Universidad de La Laguna

Cúbits y Puertas Cuánticas

Microcredencial en Introducción a la Computación Cuántica

Daniel Escanez-Exposito

Jorge Garcia-Diaz

Escuela Superior de Ingeniería y Tecnología
Grupo de Investigación en Criptología - CryptULL

La Laguna, 2025

Universidad de La Laguna

Cúbits y Puertas Cuánticas

Microcredencial en Introducción a la Computación Cuántica

Daniel Escanez-Exposito
Correo electrónico - jescanez@ull.edu.es

Jorge Garcia-Diaz
Correo electrónico - jgarcidi@ull.edu.es

Escuela Superior de Ingeniería y Tecnología
Grupo de Investigación en Criptología - CryptULL

Microcredencial en Introducción a la Computación Cuántica

La Laguna, 2025

Índice general

1. Cúbits y Puertas Cuánticas **1**
1.1. Computación clásica 1
1.1.1. Representación de la información 2
1.1.2. Operadores 3
1.2. Computación cuántica 4
1.2.1. Representación de la información 4
1.2.2. Operadores 9

1

Cúbits y Puertas Cuánticas

La computación cuántica es un punto de intersección entre la informática, las matemáticas y la física, que utiliza las leyes fundamentales la escala atómica para la realización de cálculos automáticos. El uso de este enfoque es realmente beneficioso, ya que cuenta con un paralelismo intrínseco no presente en la computación clásica. Esto permite alcanzar las soluciones a determinados problemas en menos tiempo, logrando algunas veces ventajas exponenciales. El modelo matemático que conforma la computación cuántica es sólido y comprende una elegante extensión de la computación clásica. A continuación, se realizará la exposición de las unidades de información y sus operaciones, dentro de los paradigmas clásico y cuántico.

1.1. Computación clásica

La computación clásica es el modelo tradicional de procesamiento de información que opera mediante estados discretos y bien definidos. Este enfoque, base del funcionamiento de los ordenadores actuales, realiza cálculos a través de componentes electrónicos que ejecutan operaciones de manera secuencial (una tras otra) o, en algunos casos, de forma paralela (es decir, dividiendo una tarea en varias que se resuelven simultáneamente mediante múltiples unidades de procesamiento). Sin embargo, este paralelismo clásico está limitado por la división de problemas en pasos lógicos y deterministas. La computación clásica, aun siendo la adecuada para una amplia gama de aplicaciones cotidianas, enfrenta dificultades en la resolución de ciertos problemas especialmente complejos. Entre los problemas más relevantes (que sin ser los más complejos en términos absolutos, sí representan desafíos significativos) destacan tareas como la factorización de números enteros (que tienen un gran interés desde el punto de vista de la criptografía) o la simulación de moléculas y reacciones químicas.

1.1.1. Representación de la información

La unidad mínima de información en el esquema clásico es el bit, ***bi**nary digi**t*** (dígito binario, en inglés). Este conforma un sistema que puede estar únicamente en dos estados bien diferenciados, usualmente representados como 0 y 1. De esta manera, se pueden representar multitud de sistemas que responden a la lógica binaria; es decir, que pueden estar en una de dos posibilidades.

> **Nota**
>
> Algunos ejemplos de sistemas binarios son:
>
> - Una moneda: que puede estar de cara o de cruz.
> - Una luz: que puede estar encendida o apagada.
> - Una puerta: que puede estar abierta o cerrada.
> - Un candado: que puede estar bloqueado o desbloqueado.

Estos bits pueden ser organizados en secuencias, conformando registros. Un registro de N bits representa 1 de 2^N valores posibles de ese sistema.

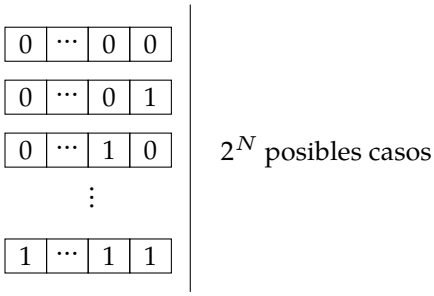

Figura 1.1: *Visualización de los valores posibles para un registro de N bits*

Para cada una de estas posibilidades, se puede establecer un significado concreto, estableciendo una codificación. Usualmente, si se carece de este significado, al trabajar con secuencias binarias se puede hacer alusión a los números decimales que representan.

