \end{pmatrix} \quad \longrightarrow \quad \begin{array}{l} P(\psi_0) = |\alpha_0|^2 \\ P(\psi_1) = |\alpha_1|^2 \\ \dots \\ P(\psi_{2^n-1}) = |\alpha_{2^n-1}|^2 \end{array}$$
$$\sum_{i=0}^{2^n-1} |\alpha_i| = 1$$

Mientras que un registro de n bits solamente puede estar en un estado de 2^n posibles, un registro de qubits de la misma longitud puede teóricamente estar en **cualquier superposición de todos ellos**.

Introducción

Puertas lógicas cuánticas

Las **puertas lógicas cuánticas** son conceptualmente análogas a las clásicas: reciben un registro de qubits en un determinado estado, y aplican una operación sobre el mismo, para transformarlo.

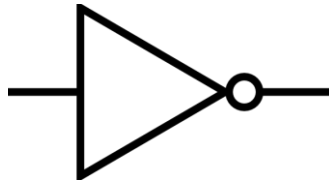


La aplicación de puertas cuánticas **no colapsa los estados**, y permite realizar distintas operaciones.

Introducción

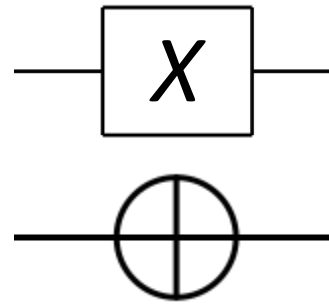
Puertas lógicas cuánticas

Se representan por **matrices cuadradas y unitarias**. Además, a diferencia de la mayoría de puertas lógicas clásicas, son **reversibles**.



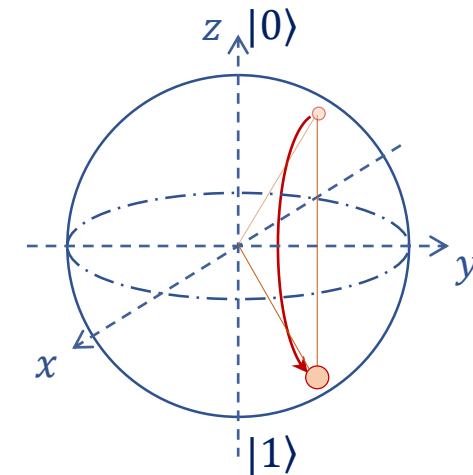
Y	NOT(Y)
0	1
1	0

Puerta NOT clásica



Y	NOT(Y)
$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$
$ \psi\rangle$	$X(\psi\rangle)$

Puerta NOT cuántica

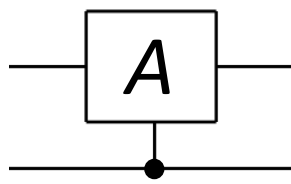


$$\text{Pauli} - X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

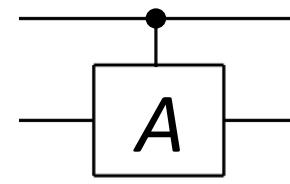
Introducción

Puertas lógicas cuánticas

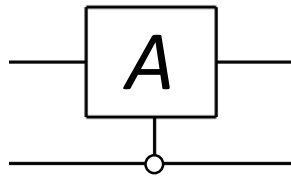
Las puertas cuánticas pueden aplicarse condicionadas al estado de otros qubits, que actúan como **controles**.



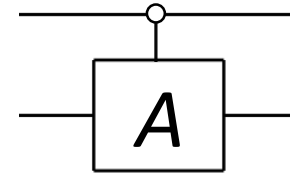
$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a_{00} & 0 & a_{10} \\ 0 & 0 & 1 & 0 \\ 0 & a_{01} & 0 & a_{11} \end{pmatrix}$$



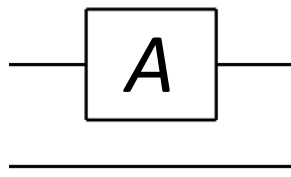
$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a_{00} & a_{01} \\ 0 & 0 & a_{10} & a_{11} \end{pmatrix}$$



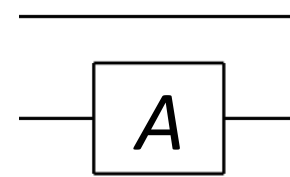
$$A = \begin{pmatrix} a_{00} & 0 & a_{10} & 0 \\ 0 & 1 & 0 & 0 \\ a_{01} & 0 & a_{11} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



$$A = \begin{pmatrix} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



$$A = \begin{pmatrix} a_{00} & 0 & a_{01} & 0 \\ 0 & a_{00} & 0 & a_{01} \\ a_{10} & 0 & a_{11} & 0 \\ 0 & a_{10} & 0 & a_{11} \end{pmatrix}$$



$$A = \begin{pmatrix} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & a_{00} & a_{01} \\ 0 & 0 & a_{10} & a_{11} \end{pmatrix}$$

