TEMat

Fundamentos de la computación cuántica

Vicente López Oliva
Universitat Jaume I
al341918@uji.es

Resumen: La computación cuántica es un nuevo paradigma que permite abordar algunos problemas intratables con los ordenadores actuales. El impacto de los futuros ordenadores cuánticos puede ser enorme en múltiples áreas como la criptografía, la simulación cuántica o el aprendizaje automático. En este artículo describimos los fundamentos de la computación cuántica, incluyendo tanto las bases matemáticas que la sustentan como las propiedades de la mecánica cuántica que aprovecha para lograr toda su potencia computacional. En concreto, introducimos conceptos como la superposición, el entrelazamiento o el paralelismo cuántico. También mostramos cómo las transformaciones de estados cuánticos se implementan en forma de puertas con las que se construyen circuitos y crean algoritmos cuánticos. Para ilustrar estos últimos mostramos el funcionamiento de un algoritmo cuántico sencillo pero sorprendente, que nos permite la teleportación de estados cuánticos.

Abstract: Quantum computing is a new paradigm that makes it possible to tackle some problems which are intractable with today's computers. The impact of future quantum computers could be enormous in many areas such as cryptography, quantum simulation and machine learning. In this paper we describe the fundamentals of quantum computing, including both the mathematical foundations that underpin it and the properties of quantum mechanics that it harnesses to achieve its full computational power. In particular, we introduce concepts such as superposition, entanglement and quantum parallelism. We also show how quantum state transformations are implemented in the form of gates with which to build circuits and create quantum algorithms. To illustrate these, we show the implementation of a simple but surprising quantum algorithm that allows us to teleport quantum states.

Palabras clave: computación cuántica, cúbit, entrelazamiento, espacio vectorial complejo, algoritmos cuánticos, teleportación cuántica.

MSC2020: 81P68, 68Q12.

Recibido: 2 de marzo de 2021.
Aceptado: 8 de julio de 2021.

Agradecimientos: Quiero mostrar mi agradecimiento al profesor Ximo Gual por darme la oportunidad de realizar el TFG [11], y al profesor José Manuel Badía, sin cuya ayuda no habría sido posible desarrollar el TFG y este artículo no habría visto la luz.

Referencia: López Oliva, Vicente. «Fundamentos de la computación cuántica». En: *TEMat*, 6 (2022), págs. 31-47. ISSN: 2530-9633. URL: https://temat.es/articulo/2022-p31.

1. Introducción

En la actualidad, tenemos computadores capaces de realizar tareas extremadamente complejas y costosas en segundos[1]. No obstante, existen problemas para los que no se conoce ninguna solución con coste polinómico y que se clasifican en la clase NP [12, cap. 3]. Las soluciones a estos problemas tienen un coste exponencial, que los hace intratables para la computación clásica.

Por ejemplo, la simulación realista del comportamiento de sistemas cuánticos sencillos, tales como pequeñas moléculas o reacciones químicas, teniendo en cuenta los efectos de la mecánica cuántica, tiene un coste espacial y temporal tan elevado que no es posible abordarla con los ordenadores clásicos actuales ni previsibles en el futuro. Debido a ello, en 1982 el físico Richard Feynman propuso la creación de ordenadores que sacaran provecho de ese mismo tipo de propiedades cuánticas para poder llevar a cabo este tipo de simulaciones [6].

Las propiedades que muestran los sistemas cuánticos han sorprendido por igual a físicos, matemáticos y todo tipo de científicos desde que fueron descubiertas, debido a que contradicen el comportamiento habitual de los objetos macroscópicos que estamos acostumbrados a observar a nuestro alrededor. A pesar de ello, propiedades como el entrelazamiento o la superposición se han podido aprovechar para diseñar algoritmos cuánticos que podrán resolver en horas problemas tan importantes como la factorización de números enteros, que se encuentra en la base de gran parte de los sistemas criptográficos actuales [9, cap. 4]. De hecho, la computación cuántica ha permitido definir nuevas clases de complejidad, tales como BQP, que incluye los problemas que pueden resolverse con una probabilidad acotada de error usando circuitos cuánticos de tamaño polinómico. Lo llamativo es que esta clase incluye algunos de los problemas NP antes mencionados, tales como el de factorización [12, cap. 1].

Se están realizando grandes avances en la construcción de ordenadores cuánticos, aunque faltan años para poder superar las diferentes dificultades tecnológicas a las que nos enfrentamos tales como, por ejemplo, el tratamiento de errores [12, cap. 10]. No obstante, el aumento de potencia de cálculo asociado a estos ordenadores puede suponer grandes avances en campos con un enorme potencial económico y social, como pueden ser los campos de la química [19], la farmacología [7] o el aprendizaje automático [17, cap. 1], entre otros.

2. Unidad básica de información

2.1. Definición de cúbit

Sabemos que la computación clásica, la que opera en los ordenadores que podemos encontrar en nuestro día a día, utiliza una unidad básica de información que llamamos bit. Estos bits representan estados y son utilizados no solo para hacer funcionar el propio ordenador, sino también para almacenar información. Empecemos por definir qué es un bit.

Definición 1. Un **bit** $b \in \{0, 1\}$ es la unidad mínima de información empleada tanto en los computadores clásicos como en la teoría de la información clásica. ◂

Es importante tener en cuenta que en cada momento un bit solo puede estar en uno de sus dos estados posibles, 0 o 1. Dicho de otro modo, ambos estados son excluyentes. La composición de múltiples bits acaba dando lugar a la información con la que trabaja nuestro ordenador. Por ejemplo, para representar la letra Q haciendo uso de los bits clásicos, utilizaremos el conjunto de bits 01011001, según la representación del código ASCII. El homólogo al bit clásico y el que es la unidad de información básica en computación cuántica es el bit cuántico o cúbit.