> **1.1 Ejercicio**
>
> Definir un código de $N = 2$ bits para representar las 4 estaciones. A continuación, establecer otro código de $N = 3$ bits para los 8 planetas del sistema solar. ¿Es posible representar los 8 planetas con un registro de 2 bits? ¿Y representar las 4 estaciones con 3 bits? Justificar las respuestas.

1.1.2. Operadores

Una vez dispuesta la representación de la información, es de gran interés poder transformarla. La computación modifica la entrada de un problema para alcanzar su solución de manera automática, por medio de la ejecución de una secuencia finita de operaciones. A este procedimiento se le denomina algoritmo. Una forma de describir las modificaciones de los bits en computación clásica es mediante el uso de puertas lógicas. Estas operaciones elementales pueden ser definidas mediante una tabla de verdad, que indica para cada valor posible de la entrada, la salida de esa operación. Por tanto, para registros de N bits de entrada y M bits de salida, es decir puertas $(N : M)$, sus tablas de verdad tienen 2^N filas, y las salidas pueden tomar valores enteros entre 0 y $2^M - 1$.

Nota

Existen 4 puertas que reciben un único bit de entrada y devuelven un único bit de salida: identidad (ID), que devuelve la entrada sin transformarla; negación (NOT), que invierte el bit de la entrada; desactivación (RESET), que devuelve siempre 0; y activación (SET), que devuelve siempre 1.

a	ID
0	0
1	1

a	NOT
0	1
1	0

a	RESET
0	0
1	0

a	SET
0	1
1	1

Otras puertas bien conocidas que reciben dos bits de entrada (a, b) y devuelven un único bit de salida son: suma (OR), multiplicación (AND), y suma exclusiva (XOR). Nótese que OR contempla $1 + 1 = 1$ y XOR $1 \oplus 1 = 0$.

a	b	AND
0	0	0
0	1	0
1	0	0
1	1	1

a	b	OR
0	0	0
0	1	1
1	0	1
1	1	1

a	b	XOR
0	0	0
0	1	1
1	0	1
1	1	0

1.2 Ejercicio

Escribir la tabla de verdad de una puerta con 3 bits de entrada (a, b, c) y 2 bits de salida (d, e), donde $d = a$ AND b y $e =$ NOT c.

En el paradigma clásico, la información puede ser consultada sin generar cambios en la misma. Un bit de información puede ser escrito, transformado, copiado y leído de

manera determinista. Sin embargo, en el esquema cuántico se afrontan algunas complejas dificultades para realizar estas tareas, debido a las imposiciones de la mecánica cuántica. En la siguiente sección se expondrán las diferencias principales y cómo se abordan estas aparentes desventajas para lograr, en algunos aspectos, una mejora exponencial en el coste computacional.

1.2. Computación cuántica

1.2.1. Representación de la información

La unidad mínima en computación cuántica es el cúbit (en inglés, *qubit* de *quantum bit*). Un cúbit puede encontrarse en uno de los estados básicos $|0\rangle$ y $|1\rangle$ o, por el contrario, en una superposición de los mismos. De manera general, se define como

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle , \tag{1.1}$$

donde $\alpha_0, \alpha_1 \in \mathbb{C}$ y $\|\alpha_0\|^2 + \|\alpha_1\|^2 = 1$.

Esta mezcla de estados se mantendrá hasta que se deseé leer la información contenida en ese cúbit. Entonces, se procederá a observar o medir el estado, colapsando en un bit clásico y eliminando los coeficientes complejos involucrados. Son precisamente estos escalares los que determinan la probabilidad de obtener como resultado el estado al que acompañan. La probabilidad de observar el cúbit de la Ec. (1.1) en estado $|0\rangle$ es $\|\alpha_0\|^2$ y la probabilidad de observarlo en estado $|1\rangle$ es $\|\alpha_1\|^2$. De esta manera queda justificada la imposición anterior en la que la suma de estas dos cantidades debe dar uno.