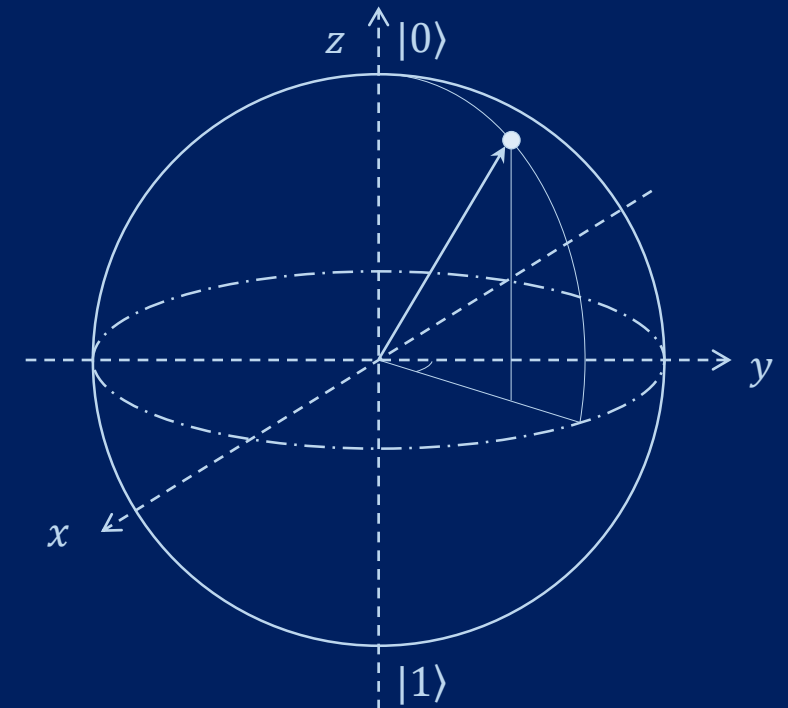
La representación de cada operación implica una matriz de tamaño 2^n .

2 Computación Cuántica discreta

Descripción del modelo

Conjunto de puertas considerado

Algoritmo de generalización de puertas de 1 qubit



Computación Cuántica discreta

Descripción del modelo

Los estados cuánticos contemplados por el modelo son de la siguiente forma:

$$|\psi\rangle = \frac{1}{\sqrt{2}^k} \cdot (x_0 + iy_0, x_1 + iy_1, \dots, x_{2^n-1} + iy_{2^n-1}), \text{ donde:}$$

- a) $k \in \mathbb{N}$ (nivel)
- b) $x_0^2 + x_1^2 + \dots + x_{2^n-1}^2 + y_0^2 + y_1^2 + \dots + y_{2^n-1}^2 = 2^k$
- c) $x_d, y_d \in \mathbb{Z}$ para todo $0 \leq d < 2^n$ (enteros de Gauss)
- a) $2 \nmid \text{mcd}(x_0, x_1, \dots, x_{2^n-1}, y_0, y_1, \dots, y_{2^n-1})$

Computación Cuántica discreta

Conjunto de puertas considerado

Se consideran conjuntos universales de puertas cuánticas a aquellos cuyas puertas permiten generar, de forma exacta o aproximada, a todas las demás. El considerado en el modelo es el siguiente:

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

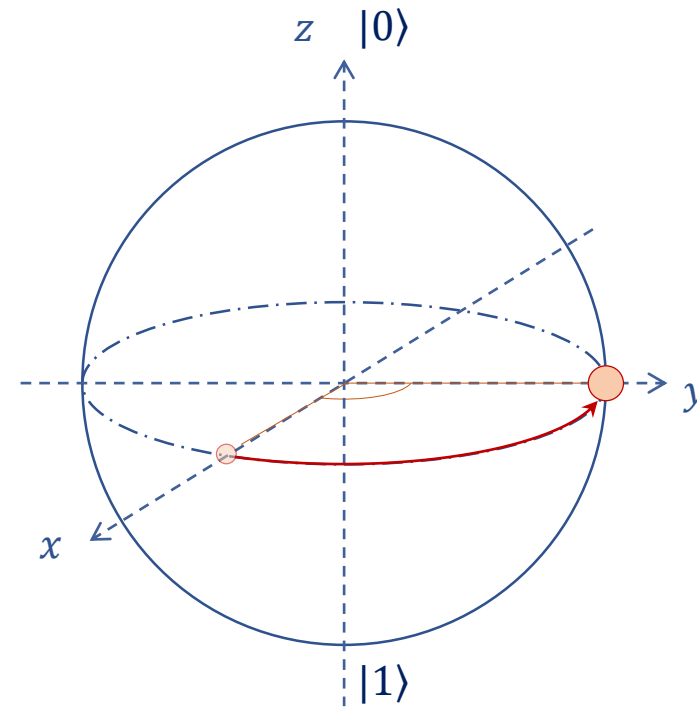
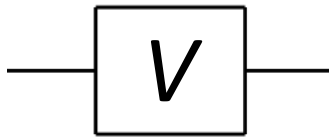
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & i \end{pmatrix} = \begin{pmatrix} I_6 & V \end{pmatrix}$$