Podemos dar una primera definición de cúbit de forma análoga al bit de la siguiente forma.

Definición 2. Un **cúbit** ψ es la unidad mínima de información cuántica empleada tanto en los computadores cuánticos como en la teoría de la información cuántica. ◂

[1] https://top500.org

Un cúbit, al igual que un bit clásico, puede estar en dos estados básicos que se representan utilizando una notación especial. La *notación de Dirac*, también denominada *notación bra-ket*, fue propuesta por primera vez por Dirac [4]. Haremos uso de la notación *ket* para representar el vector v de la forma $|v\rangle = [v_1, \dots, v_n]^\top$ y la notación *bra* para expresar el vector $w^\dagger$, que es el transpuesto conjugado de w, de la forma $\langle w| = [\overline{w}_1, \dots, \overline{w}_n]$. Utilizando esta notación, el producto escalar de $w^\dagger$ y v vendría representado como $\langle w|v\rangle$. Esta notación es utilizada en mecánica cuántica para hacer referencia a vectores en un espacio de Hilbert y está justificada porque un espacio de este tipo y su dual son isomorfos. De este modo, cada *bra* corresponde exactamente a un *ket* y viceversa [12].

La diferencia esencial respecto a los bits clásicos es que los bits cuánticos aprovechan propiedades de la mecánica cuántica para conseguir en algunas circunstancias un aumento enorme en la capacidad de información que pueden almacenar y procesar. La propiedad que explotan para lograrlo es la *superposición de estados*, que hace que un cúbit no esté restringido a sus dos estados básicos, sino que puede estar en una combinación lineal de ambos. Esto da lugar a un conjunto infinito de estados posibles en los que puede estar el cúbit. Más formalmente, los estados de un cúbit se definen de la siguiente forma.

Definición 3. Sean $\alpha, \beta \in \mathbb{C}$ con $|\alpha|^2 + |\beta|^2 = 1$. Definimos el **estado de un cúbit** ψ sobre la base estándar $\{|0\rangle, |1\rangle\}$ como

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

donde α y β se denominan **amplitudes de estado**. Es habitual representar el estado en forma vectorial como $[\alpha, \beta]^\top$, lo que nos permite ver que la base estándar viene dada por $\{[1, 0]^\top, [0, 1]^\top\}$. ◂

Según la definición anterior, un cúbit puede estar en una combinación lineal de estados básicos. Sin embargo, las amplitudes que determinan dicha combinación no pueden ser obtenidas de forma simultánea. Solo podemos obtenerlas de forma experimental bajo ciertas condiciones utilizando técnicas como la tomografía cuántica. Para acceder a la información del cúbit, es necesario realizar una *medida*. La medida de un cúbit en la base estándar nos dará un único valor 0 o 1, «colapsando» el estado de nuestro cúbit en uno de los estados básicos con probabilidad $|\alpha|^2$ de medir un 0 y $|\beta|^2$ de medir un 1. El hecho de que la probabilidad total de medir uno de los dos estados sea 1 explica la condición impuesta en la definición ($|\alpha|^2 + |\beta|^2 = 1$). Una vez el estado ha colapsado, no importa cuántas veces volvamos a realizar la medida en la misma base, el resultado siempre será el mismo.

La medición de estado de un cúbit puede interpretarse geométricamente como la proyección del vector asociado $|\psi\rangle$ sobre alguno de los vectores de una determinada base (por ejemplo, $\{|v_1\rangle, |v_2\rangle\}$). En concreto, la probabilidad de obtener el estado $|v_i\rangle$ tras realizar la medida viene dada por $p(|v_i\rangle) = |\langle v_i|\psi\rangle|^2$.

Hemos visto que el cúbit suele representarse como un vector. En concreto como un vector complejo en un espacio de Hilbert. Vamos a concretar brevemente esta definición.

Definición 4. Un **espacio vectorial complejo** es un espacio vectorial cuyas propiedades se extienden al dominio de los complejos. ◂

Si añadimos el producto escalar $\langle\cdot|\cdot\rangle$ y una propiedad adicional a un espacio vectorial, obtenemos un espacio de Hilbert, que podemos definir de la siguiente forma.

Definición 5. Un **espacio de Hilbert** es un espacio vectorial completo cuya norma procede de un producto escalar. ◂

Que el espacio vectorial sea completo significa que cualquier secuencia de Cauchy de vectores del mismo converge a algún vector que también pertenece al espacio [10]. El producto escalar dota de una métrica al espacio vectorial, lo que nos permite definir la longitud de los vectores usando la siguiente norma:

$$\|\psi\| = \sqrt{\langle\psi|\psi\rangle}. \tag{1}$$

Una vez definido el concepto de espacio de Hilbert, podemos dar una nueva definición tanto de cúbit como de los estados que puede adoptar.

Definición 6. Un **cúbit** es un espacio de Hilbert de dos dimensiones. ◂

Definición 7. Un **estado puro de un cúbit** es cualquier vector unitario (de longitud 1) en el espacio de Hilbert. ◂

A partir de (1) y de la definición 3, podemos ver que la longitud de todo vector representando un estado puro viene dada por

$$\|\psi\| = \sqrt{\overline{\alpha} * \alpha + \overline{\beta} * \beta} = \sqrt{|\alpha|^2 + |\beta|^2} = 1,$$

donde $\overline{\alpha}$ y $\overline{\beta}$ son las amplitudes complejas conjugadas y $*$ representa el producto de números complejos.

La unitariedad de los vectores representando estados cuánticos, y no solo los basados en un solo cúbit sino también en varios, es fundamental puesto que, como hemos comentado anteriormente, las componentes de dichos vectores están asociadas a las probabilidades de cada uno de los estados básicos y estas siempre tienen que sumar 1. Podemos ver más detalles en el libro de Loceff [10].