La forma de representar los estados básicos como $|0\rangle$ y $|1\rangle$ es conocida como la notación ket o notación de Dirac, ampliamente utilizada en mecánica cuántica. Cada uno de estos estados corresponde con un elemento de la base canónica de $\mathbb{C}^2$, siendo

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{y} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.2}$$

Por tanto, un cúbit puede representarse vectorialmente como:

$$\alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}, \tag{1.3}$$

donde $\alpha_0, \alpha_1 \in \mathbb{C}$ y $\|\alpha_0\|^2 + \|\alpha_1\|^2 = 1$. A este vector también se le suele denominar vector de estado y en algunas ocasiones, por economía del lenguaje, simplemente estado.

Además, los sistemas cuánticos no están limitados a un solo cúbit. Por ejemplo, un registro de 2 cúbits puede ser descrito como:

$$\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle , \tag{1.4}$$

con $\alpha_i \in \mathbb{C}, \forall i \in \{0,1,2,3\}$ y $\sum_{i\in\{0,1,2,3\}} \|\alpha_i\|^2 = 1$. También se pueden representar de manera vectorial, bajo las mismas consideraciones para los coeficientes:

$$\alpha_0 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \alpha_3 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{1.5}$$

Se puede observar que cada α_i acompaña a su correspondiente estado $|i\rangle$, que es igual al vector de la base que tiene un cero en todas las posiciones excepto en la posición i. Se da la particularidad de que esta propiedad se cumple debido a la construcción de estos vectores mediante el producto tensorial de sus componentes.

Nota

El producto tensorial o producto de Kronecker entre dos cúbits $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ y $\begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}$ se define de la siguiente manera:

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \\ \alpha_1 \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} \tag{1.6}$$

Por ejemplo, el estado $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ viene definido por el producto tensorial:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{1.7}$$

1.3 Ejercicio

Comprobar que la construcción de la Ec. (1.7) se cumple para el resto de estados básicos de 2 cúbits: $|01\rangle, |10\rangle, |11\rangle$.

Por consiguiente, es posible definir como estado producto de N cúbits a aquel que puede ser expresado como producto $(\otimes)$ de N estados de un cúbit. A continuación, se expone el desarrollo del producto tensorial con la notación ket:

$$\begin{aligned}\begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix}\otimes\begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix} &= (\alpha_0|0\rangle+\alpha_1|1\rangle)\otimes(\beta_0|0\rangle+\beta_1|1\rangle)\\ &= \alpha_0\beta_0|00\rangle+\alpha_0\beta_1|01\rangle+\alpha_1\beta_0|10\rangle+\alpha_1\beta_1|11\rangle\,.\end{aligned} \tag{1.8}$$

1.4 Ejercicio

Demostrar que el estado $\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle$ no puede ser expresado como producto ($\otimes$) de dos estados de un cúbit.

Sin embargo, no siempre es posible expresar un estado cuántico como producto de estados. Existen sistemas cuánticos cuyas componentes se encuentran correlacionadas; es decir, el valor de una componente determina el de la otra. Por ejemplo, un registro de dos cúbits, un estado en entrelazamiento sería aquel que no pudiera ser expresado como producto de dos estados de un cúbit. Por ello, si estos se encuentran en un estado de superposición, esta no sería independiente, y al medir uno de ellos provocaría un cambio en el otro.