Computación Cuántica discreta

Conjunto de puertas considerado – Puerta V

La puerta V añade una fase relativa i al estado $|1\rangle$, dejando el estado $|0\rangle$ inalterado. Equivale a una rotación de $\pi/2$ alrededor del eje Z.

$$V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

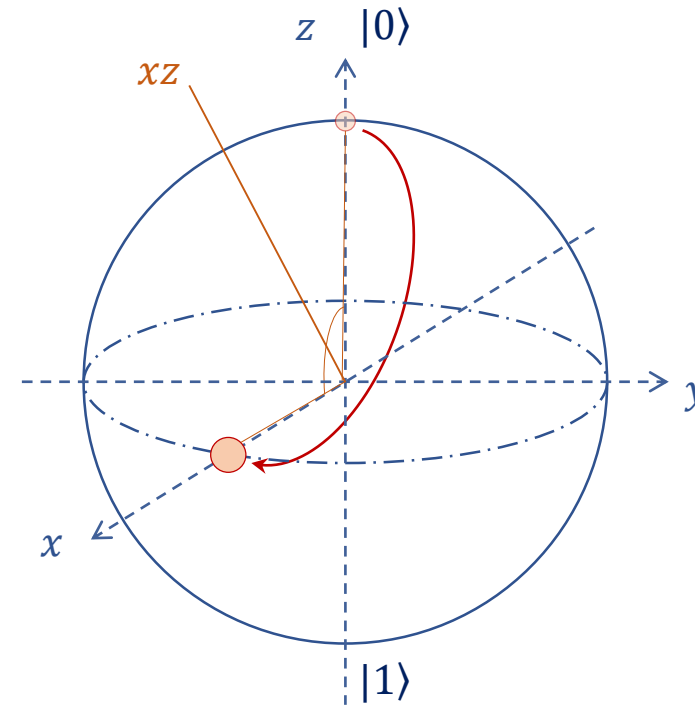
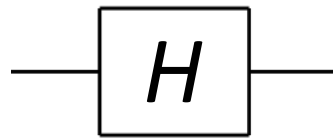


Computación Cuántica discreta

Conjunto de puertas considerado – Puerta de Hadamard

La puerta de Hadamard es usada principalmente para generar superposiciones a partir de los estados de la base computacional: mapea el estado $|0\rangle$ a $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, y el $|1\rangle$ a $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Equivale a una rotación de π alrededor del eje XZ.

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

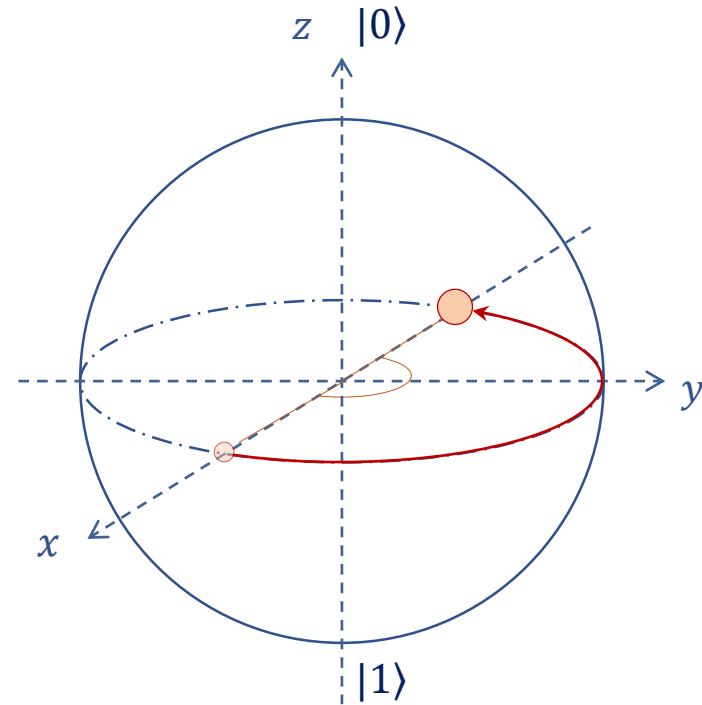
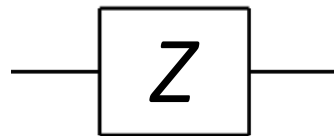


Computación Cuántica discreta

Conjunto de puertas considerado – Puerta Z

La puerta Z mapea el estado $|1\rangle$ al $-|1\rangle$, dejando $|0\rangle$ inalterado. Equivale a una rotación de π alrededor del eje Z.