Tengamos en cuenta que los estados puros son aquellos de los que conocemos toda la información. Sin embargo, también existen los estados mezcla, de los que no se dispone de toda la información. Estos se suelen definir mediante una combinación de distintos estados puros con una determinada distribución de probabilidad y se representan mediante matrices de densidad [12, cap. 2]. En lo que resta de artículo, nos centraremos en las propiedades y funcionamiento de los estados puros.

2.2. Esfera de Bloch

En este apartado, vamos a ver una representación alternativa de los cúbits que nos ayudará a visualizar sus estados y las transformaciones que hagamos sobre ellos. Según la definición 3, un cúbit viene dado por dos números complejos, lo que quiere decir que tenemos cuatro valores reales, que no pueden representarse gráficamente de forma sencilla. No obstante, si revisamos la definición con más detalle nos daremos cuenta de que podemos representar un cúbit en un espacio de tres dimensiones aprovechando ciertas restricciones sobre los valores posibles de ambos números complejos. Para llegar a esta representación comenzaremos por usar la forma polar para las dos amplitudes:

$$\alpha = r_0 e^{i\phi_0}, \qquad \beta = r_1 e^{i\phi_1}.$$

A partir de ellas podemos representar nuestro cúbit como

$$|\psi\rangle = r_0 e^{i\phi_0}|0\rangle + r_1 e^{i\phi_1}|1\rangle. \tag{2}$$

Si extraemos $e^{i\phi_0}$ como factor común, obtenemos que

$$|\psi\rangle = e^{i\phi_0}\left(r_0|0\rangle + r_1 e^{i(\phi_1-\phi_0)}|1\rangle\right),$$

donde ϕ_0 se denomina *fase global* y $(\phi_1 - \phi_0)$ se denomina *fase relativa*.

La fase global, tal y como la hemos definido, cumple la siguiente propiedad.

Propiedad 8. *La fase global de un cúbit no altera la probabilidad de medir sus estados base.*

Demostración. Sea ψ un cúbit con $\alpha, \beta \in \mathbb{C}$ de forma que $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Si le aplicamos una fase global $c = e^{i\phi}$, obtenemos que

$$|c\psi\rangle = c\alpha|0\rangle + c\beta|1\rangle.$$

Dado que $|c| = |e^{i\phi}| = 1$, para todo ϕ, las probabilidades de medir los estados base $|0\rangle$ y $|1\rangle$, respectivamente, son

$$\begin{aligned} |0\rangle &= |c\alpha|^2 = |c|^2|\alpha|^2 = |\alpha|^2, \\ |1\rangle &= |c\beta|^2 = |c|^2|\beta|^2 = |\beta|^2. \end{aligned}$$ ■

Esto hace que los efectos de la fase global no sean observables mediante ningún experimento que mida el estado del cúbit.

Por el contrario, la fase relativa sí puede medirse si elegimos la base adecuada y, además, su influencia será fundamental para la implementación de los algoritmos cuánticos.

Por otro lado, teniendo en cuenta que $|\alpha|^2 + |\beta|^2 = 1$ y su representación en (2),

$$|\alpha|^2 + |\beta|^2 = |r_0 e^{i\phi_0}|^2 + |r_1 e^{i\phi_1}|^2 = |r_0|^2 |e^{i\phi_0}|^2 + |r_1|^2 |e^{i\phi_1}|^2 = 1.$$

Luego, dado que r_0 y r_1 son números reales, tenemos que $r_0^2 + r_1^2 = 1$. Por lo tanto, podemos encontrar un ángulo $\theta/2$ de forma única tal que

$$r_0 = \cos\left(\frac{\theta}{2}\right), \qquad r_1 = \operatorname{sen}\left(\frac{\theta}{2}\right).$$

Esto nos permite reescribir un cúbit como

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi} \operatorname{sen}\left(\frac{\theta}{2}\right)|1\rangle,$$

que tiene únicamente dos parámetros reales, cuyos valores cumplen $0 \leq \phi < 2\pi$ y $0 \leq \theta/2 < \pi/2$ (véase el libro de Sutor [17]). Podemos, pues, obtener una representación de los cúbits como puntos en la superficie de una esfera en un espacio $\mathbb{R}^3$ que podemos ver en la figura 1. Esta representación esférica es la que se conoce como *esfera de Bloch*. Cada estado de un cúbit viene dado de forma única por dos ángulos en esta esfera, que corresponden a la latitud (θ) y la longitud (ϕ) que utilizamos, por ejemplo, para representar la posición de un objeto en la esfera terrestre.

Podemos ver que en la esfera los dos estados que definen la base estándar, $|0\rangle$, $|1\rangle$, que son ortogonales en el espacio de Hilbert, se representan como antipodales. Haber elegido $\theta/2$ como ángulo definido por r_0 y r_1 permite que cada estado puro quede representado por un único punto en la superficie de la esfera y que el ángulo que nos da la latitud sea θ. De hecho, mientras los estados puros quedan representados sobre la superficie, los estados mezcla, de los que hemos hablado anteriormente, se corresponden a los puntos en el interior de la misma.

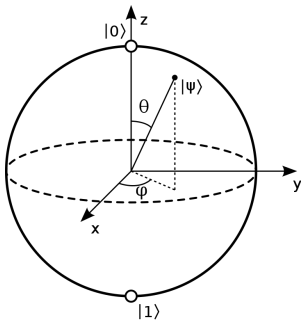


Figura 1: Esfera de Bloch para un cúbit arbitrario $|\psi\rangle$.

2.3. Transformaciones de estados cuánticos

Una vez definida la unidad básica de información cuántica, veamos cómo manipularla. En computación cuántica, para manipular el estado de los cúbits se usan transformaciones lineales, que vienen definidas de la siguiente forma.