Nota

Algunos estados particulares de un cúbit son:

$$|+\rangle=\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle \qquad |-\rangle=\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle$$

También son relevantes estos estados entrelazados de dos cúbits, llamados pares EPR o pares de Bell:

$$|\Phi^+\rangle=\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle \qquad |\Psi^+\rangle=\frac{1}{\sqrt{2}}|01\rangle+\frac{1}{\sqrt{2}}|10\rangle$$

$$|\Phi^-\rangle=\frac{1}{\sqrt{2}}|00\rangle-\frac{1}{\sqrt{2}}|11\rangle \qquad |\Psi^-\rangle=\frac{1}{\sqrt{2}}|01\rangle-\frac{1}{\sqrt{2}}|10\rangle$$

Consejo

Por facilidad de lectura, en ocasiones puede expresarse el producto tensorial entre dos vectores de la siguiente manera:

$$|a\rangle\otimes|b\rangle=|a\rangle|b\rangle=|ab\rangle$$

Esfera de Bloch

Una de las representaciones gráficas más recurrentes en computación cuántica es la interpretación geométrica de un cúbit por medio de la esfera de Bloch. Esta idea intenta simplificar los dos coeficientes complejos de un cúbit, para lograr representar la información útil (en términos de computación cuántica) dentro de un espacio tridimensional. Para cada posible estado de un cúbit, existe un único punto en la superficie de la esfera que lo representa. A continuación, se expone el desarrollo de esta transformación.

Dado el estado de un cúbit arbitrario $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ (con $\alpha_0, \alpha_1 \in \mathbb{C}$ y $\|\alpha_0\|^2 + \|\alpha_1\|^2 = 1$), es posible expresar sus coeficientes, mediante sus formas exponenciales (es decir $\alpha = re^{i\delta}$, siendo $r \geq 0$ su módulo, $\delta \in [0, 2\pi)$ su fase, e i la unidad imaginaria):

$$|\psi\rangle = r_0 e^{i\gamma} |0\rangle + r_1 e^{i\phi} |1\rangle . \tag{1.9}$$

Al ser el estado de un cúbit se tiene que $\|\alpha_0\|^2 + \|\alpha_1\|^2 = 1$, y por ello:

$$\|r_0 e^{i\gamma}\|^2 + \|r_1 e^{i\phi}\|^2 = r_0^2 + r_1^2 = 1. \tag{1.10}$$

Nota

Como $r_0 \geq 0$ y $r_1 \geq 0$ y $r_0^2 + r_1^2 = 1$ se puede encontrar un único $\theta \in [0, \pi)$ tal que:

$$r_0 = \cos\left(\frac{\theta}{2}\right) \quad \wedge \quad r_1 = \sin\left(\frac{\theta}{2}\right)$$

1.5 Ejercicio

Expresar los siguientes pares de módulos en función de sin y cos con respecto a θ, calculando el valor de esta:

- $r_0 = 0 \wedge r_1 = 1$
- $r_0 = 1 \wedge r_1 = 0$
- $r_0 = \frac{1}{2} \wedge r_1 = \frac{1}{2}$
- $r_0 = \frac{\sqrt{3}+1}{2\sqrt{2}} \wedge r_1 = \frac{\sqrt{3}-1}{2\sqrt{2}}$

Reescribiendo la Ecuación 1.9 con los módulos en su forma sinusoidal y definiendo $\varphi = \phi - \gamma \in [0, 2\pi)$, se obtiene:

$$\begin{aligned} |\psi\rangle &= e^{i\gamma} \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right) |1\rangle \\ &= e^{i\gamma} \left(\cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right) |1\rangle \right), \end{aligned} \tag{1.11}$$

donde $\theta, \varphi, \gamma \in \mathbb{R}$. Como $\|e^{i\gamma}\| = 1$, este término (que recibe el nombre de fase global) no tiene ningún efecto físico observable, no tiene efecto en la medición independientemente de la base escogida. Por ello es equivalente expresar (en términos de probabilidades observables):

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle\,. \tag{1.12}$$

Las coordenadas esféricas, los valores reales φ (que controla su fase relativa, que si es importante en términos de medición) y θ (que controla su amplitud), definen un único punto en la esfera unidad tridimensional:

$$\begin{cases} x = \sin\theta\cos\varphi \\ y = \sin\theta\sin\varphi \\ z = \cos\theta \end{cases} \tag{1.13}$$

Por tanto, el punto $(\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ representa un único punto en la superficie de la esfera unidad, las coordenadas en la esfera de Bloch. Esto se puede observar en la Figura 1.2.