$$Z = V^2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

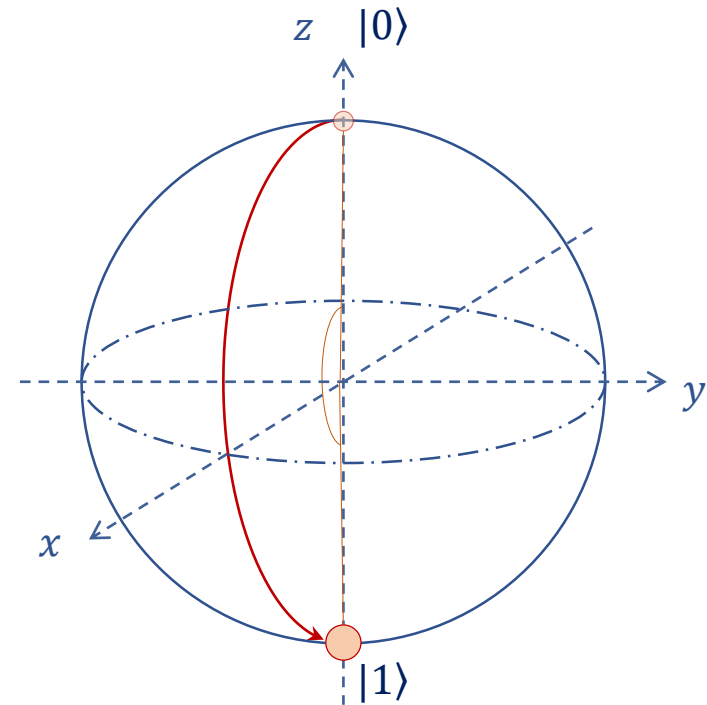
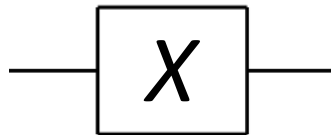


Computación Cuántica discreta

Conjunto de puertas considerado – Puerta X

La puerta X representa una negación: mapea el estado $|0\rangle$ al $|1\rangle$, y el estado $|1\rangle$ al $|0\rangle$. Equivale a una rotación de π alrededor del eje Y.