Definición 9. Sean dos espacios vectoriales V y W y sea una función $T\colon V \to W$. Diremos que T es una **transformación lineal** si cumple las siguientes propiedades:

(I) para todo $v \in V$ y todo $w \in W$, $T(v + w) = T(v) + T(w)$;

(II) para todo $v \in V$ y todo $c \in \mathbb{C}$, $T(cv) = cT(v)$. ◂

Más concretamente, al operar con cúbits, se utilizan transformaciones lineales unitarias que vienen dadas por matrices unitarias[2]. Recordemos su definición.

Definición 10. Sea $M \in \mathbb{C}^{n\times n}$. Diremos que M es una **matriz unitaria** si cumple que $MM^\dagger = I$, siendo $M^\dagger$ la transpuesta conjugada de M. ◂

Las matrices unitarias tienen propiedades que permiten realizar modificaciones sucesivas de los cúbits, manteniendo siempre un estado cuántico puro conforme a la definición 7. La primera de estas propiedades es la siguiente.

Propiedad 11. *Sean $M, M' \in \mathbb{C}^{n\times n}$ dos matrices unitarias. Entonces, MM' es una matriz unitaria.*

Esta propiedad implica que podemos componer sucesivas transformaciones unitarias en una nueva transformación unitaria. La segunda propiedad importante es que las matrices unitarias preservan el producto escalar.

Propiedad 12. *Sea $M \in \mathbb{C}^{n\times n}$ una matriz unitaria y sean $v, w \in \mathbb{C}^n$. Entonces, $\langle Mv|Mw\rangle = \langle v|w\rangle$.*

Esto implica que el módulo del vector asociado a los estados de los cúbits se mantiene inalterado, preservando su longitud unidad. Podemos ver más detalles, por ejemplo, en el libro de Yanofsky y Mannucci [18].

En los sistemas clásicos, para modificar la información, disponemos de puertas como la AND o como la OR que nos sirven para operar con los bits [17, cap. 2]. En computación cuántica, tenemos sus homólogos, las puertas cuánticas, que pueden definirse del siguiente modo.

Definición 13. Una **puerta cuántica** es un operador que actúa sobre cúbits y está representado por una matriz unitaria. ◂

Esto implica que, dada una puerta cuántica G, siempre vamos a poder encontrar otra puerta G' de forma que $GG' = \mathbb{I}$ (en particular, con $G' = G^\dagger$, por ser G unitaria). Así pues, podemos decir que toda puerta cuántica es *reversible*, es decir, podemos deducir los valores de entrada conociendo solamente los valores de salida, al contrario de lo que ocurre con algunas puertas clásicas [10, cap. 5].

Veamos algunas de las puertas cuánticas sobre un cúbit más utilizadas. La primera puerta que vamos a describir es la conocida como *puerta de Hadamard* y se representa como H. Esta puerta es una de las más importantes, ya que es la que nos permite conseguir un cúbit en un estado de superposición partiendo de un cúbit que se encontraba en uno de los estados básicos $\{|0\rangle, |1\rangle\}$. Si aplicamos la puerta sobre los estados básicos, obtenemos los siguientes estados:

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

De este modo, al aplicar la puerta de Hadamard sobre los estados básicos, obtenemos una superposición equiprobable de los mismos. Esto es, si medimos cualquiera de los estados resultantes, obtendremos los estados $|0\rangle$ o $|1\rangle$ con un 50 % de probabilidad. Notemos que $\{|+\rangle, |-\rangle\}$ forman también una base del espacio de Hilbert, que se conoce como *base de Hadamard* o base Pauli X. Podemos ver en la figura 2 que la aplicación de la puerta de Hadamard, como la del resto de puertas cuánticas, corresponde con una rotación del vector asociado al estado cuántico en la esfera de Bloch. La puerta de Hadamard tiene asociada la siguiente matriz unitaria:

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

Si se aplica una puerta de Hadamard sobre un elemento de la base de Hadamard, por ejemplo sobre el estado $|+\rangle$, se tiene que

$$H|+\rangle = H\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) = \frac{1}{2}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) = |0\rangle,$$

[2] Recordemos que, dada una transformación lineal, podemos encontrar una matriz que represente dicha transformación y viceversa (véase el libro de Loceff [10, cap. 5]), luego podemos hablar de ellas indistintamente.

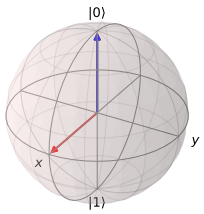


Figura 2: Efecto al aplicar Hadamard sobre el estado $|0\rangle$.

donde se puede observar que las fases del estado $|0\rangle$ se han sumado, mientras que las fases del estado $|1\rangle$ se han cancelado. Este fenómeno se denomina *interferencia* y en algunos casos actúa de forma constructiva y en otros destructiva. Muchos algoritmos cuánticos aprovechan esta propiedad y transforman los estados cuánticos para lograr incrementar las probabilidades asociadas a los estados que son solución del problema y reducir o eliminar las probabilidades del resto de estados.

Las siguientes puertas que introducimos son las *puertas de Pauli*, que son los generadores del grupo especial unitario SU(2). Dado que este grupo es isomorfo con el grupo de rotación SO(3), las tres puertas de Pauli nos permiten representar cualquier rotación en tres dimensiones. De hecho, sus nombres corresponden a los ejes sobre los que cada una de ellas realiza una rotación: X, Y y Z. Sus matrices unitarias asociadas son las siguientes:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

La puerta X corresponde a una rotación de 180° respecto al eje x de la esfera, tal y como puede verse en la figura 3a, donde la flecha azul representa el estado anterior a la transformación del estado $|0\rangle$ y la flecha roja el estado posterior. Esta puerta se suele denominar también NOT porque transforma el estado $|0\rangle$ en $|1\rangle$ y viceversa. También se denomina *bit-flip* debido a que, dado un cúbit en superposición $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, lo transforma en $X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$, es decir, intercambia las amplitudes de los estados base.