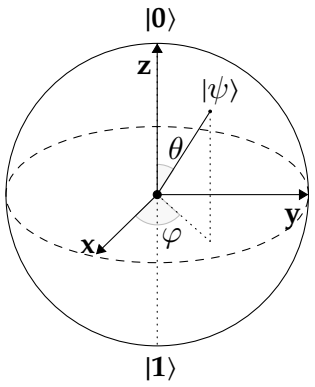

Figura 1.2: *Representación de un cúbit en la esfera de Bloch.*

Nota

Por ejemplo, para el estado $|0\rangle$:

1. Calcular módulos: Dados $\alpha_0 = 1$ y $\alpha_1 = 0$, se calculan $r_0 = 1$ y $r_1 = 0$.
2. Calcular θ: Se tiene que $r_0 = \cos\left(\frac{\theta}{2}\right)$, por lo que $\theta = 2\arccos(1) = 0$. También se puede calcular a partir de $r_1 = \sin\left(\frac{\theta}{2}\right)$, y por tanto $\theta = 2\arcsin(0) = 0$.
3. Calcular φ: Dados $\gamma = 0$ y $\phi = 0$, se tiene que $\varphi = \phi - \gamma = 0$.
4. Calcular coordenadas esféricas: A partir de los senos y cosenos de θ y φ, se establece el punto $(0, 0, 1)$ que coincide con el polo norte de la esfera de Bloch.

1.6 Ejercicio

Para cada uno de los estados $|1\rangle$, $|+\rangle$, $|-\rangle$:

- Calcular θ y φ.
- Calcular sus coordenadas en la esfera de Bloch.
- Dibujar su vector de estado en la esfera de Bloch.

1.2.2. Operadores

De manera análoga a las puertas del paradigma clásico, se definen las puertas cuánticas. Estas son las operaciones que permiten transformar los estados de los cúbits, y se representan usualmente como matrices unitarias que definen su comportamiento para cada estado básico del sistema. Son siempre de $(N : N)$; es decir, si reciben N cúbits de entrada, devuelven N cúbits de salida. Por ello, son matrices de $2^N \times 2^N$ elementos complejos. La unitariedad de las matrices garantiza la linealidad y reversibilidad de las operaciones realizadas, que son condiciones impuestas por las leyes de la mecánica cuántica.

Puertas de un sólo cúbit

Un ejemplo sencillo de operación cuántica es la puerta X, análoga al NOT clásico. Esta transforma el estado $|0\rangle$ en el estado $|1\rangle$ y viceversa. Su aplicación sobre un cúbit genérico puede representarse, en notación ket, como:

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle \xrightarrow{X} \alpha_1 |0\rangle + \alpha_0 |1\rangle , \tag{1.14}$$

y matricialmente como:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{1.15}$$

Consejo

Resulta muy útil visualizar las columnas de las matrices como los estados resultantes tras aplicar una trasformación para cada estado básico del sistema.
Por ejemplo, en el caso de la puerta X, se puede observar como la primera columna (aquella que equivale al resultado de la operación sobre el estado $|0\rangle$) corresponde con el vector $|1\rangle$ y la segunda columna (aquella que equivale al resultado de la operación sobre el estado $|1\rangle$) corresponde con el vector $|0\rangle$.

$$\begin{array}{rc} \text{Entrada:} & \begin{matrix} |0\rangle & |1\rangle \\ \downarrow & \downarrow \end{matrix} \\ X = & \begin{pmatrix} \boxed{0} & \boxed{1} \\ 1 & 0 \end{pmatrix} \\ \text{Salida:} & \begin{matrix} \downarrow & \downarrow \\ |1\rangle & |0\rangle \end{matrix} \end{array}$$

Nota

Algunas puertas particulares de un cúbit son:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

1.7 Ejercicio

Definir el efecto de la puerta H sobre un cúbit en estado básico.

1.8 Ejercicio

Identificar la puerta resultado de la expresión: $\frac{1}{\sqrt{2}}(X + Z)$.