$$X = HZH = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



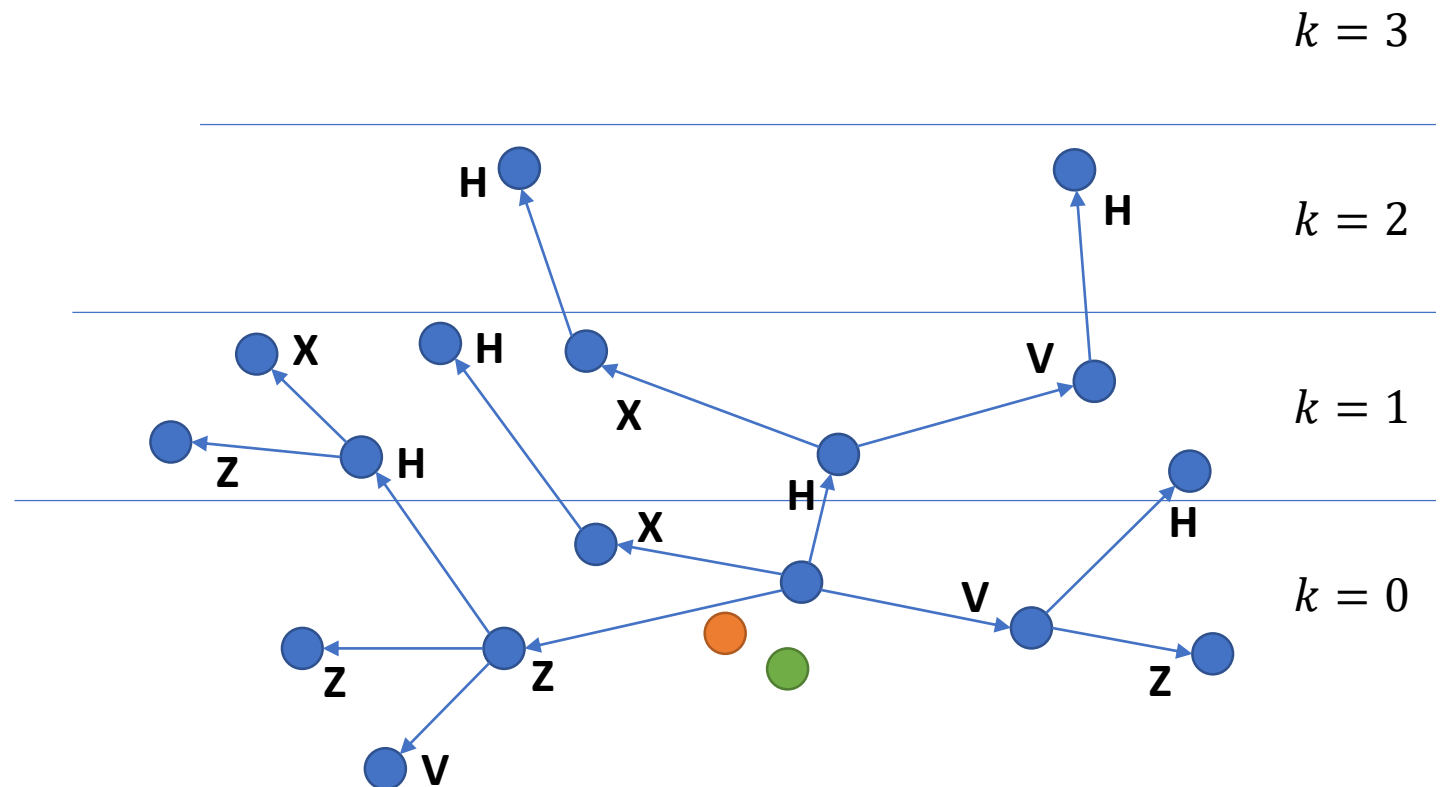
Computación Cuántica discreta

Conjunto de puertas considerado

De las cuatro puertas consideradas, la puerta H es la única que altera el parámetro k de un estado cuántico, por su factor de normalización $1/\sqrt{2}$.

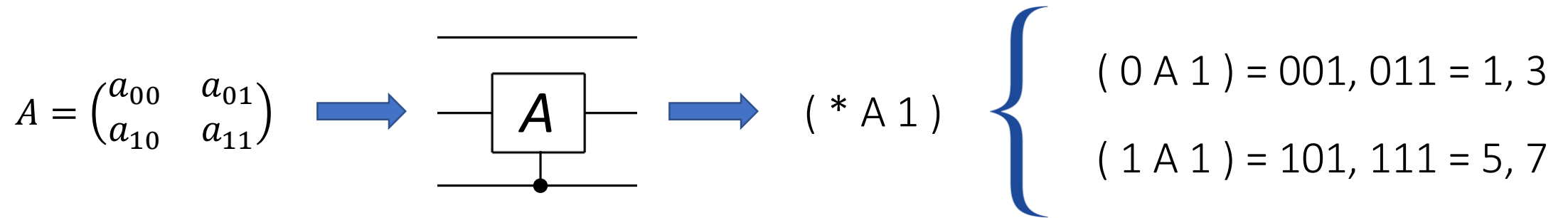
Aplicación de una puerta
 $|\psi'\rangle = A \cdot |\psi\rangle$


Si $A = H \rightarrow k' = k \pm 1$
Si $A \in \{V, Z, X\} \rightarrow k' = k$



Computación Cuántica discreta

Algoritmo de generalización de puertas de 1 qubit



$\begin{matrix} 1, 3 \\ 5, 7 \end{matrix}$

 $A' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_{00} & 0 & a_{01} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_{10} & 0 & a_{11} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & a_{00} & 0 & a_{01} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & a_{10} & 0 & a_{11} \end{pmatrix}$

Computación Cuántica discreta

Algoritmo de generalización de puertas de 1 qubit

1. Inicializar una lista de secuencias $s = \{S\}$, siendo S la cadena de caracteres que representa la operación a realizar. Los qubits sin uso se representarán por un asterisco.
2. Elegir una secuencia S_i de la lista s que contenga al menos un asterisco, y reemplazarlo con un control a 0 para generar S_{i0} , y por otro lado por un 1 para generar S_{i1} . Añadir ambas secuencias a la lista inicial y retirar la que se usó para generarlas. Repetir este paso en cada secuencia de s , hasta que todas representen la aplicación de una puerta completamente controlada.
3. Identificar los dos decimales $p_i = (d_{i0}, d_{i1})$ que son representados por cada S_i en notación binaria, considerando que d_{i0} sustituye la puerta por un 0, y d_{i1} sustituye la puerta por un 1.
4. Construir A' como I_{2^n} y, para cada par $p_i = (d_{i0}, d_{i1})$ obtenido de S_i , fijar:

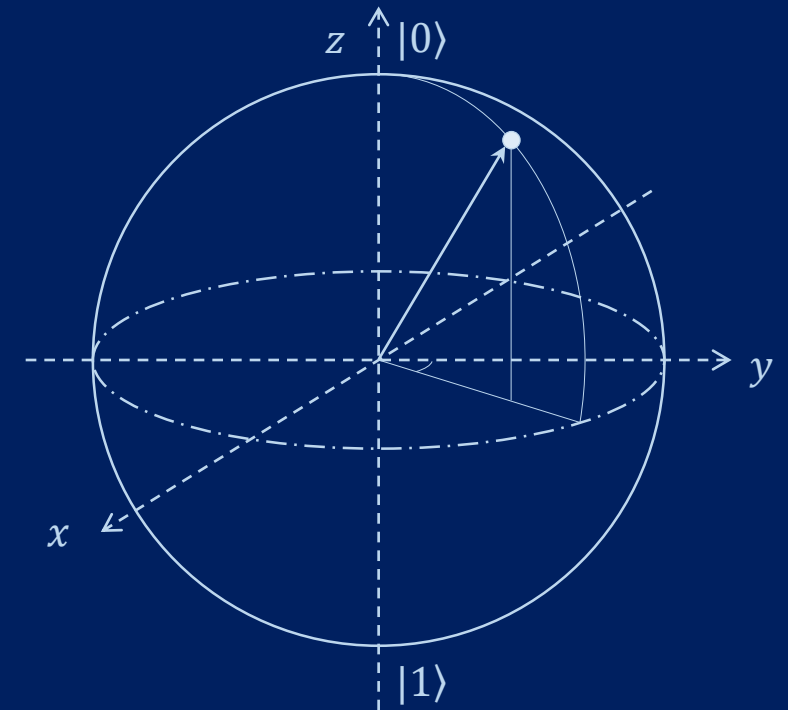
$$\begin{aligned} a_{00} &\text{ en } a'_{d_{i0}d_{i0}}, \\ a_{01} &\text{ en } a'_{d_{i0}d_{i1}}, \\ a_{10} &\text{ en } a'_{d_{i1}d_{i0}}, \text{ y} \\ a_{11} &\text{ en } a'_{d_{i1}d_{i1}}. \end{aligned}$$