La puerta Z corresponde a una rotación de 180° respecto al eje z. Su efecto sobre los estados básicos es dejar inalterado el estado $|0\rangle$ y convertir el estado $|1\rangle$ en $-|1\rangle$. Estas transformaciones no modifican la representación de ambos estados en la esfera de Bloch, tal y como puede observarse en la figura 3b. La mejor forma de ver el efecto de esta puerta es aplicarla sobre los estados de la base de Hadamard. El estado $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ lo transforma en $Z|\psi\rangle = (|0\rangle - |1\rangle)/\sqrt{2} = |-\rangle$ y viceversa. Con este ejemplo podemos ver que esta puerta aplica una fase relativa adicional de 180° al estado, cambiando el signo + por − y viceversa, de ahí que la puerta Z se denomine también *phase-flip*.

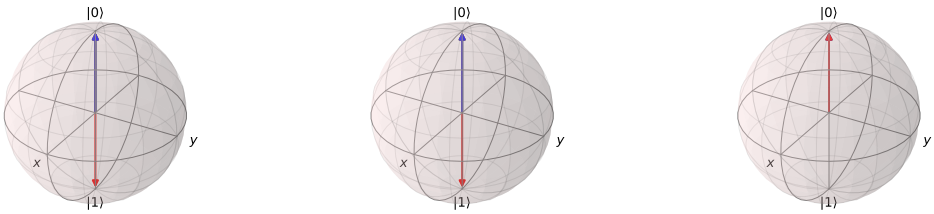
Por último, la puerta Y corresponde a una rotación de 180° respecto al eje Y. Su efecto sobre los estados básicos es convertir el estado $|0\rangle$ en $\mathrm{i}|1\rangle$ y el estado $|1\rangle$ en $-\mathrm{i}|0\rangle$. Podemos ver que, si aplicamos una puerta Y sobre un estado cualquiera en superposición, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, su efecto es el siguiente:

$$Y|\psi\rangle = -\mathrm{i}\beta|0\rangle + \mathrm{i}\alpha|1\rangle = -\mathrm{i}(\beta|0\rangle - \alpha|1\rangle) \equiv \beta|0\rangle - \alpha|1\rangle.$$

La última equivalencia viene dada por el hecho ya comentado con anterioridad de que dos estados cuánticos que solo se diferencien por una fase global de módulo unidad son indistinguibles. Por tanto, podemos ver que la puerta Y combina un *bit-flip* con un *phase-flip*.

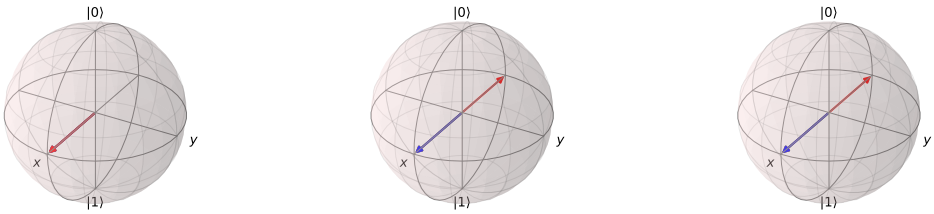
La figura 3 representa el efecto de aplicar las puertas de Pauli sobre el estado $|0\rangle$. Debemos notar que las figuras 3a y 3b son iguales, aunque hemos llegado al mismo estado a través de la rotación alrededor dos ejes diferentes, x e y. Notemos también que, en la figura 3c, el estado $|0\rangle$ no se ha visto afectado por la transformación Z, dado que esta realiza una rotación sobre el eje z en el que se sitúa el vector.

Para ver mejor la diferencia entre las puertas X e Y, vamos a aplicarlas sobre el estado resultante de la figura 2 (es decir, sobre el estado $|+\rangle$), obteniendo como resultado las esferas de la figura 4. En este caso, podemos ver como es la puerta X la que deja invariante el cúbit, ya que gira sobre el mismo eje en que se



(a) Efecto de X. **(b)** Efecto de Y. **(c)** Efecto de Z.

Figura 3: Efectos de las puertas de Pauli sobre el estado $|0\rangle$. En azul el estado inicial y en rojo el final.



(a) Efecto de X. **(b)** Efecto de Y. **(c)** Efecto de Z.

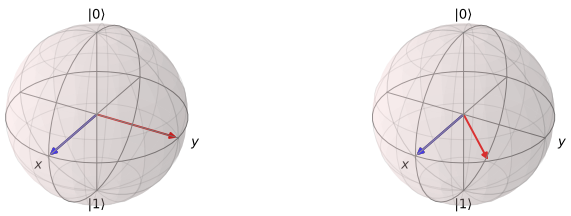
Figura 4: Efectos de las puertas de Pauli sobre el estado $|+\rangle$. En azul el estado inicial y en rojo el final.

encuentra, mientras que las puertas Y y Z confluyen en el mismo resultado, aunque rotando alrededor de dos ejes distintos.

Podemos generalizar las rotaciones alrededor del eje z mediante la puerta R_ϕ^Z, asociada a la siguiente matriz unitaria:

$$R_\phi^Z = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}. \tag{3}$$

Esta puerta realiza una rotación de ángulo ϕ alrededor de z, lo que supone un cambio de fase en el estado del cúbit. Podemos ver que la puerta Z es un caso particular de esta puerta ($Z = R_\pi^Z$). Otros casos particulares de esta puerta son $S = R_{\pi/2}^Z$ y $T = R_{\pi/4}^Z$, cuyos efectos sobre el estado $|+\rangle$ pueden verse en la figura 5.