1.9 Ejercicio

Definir en notación ket el efecto de las puertas I, Y, Z y H sobre un cúbit en estado de superposición.

Puertas de varios cúbits

Además, existen puertas de más de un cúbit, necesarias para lograr el entrelazamiento, entre otros motivos. Una operación cuántica muy común para lograr este fin es el NOT controlado, CNOT (del inglés, *Controlled-NOT*) o CX (del inglés, *Controlled-X*). Este operador utiliza dos cúbits, uno que cumple el papel de control y otro de objetivo. La puerta aplica la negación del objetivo, para aquellos casos en los que el control tenga el valor $|1\rangle$, dejando el objetivo intacto cuando el control es $|0\rangle$. La expresión de la aplicación de esta puerta sobre dos cúbits, uno de control c (del inglés, *control*) y otro de objetivo t (del inglés, *target*), puede describirse como:

$$CX\ |c\ \ t\rangle = |c\ \ t \oplus c\rangle\,, \tag{1.16}$$

o mediante la Tabla 1.1, que refleja el comportamiento de la puerta para todos los estados básicos de dos cúbits.

Tabla 1.1: *Funcionamiento de la puerta CX sobre los estados básicos de un sistema de 2 cúbits*

c_{in}	t_{in}	c_{out}	t_{out}
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

A continuación se expresa la matriz para describir esta operación:

$$CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.17}$$

Consejo

Aplicando el consejo anterior, se puede visualizar el trabajo realizado por esta puerta que, para los vectores $|00\rangle$ y $|01\rangle$, no modifica nada, ya que el primer cúbit (control) está a cero. Sin embargo, para los vectores $|10\rangle$ y $|11\rangle$, niega el segundo cúbit (objetivo).

$$\begin{array}{rc} \text{Entrada:} & \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \\ \downarrow & \downarrow & \downarrow & \downarrow \end{array} \\ CX = & \begin{pmatrix} \boxed{1} & \boxed{0} & \boxed{0} & \boxed{0} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ \text{Salida:} & \begin{array}{cccc} \downarrow & \downarrow & \downarrow & \downarrow \\ |00\rangle & |01\rangle & |11\rangle & |10\rangle \end{array} \end{array}$$

1.10 Ejercicio

Identificar el estado bien conocido que resulta del siguiente desarrollo, utilizando la notación ket:

$$CX\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle\right)$$

1.11 Ejercicio

Identificar el estado bien conocido que resulta del siguiente desarrollo, utilizando la notación matricial:

$$CX\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$$

1.12 Ejercicio

Definir la matriz para el operador CX', que utiliza como objetivo el primer cúbit y como control el segundo:

$$CX'\ |t\ \ c\rangle = |t \oplus c\ \ c\rangle$$

De manera general, se puede considerar la versión controlada una puerta unitaria

U como CU. En el caso de ser U una puerta de un solo cúbit, que pueda describirse mediante su matriz unitaria:

$$U = \begin{pmatrix} u_{1,1} & u_{1,2} \\ u_{2,1} & u_{2,2} \end{pmatrix}, \tag{1.18}$$

entonces la matriz de su versión controlada será:

$$CU = \left(\begin{array}{cc:cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hdashline 0 & 0 & u_{1,1} & u_{1,2} \\ 0 & 0 & u_{2,1} & u_{2,2} \end{array}\right) \equiv \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}. \tag{1.19}$$

1.13 Ejercicio

Comprobar que la puerta CX cumple la definición general matricial.

1.14 Ejercicio

Describir las puertas CY, CZ y CH de manera matricial.