3 Complejidad de estados cuánticos

Concepto de complejidad

Algoritmo de generación del árbol de estados

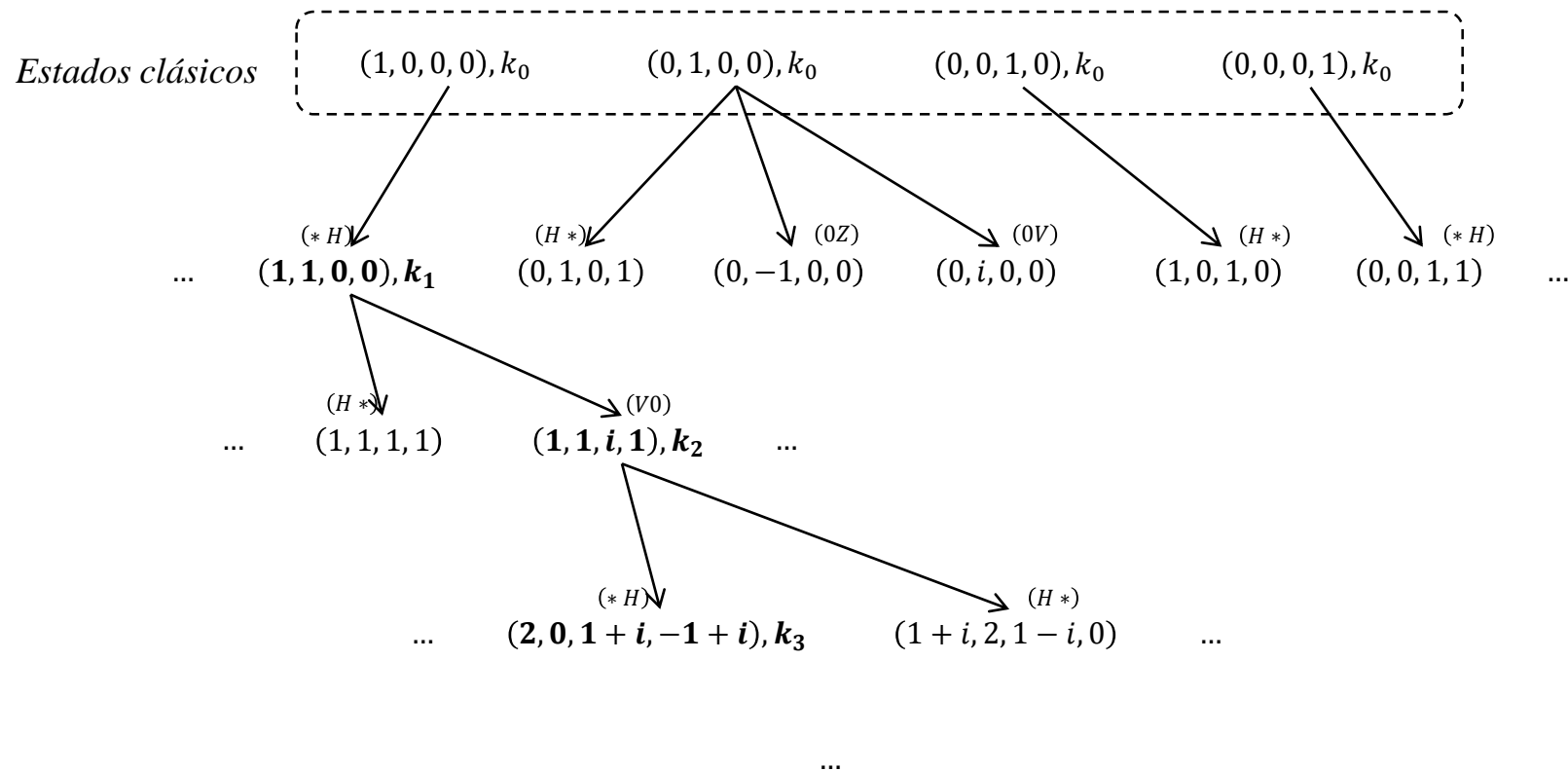
Conjeturas



Complejidad de estados cuánticos

Concepto de complejidad

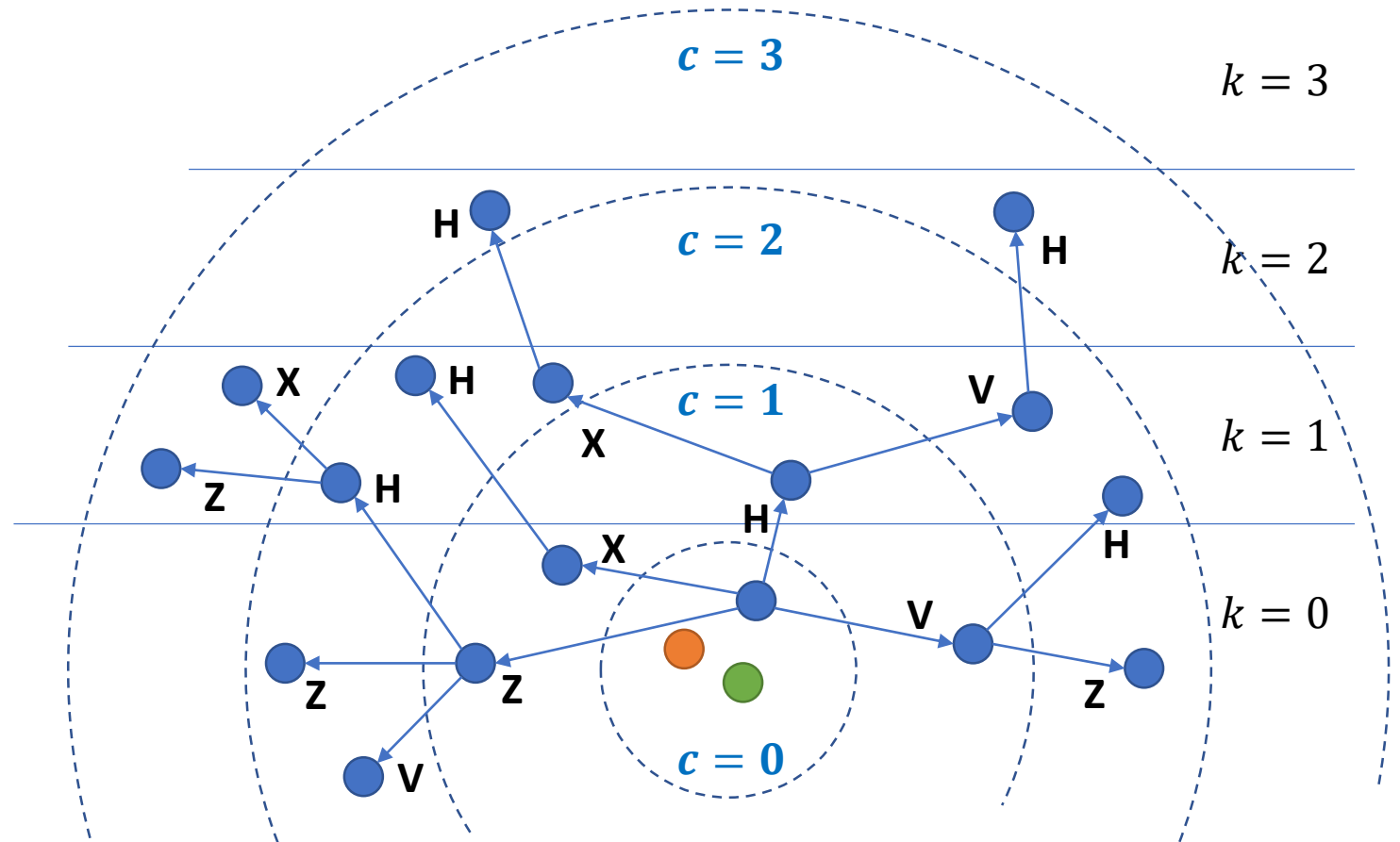
Si consideramos los estados de la base computacional como aquellos con complejidad 0, la aplicación de una puerta para alcanzar un estado distinto incrementa la complejidad de dicho estado en uno.



Complejidad de estados cuánticos

Algoritmo de generación del árbol de estados

Las puertas V, Z y X deben ser las primeras en ser aplicadas, para completar el rastreo de un nivel k antes de usar la puerta de Hadamard y cambiar a un nivel siguiente.