(a) Efecto de S. **(b)** Efecto de T.

Figura 5: Efectos de las rotaciones sobre el estado $|+\rangle$. En azul, el estado inicial y en rojo, el final.

3. Sistemas cuánticos

3.1. Combinar múltiples cúbits

Al igual que disponer de un ordenador clásico con un único bit no es de mucha utilidad, un ordenador cuántico con un único cúbit tampoco, debido a la cantidad limitada de información que se puede manejar.

En concreto, un cúbit nos permite almacenar dos números complejos correspondientes a sus amplitudes. Es por ello que se hace necesario combinar cúbits para poder conseguir sistemas que permitan trabajar con mayores cantidades de información. Los espacios vectoriales asociados a los cúbits se combinan usando el producto tensorial. En concreto, utilizaremos el producto de Kronecker, que podemos definir para vectores complejos de la siguiente forma.

Definición 14. Sean $A \in \mathbb{C}^n$ y $B \in \mathbb{C}^m$ de la forma

$$A = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}, \qquad B = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}.$$

Se define el **producto de Kronecker para vectores** como

$$A \otimes B = \begin{bmatrix} a_1 \cdot B \\ \vdots \\ a_n \cdot B \end{bmatrix} = \begin{bmatrix} a_1 b_1 \\ \vdots \\ a_1 b_m \\ a_2 b_1 \\ \vdots \\ a_n b_m \end{bmatrix}. \qquad \triangleleft$$

Esto es, para llevar a cabo el producto, multiplicamos cada uno de los elementos del primer vector por todos los del segundo.

Veamos un ejemplo sencillo de cómo combinar dos cúbits. Supongamos que tenemos los cúbits representados por los siguientes vectores: $|\psi_1\rangle = [\alpha_1, \beta_1]^\top$ y $|\psi_2\rangle = [\alpha_2, \beta_2]^\top$. Entonces, el sistema cuántico definido por ambos es

$$|\psi_1\rangle \otimes |\psi_2\rangle = \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix} \otimes \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} = \begin{bmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{bmatrix}. \tag{4}$$

Este producto se puede aplicar sobre los vectores de la base del espacio vectorial. Por ejemplo, si utilizamos la base de cálculo $\{|0\rangle, |1\rangle\}$ de un cúbit, la combinación de todas las parejas posibles formadas con sus elementos da lugar a la base análoga para un sistema de dos cúbits. Así, dicha base se construye como $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$, y suele expresarse de forma compacta como $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Podemos comprobar que dichos vectores tienen dimensión 2^2 y son

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad y \quad |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Así pues, los cúbits se combinan con el producto tensorial conforme al siguiente teorema.

Teorema 15. *Sean dos sistemas cuánticos independientes Q y Q', representados respectivamente por los espacios de Hilbert $\mathbb{V}$ y $\mathbb{V}'$. Entonces, el sistema cuántico resultante al combinar Q y Q' tendrá el producto tensorial $\mathbb{V} \otimes \mathbb{V}'$ como espacio de los estados.*

El estado resultante de combinar dos cúbits usando (4) se denomina *estado separable*, ya que, dado el estado $[\alpha_1\alpha_2, \alpha_1\beta_2, \beta_1\alpha_2, \beta_1\beta_2]^\top$, podemos obtener los estados (las amplitudes) de los dos cúbits combinados. Sin embargo, en la gran mayoría de los casos, no es posible separar dichos estados. Por ejemplo, el estado $|\psi\rangle = [1/\sqrt{2}, 0, 0, 1/\sqrt{2}]^\top$ no puede separarse en dos cúbits independientes. Cuando esto ocurre se dice que el sistema cuántico está en un *estado no separable*, más habitualmente denominado *estado entrelazado*.

Definición 16. Diremos que un sistema cuántico $|\psi\rangle$ está en un **estado entrelazado** o no separable si no existen $|\psi_1\rangle, |\psi_2\rangle$ de forma que $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. $\triangleleft$

El entrelazamiento es uno de los fenómenos más llamativos y difíciles de explicar de la mecánica cuántica y también es una de las propiedades que son la base del funcionamiento de la mayoría de los algoritmos cuánticos. Esto se debe a la siguiente propiedad.

Propiedad 17. *Sea un sistema cuántico $|\psi\rangle$ en un estado entrelazado de dos cúbits $|\psi_1\rangle$ y $|\psi_2\rangle$. Entonces, cualquier cambio sobre el estado del cúbit $|\psi_1\rangle$ modificará el estado del cúbit $|\psi_2\rangle$ independientemente de la distancia entre ellos.*

Intentemos explicarlo con un ejemplo. Supongamos que tenemos dos cúbits entrelazados en el siguiente estado:

$$|\psi\rangle = \left[\frac{1}{\sqrt{2}}, 0, 0, \frac{1}{\sqrt{2}}\right]^{\top} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