Esto es extrapolable a cuando U es una matriz de N cúbits, que sigue la expresión matricial:

$$U = \begin{pmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,2^N} \\ u_{2,1} & u_{2,2} & \cdots & u_{2,2^N} \\ \vdots & \vdots & \ddots & \vdots \\ u_{2^N,1} & u_{2^N,2} & \cdots & u_{2^N,2^N} \end{pmatrix}, \tag{1.20}$$

siendo su versión controlada:

$$CU = \left(\begin{array}{ccc:ccc} 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 & \cdots & 0 \\ \hdashline 0 & \cdots & 0 & u_{1,1} & \cdots & u_{1,2^N} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & u_{2^N,1} & \cdots & u_{2^N,2^N} \end{array}\right) \equiv \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}. \tag{1.21}$$

Nota

Una de las operaciones cuánticas más ampliamente utilizadas, que se aplica sobre tres cúbits, es la puerta Toffoli. Puede ser interpretada como una versión de la puerta CX, que en vez de tener un único cúbit de control, tiene dos. En notación ket, se puede definir su comportamiento como:

$$CCX\ |c_1\ \ c_2\ \ t\rangle = |c_1\ \ c_2\ \ t \oplus (c_1 \cdot c_2)\rangle$$

Como puede observarse, esta puerta niega el objetivo únicamente en aquellos estados básicos en los que los dos controles están en estado $|1\rangle$. Por tanto, se puede interpretar como una puerta CU, donde $U = CX$; ya que sólo cuando el primer control c_1 está en estado $|1\rangle$, se ejecuta la CX normalmente entre el segundo control c_2 y el objetivo t. En otro caso, la puerta deja los cúbits inalterados.

1.15 Ejercicio

Calcular la expresión matricial de CCX.

Nota

Otra operación también muy recurrida es la puerta $SWAP$ que realiza el intercambio de dos cúbits:

$$SWAP\ |a\ \ b\rangle = |b\ \ a\rangle$$

1.16 Ejercicio

Considerando cómo se comporta para los cuatro estados básicos de dos cúbits ($|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$), calcular la expresión matricial de CCX.

Medición

Por último, una de las instrucciones más importantes en computación cuántica es la medición. Esta es la que se encarga de la proyección o colapso del estado cuántico, consumiendo sus coeficientes complejos y devolviendo un valor clásico que es emitido por un canal clásico. El estado cuántico colapsado mantiene coherencia con lo obtenido en la medición, ya que elimina aquellas posibilidades que entren en contradicción con el resultado de la misma, por lo que se trata de una operación no lineal.

Aviso

La medición no es una puerta unitaria, se trata de una transformación no lineal que puede destruir parte de la información del sistema.

En el caso más básico de esta operación, la instrucción M de un único cúbit devuelve un único bit de información, según la siguiente expresión:

$$M\ (\alpha_0 |0\rangle + \alpha_1 |1\rangle) = \begin{cases} |0\rangle\,, & \text{con probabilidad } \|\alpha_0\|^2 \\ |1\rangle\,, & \text{con probabilidad } \|\alpha_1\|^2 \end{cases} \tag{1.22}$$

1.17 Ejercicio

Calcular la probabilidad de obtener $|0\rangle$ al ejecutar la instrucción M sobre los estados $|+\rangle$ y $|-\rangle$.

En general, si se miden N cúbits de un sistema $\sum_{j=0}^{2^N-1} \alpha_j |j\rangle$, se obtendrá $|j\rangle$ con probabilidad $\|\alpha_j\|^2$, $\forall j \in \{0, \dots, 2^N - 1\}$.

1.18 Ejercicio

Calcular la probabilidad de obtener $|11\rangle$ al ejecutar la instrucción M sobre los estados $|+-\rangle$ y $\frac{1}{\sqrt{6}} |00\rangle + \frac{2}{3} |01\rangle + \frac{2}{\sqrt{18}} |10\rangle + \frac{1}{\sqrt{6}} |11\rangle$.