Complejidad de estados cuánticos

Algoritmo de generación del árbol de estados

1. Seleccionar una longitud n de qubits, y formar F_0 como el conjunto que contiene los 2^n estados de la base computacional, con complejidad $c = 0$.
2. Formar el conjunto Q como $Q = F_0$ al inicio. Este conjunto siempre contendrá los estados que aún deben ser considerados, en los pasos siguientes del algoritmo.
3. Formar el conjunto A como el que contiene el conjunto de puertas a aplicar: $A = \{V, Z, X, H\}$. Construir el conjunto A' como el formado por todas las posibles operaciones en las que se aplica una vez alguna puerta de A a alguno de los qubits disponibles, usando algunos, ninguno y todos los controles asociados posibles.
4. Para cada estado cuántico de Q , identificar el conjunto F_c en que el estado está contenido, obtener todos los posibles estados alcanzables con A' , y añadir los resultantes a F_{c+1} . Descartar todos aquellos estados que ya figurasen en cualquiera de los conjuntos de F_0 a F_{c+1} , para evitar duplicados.

Complejidad de estados cuánticos

Algoritmo de generación del árbol de estados

Cadenas de n -qubits con longitud $n = 1$.

		Nivel k										Total			
		0	1	2	3	4	5	6	7	8	9		10		
Complejidad – Puertas	0	2													2
	1	2	2												4
	2	3	4												7
	3	1	6	2											9
	4		4	5											9
	5		2	6											8
	6		3	3											6
	7		3												3
Total		8	24	16										48	

Datos pendientes de confirmación

Complejidad de estados cuánticos

Algoritmo de generación del árbol de estados

Cadenas de n-qubits con longitud $n = 2$.

		Nivel k											Total											
		0	1	2	3	4	5	6	7	8	9	10												
Complejidad – Puertas	0	4															4							
	1	4	8														12							
	2	5	29	4													38							
	3	1	42	47													90							
	4		17	150	36												203							
	5			11	130	275	12										428							
	6				4	117	456	179									756							
	7					1	411	372	743								1.527							
	8							241	1.668	973							2.882							
	9								20	3.819	1.391						5.230							
	10										2.271	7.353	526				10.150							
	11											318	11.211	8.156	108		19.793							
	12												1	4.887	29.326	3.025	37.239							
	13														20.714	24.868	24.331	69.913						
	14															23.759	43.971	69.616	137.346					
	15																2.506	200.300	53.908	256.714				
	16																		215.723	249.823	6.812	472.358		
	17																				51.752	277.380	28.846	108
Total		14	112	1.120	9.216	73.728	574.622	678.191	35.658	108														1.372.769

Datos pendientes de confirmación

Complejidad de estados cuánticos

Algoritmo de generación del árbol de estados

Cadenas de n -qubits con longitud $n = 3$.

		Nivel k										Total		
		0	1	2	3	4	5	6	7	8	9		10	
Complejidad – Puertas	0	8												8
	1	20	24											44
	2	9	114	24										147
	3	1	191	417	8									617
	4		104	2.378	687									3.169
	5		41	6.496	9.736	518								16.791
	6		5	7.774	60.926	18.648	252							87.605
	7		1	6.240	217.679	238.959	16.673	56						479.608
	8			2.439	188.741	407.780	78.751	988						678.699
	9													
Total		38	480	25.768	477.777	665.905	95.676	1.044						1.266.688

Datos pendientes de confirmación

Complejidad de estados cuánticos

Algoritmo de generación del árbol de estados

Cadenas de n-qubits con longitud $n = 3$.

		Nivel k										Total		
		0	1	2	3	4	5	6	7	8	9		10	
Complejidad – Puertas	0	16												16
	1	44	64											108
	2	17	360	96										473
	3	1	712	2.202	64									2.979
	4		559	18.560	6.140	16								25.275
	5		255	81.779	144.282	8.476								234.792
	6		33	181.728	1.831.864	486.316	6.744							2.506.685
	7		1	49.887	1.646.018	1.043.031	56.075	242						2.795.254
	8													
	9													
	10													
	11													
Total		78	1.984	334.252	3.628.368	1.537.839	62.819	242					5.565.582	

Datos pendientes de confirmación

Complejidad de estados cuánticos

Conjeturas

Conjetura 1: En cada rama del árbol, el nivel k es monótonamente no decreciente.

Conjetura 2: La complejidad mínima de cada nivel k crece linealmente cuando $n \rightarrow \infty$. Idealmente, la puerta de Hadamard siempre puede aplicarse de alguna forma que permite aumentar el parámetro k .

Conjetura 3: La complejidad máxima de cada nivel k crece de forma exponencial.

Datos pendientes de confirmación

rafael.martincuevas@accenture.com

L. N. Gatti, J. Lacalle. A model of discrete quantum computing, Quantum Information Processing (submitted).

<http://innovis.cpsc.ucalgary.ca/Research/PhylloTrees>

<http://inspirehep.net/record/1251940/plots>