y que hemos separado los sistemas físicos que almacenan ambos cúbits una enorme distancia; por ejemplo, tenemos uno en la Tierra y otro en Júpiter. Sabemos que si medimos en la Tierra el primer cúbit y obtenemos el estado $|0\rangle$, el segundo estará necesariamente en ese mismo estado $|0\rangle$, y lo mismo ocurrirá si al medir el estado del primer cúbit obtenemos $|1\rangle$. Además, el colapso del estado del segundo cúbit se producirá de modo simultáneo al producido al medir el primero, independientemente de la distancia y de que el límite de la velocidad de la luz impide que se dé una comunicación instantánea entre la Tierra y Júpiter. El entrelazamiento da lugar, pues, a un fenómeno «misterioso» que Albert Einstein denominó «*acción fantasmal a distancia*». Esto es, sabemos que el resultado de medir cada cúbit por separado es totalmente aleatorio y que existe una probabilidad del 50 % de que lo midamos en cada uno de los dos estados básicos. Sin embargo, existe una correlación total entre los estados de ambos cúbits que hace que el estado del segundo cúbit quede, en ese caso, definido con un 100 % de probabilidad. Así pues, el estado del sistema de dos cúbits entrelazados solo puede entenderse completamente como un estado global y no como dos componentes manipulables por separado. No obstante, el entrelazamiento no permite la transmisión de información más rápido que la luz. Si medimos el cúbit en la Tierra y obtenemos un $|0\rangle$, no podremos saber si ha sido un resultado aleatorio o es porque se ha medido primero el cúbit en Júpiter y se ha obtenido ese mismo valor. Tal y como veremos al describir la teleportación cuántica, solo usando un canal clásico para comunicar esa información podremos saber quién lo midió primero [1, 5].

En (4) hemos visto que el producto tensorial de dos sistemas de $\mathbb{C}^2$ resulta en un nuevo sistema en $\mathbb{C}^4$. Esto es, combinar dos cúbits duplica el tamaño del espacio vectorial. En general, el crecimiento del tamaño de los sistemas cuánticos viene dado por la siguiente propiedad.

Propiedad 18. *Sea $A \in \mathbb{C}^n$ y sea $B \in \mathbb{C}^m$. Entonces, el producto tensorial $A \otimes B$ pertenece al espacio $\mathbb{C}^{nm}$.*

Sabemos que los cúbits nos permiten almacenar información codificada en las amplitudes. Un cúbit nos permite almacenar dos estados posibles al mismo tiempo, cada uno de ellos con una cierta probabilidad. En base a la propiedad anterior asociada al producto tensorial, dos cúbits nos permitirán almacenar $2 \times 2 = 2^2$ estados y, en general, n cúbits nos permitirán almacenar 2^n estados. Aumentar en uno la cantidad de cúbits disponibles duplica la cantidad de información que podemos almacenar. Esto es, la información almacenable y utilizable en los algoritmos aumenta exponencialmente con el número de cúbits. En contraste, en el caso de los bits clásicos, la información almacenable aumenta solo linealmente con el número de bits.

3.2. Transformaciones con múltiples cúbits

En el apartado 3.1 vimos que las transformaciones de los estados de un cúbit se asocian a matrices complejas de tamaño 2×2. Dado que los estados de n cúbits se representan mediante vectores de tamaño 2^n, las matrices asociadas a sus transformaciones serán de tamaño $2^n \times 2^n$. Estas transformaciones se suelen implementar mediante la combinación de puertas cuánticas de uno y dos cúbits.

Por ejemplo, supongamos que tenemos un sistema cuántico de dos cúbits dado por $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ y queremos aplicar una transformación de Hadamard a cada uno de ellos. En ese caso, en base a las propiedades del producto tensorial (véase el libro de Scherer [15]), obtenemos que

$$H|\psi_1\rangle \otimes H|\psi_2\rangle = (H \otimes H)(|\psi_1\rangle \otimes |\psi_2\rangle) = (H \otimes H)|\psi\rangle = H^{\otimes 2}|\psi\rangle.$$

Por tanto, $H^{\otimes 2} = H \otimes H$ es una transformación sobre dos cúbits que tiene el efecto de aplicar una Hadamard sobre el primer cúbit y otra sobre el segundo. De forma análoga, si se quiere aplicar la transformación de Hadamard únicamente sobre el primer cúbit, aplicaremos a ambos cúbits la transformación dada por $H \otimes I_2$, siendo I_2 la matriz identidad en $\mathbb{C}^2$. Para poder realizar estas operaciones, es necesario extender la definición del producto de Kronecker a matrices complejas.

Definición 19. Sean dos matrices complejas A y B de la forma

$$A = \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{bmatrix}, \qquad B = \begin{bmatrix} b_{1,1} & \cdots & b_{1,t} \\ \vdots & \ddots & \vdots \\ b_{p,1} & \cdots & b_{p,t} \end{bmatrix}.$$

Se define el producto de Kronecker como

$$A \otimes B = \begin{bmatrix} a_{1,1} \cdot B & \cdots & a_{1,n} \cdot B \\ \vdots & \ddots & \vdots \\ a_{m,1} \cdot B & \cdots & a_{m,n} \cdot B \end{bmatrix} = \begin{bmatrix} a_{1,1}b_{1,1} & \cdots & a_{1,1}b_{1,t} & a_{1,2}b_{1,1} & \cdots & a_{1,n}b_{1,t} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{1,1}b_{p,1} & \cdots & a_{1,1}b_{p,t} & a_{1,2}b_{p,1} & \cdots & a_{1,n}b_{p,t} \\ a_{2,1}b_{1,1} & \cdots & a_{2,1}b_{1,t} & a_{2,2}b_{1,1} & \cdots & a_{2,n}b_{1,t} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{m,1}b_{1,1} & \cdots & a_{m,1}b_{p,t} & a_{m,2}b_{p,1} & \cdots & a_{m,n}b_{p,t} \end{bmatrix}.$$

Esta nueva definición permite obtener la matriz asociada a $H \otimes H$:

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

Si aplicamos esta transformación $H^{\otimes 2}$ al estado $|00\rangle$ obtenemos un estado especial y muy utilizado para iniciar algoritmos cuánticos:

$$H^{\otimes 2}|00\rangle = H^{\otimes 2}|0\rangle_2 = \frac{1}{\sqrt{2^2}} \sum_{x \in \{0,1\}^2} |x\rangle_2 = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).$$