Además, aunque colapse sólo una parte del sistema, el estado cuántico completo debe ser congruente con lo obtenido en la medición, eliminando aquellas posibilidades que entren en contradicción y reescalando en consecuencia. De manera general, si se mide únicamente un cúbit j de todo un sistema $|\psi\rangle$:

$$(I \otimes \cdots \otimes I \otimes \underbrace{M}_{j} \otimes I \otimes \cdots \otimes I)\ |\psi\rangle = \begin{cases} \frac{1}{\| |\psi_{q_j=0}\rangle \|} |\psi_{q_j=0}\rangle\,, & \text{con probabilidad } \| |\psi_{q_j=0}\rangle \|^2 \\ \frac{1}{\| |\psi_{q_j=1}\rangle \|} |\psi_{q_j=1}\rangle\,, & \text{con probabilidad } \| |\psi_{q_j=1}\rangle \|^2 \end{cases} \tag{1.23}$$

siendo el estado $|\psi_{q_j=0}\rangle$ aquellas componentes de $|\psi\rangle$ en las que el cúbit j está a 0, y el estado $|\psi_{q_j=1}\rangle$ las posibilidades restantes en las que el cúbit j está a 1. La expresión anterior determina que al aplicar la medición, se debe:

1. Calcular los dos estados posibles tras la medición, denotados de manera genérica como $|\psi_{q_j=x}\rangle$, para $x \in \{0, 1\}$.
2. Calcular su norma $\| |\psi_{q_j=x}\rangle \|$.
3. Realizar la normalización multiplicando el inverso de esta norma por el estado

su norma $\frac{1}{\||\psi_{q_j=x}\rangle\|}|\psi_{q_j=x}\rangle$.

4. Determinar la probabilidad con la que ocurre cada posibilidad elevando esta norma al cuadrado $\||\psi_{q_j=x}\rangle\|^2$.

Por ejemplo, si se tiene el estado $|\psi\rangle = \frac{1}{\sqrt{3}}|00\rangle + \frac{1}{3}|01\rangle + \frac{\sqrt{2}}{3}|10\rangle + \frac{1}{\sqrt{3}}|11\rangle$, y se mide el primer cúbit:

1. Tras la medición:
$$|\psi_{q_1=0}\rangle = \frac{1}{\sqrt{3}}|00\rangle + \frac{1}{3}|01\rangle$$
$$|\psi_{q_1=1}\rangle = \frac{\sqrt{2}}{3}|10\rangle + \frac{1}{\sqrt{3}}|11\rangle$$
2. Normas:
$$\left\||\psi_{q_1=0}\rangle\right\| = \sqrt{\left\|\frac{1}{\sqrt{3}}\right\|^2 + \left\|\frac{1}{3}\right\|^2} = \sqrt{\frac{4}{9}}$$
$$\||\psi_{q_1=1}\rangle\| = \sqrt{\left\|\frac{\sqrt{2}}{3}\right\|^2 + \left\|\frac{1}{\sqrt{3}}\right\|^2} = \sqrt{\frac{5}{9}}$$
3. Normalización:
$$\frac{1}{\sqrt{\frac{4}{9}}}|\psi_{q_1=0}\rangle = \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|01\rangle$$
$$\frac{1}{\sqrt{\frac{5}{9}}}|\psi_{q_1=1}\rangle = \sqrt{\frac{2}{5}}|10\rangle + \sqrt{\frac{3}{5}}|11\rangle$$
4. Probabilidades:
$$\||\psi_{q_1=0}\rangle\|^2 = \frac{4}{9}$$
$$\||\psi_{q_1=1}\rangle\|^2 = \frac{5}{9}$$

Por lo que el resultado de la medición será:

$$(M \otimes I)\ |\psi\rangle = \begin{cases} \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|01\rangle, & \text{con probabilidad } \frac{4}{9} \\ \sqrt{\frac{2}{5}}|10\rangle + \sqrt{\frac{3}{5}}|11\rangle, & \text{con probabilidad } \frac{5}{9} \end{cases} \tag{1.24}$$

1.19 Ejercicio

Calcular la probabilidad de obtener $|1\rangle$ al ejecutar la instrucción M sobre el segundo cúbit de los estados $|+-\rangle$ y $\frac{1}{\sqrt{6}}|00\rangle + \frac{2}{3}|01\rangle + \frac{2}{\sqrt{18}}|10\rangle + \frac{1}{\sqrt{6}}|11\rangle$; e indicar los estados cuánticos completos resultantes tras la operación.