Podemos ver que, de modo análogo a lo que ocurre con la puerta de Hadamard aplicada a un cúbit, obtenemos una superposición equiprobable de todos los estados básicos de dos cúbits. Este mismo comportamiento puede extenderse a n cúbits usando la transformación $H^{\otimes n}$:

$$H^{\otimes n}|0\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle_n. \tag{5}$$

Las transformaciones con varios cúbits descritas hasta el momento se aplican individualmente sobre cada cúbit y mantienen el sistema en un estado separable. Para poder obtener toda la potencia dada por el entrelazamiento de sistemas cuánticos es necesario utilizar alguna puerta que permita, tal y como veremos en el próximo apartado, entrelazar varios cúbits. La más conocida de estas es la puerta NOT controlada o CNOT. El primero de los cúbits sobre los que se aplica se denomina *control* y el segundo *objetivo*. Esta puerta tiene como efecto aplicar una puerta NOT (otra denominación de X) sobre el objetivo cuando el control se encuentra en el estado $|1\rangle$ y de no aplicar ningún cambio (es decir, aplicar la identidad sobre el objetivo) cuando el control se encuentra en el estado $|0\rangle$. Su matriz unitaria es

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

y si la aplicamos sobre los cuatro estados básicos de dos cúbits su efecto es el siguiente:

$$\text{CNOT}|00\rangle = |00\rangle, \qquad \text{CNOT}|10\rangle = |11\rangle,$$
$$\text{CNOT}|01\rangle = |01\rangle, \qquad \text{CNOT}|11\rangle = |10\rangle.$$

Esta puerta es el equivalente reversible de la puerta XOR, ya que obtiene en el cúbit objetivo el resultado de aplicar esa operación sobre los dos cúbits de entrada. Otras dos puertas importantes de varios cúbits son la SWAP y la Toffoli. La puerta SWAP sobre dos cúbits debe su nombre a que intercambia las amplitudes de ambos estados. Esta puerta es muy utilizada por los compiladores cuando realizan transformaciones sobre los circuitos cuánticos [2]. La puerta de Toffoli sobre tres cúbits es una puerta NOT doblemente controlada. Esto es, aplicará una puerta NOT sobre el tercer cúbit si y solo si los dos primeros cúbits se encuentran en el estado $|1\rangle$. Esta puerta permite la implementación reversible de todas las puertas clásicas: OR, AND, NAND, etc. [18].

3.3. Circuitos cuánticos

El modelo más utilizado para representar los algoritmos cuánticos es el basado en circuitos cuánticos, aunque existen otros como el basado en *quantum annealers* [9, cap. 2]. Como ocurre con los circuitos en los ordenadores clásicos, estos se construyen aplicando en un cierto orden puertas, pero en este caso puertas cuánticas sobre cúbits. Dichos cúbits se agrupan en registros.

Definición 20. Un **registro cuántico** es una colección de cúbits $\psi_1, \dots, \psi_n$ que se utilizan para el cálculo. ◂

Es decir, un registro cuántico define el número y orden de los cúbits. Esto, combinado con la sucesión de puertas cuánticas, nos permite definir un circuito cuántico como sigue.

Definición 21. Un **circuito cuántico** es una sucesión de puertas cuánticas $P_1, \dots, P_n$ que se aplican sobre un registro cuántico. ◂

Para representar un circuito cuántico, se disponen los cúbits del registro cuántico en el eje vertical en orden descendente conforme a su posición del registro. Asociada a cada cúbit del registro, se dibuja una línea horizontal que denota el tiempo de izquierda a derecha. Sobre dichas líneas se dibujan las puertas cuánticas que se aplican sobre uno o varios cúbits.

En la figura 6 podemos ver un ejemplo de circuito cuántico sencillo pero muy importante, puesto que se utiliza para entrelazar los estados de los dos cúbits sobre los que se aplica: $|x\rangle$ y $|y\rangle$. Se suele analizar el funcionamiento de un circuito cuántico estudiando el estado del sistema en determinados momentos, tras la aplicación de algunas de las puertas incluidas. En este ejemplo estudiaremos el estado en tres momentos, dados por $|\varphi_1\rangle$, $|\varphi_2\rangle$ y $|\varphi_3\rangle$.

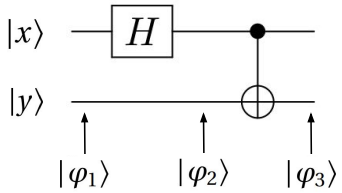


Figura 6: Ejemplo circuito cuántico.

En el estado $|\varphi_1\rangle$, tenemos los cúbits en el estado inicial, es decir, tenemos que $|\varphi_1\rangle = |x\rangle \otimes |y\rangle$. Tras aplicar una puerta de Hadamard (H) sobre el primer cúbit, llegamos al estado

$$|\varphi_2\rangle = H|x\rangle \otimes |y\rangle = (H \otimes I_2)(|x\rangle \otimes |y\rangle).$$

Por último, aplicamos una puerta CNOT usando el primer cúbit como control y el segundo como objetivo. El estado resultante viene dado por

$$|\varphi_3\rangle = \mathrm{CNOT}(H|x\rangle \otimes |y\rangle) = \mathrm{CNOT}(H \otimes I_2)(|x\rangle \otimes |y\rangle).$$

Es interesante observar que las transformaciones aparecen en la ecuación en orden inverso a las puertas en el circuito.

Estudiemos el circuito cuántico para un caso concreto para entender su efecto. Supongamos que el registro cuántico está compuesto por dos cúbits en estado $|0\rangle$. Este es el estado habitual en que suelen iniciarse todos los algoritmos cuánticos. Así pues, el estado inicial será

$$|\varphi_1\rangle = |0\rangle \otimes |0\rangle = |00\rangle.$$

Tras aplicar la puerta de Hadamard sobre el primer cúbit obtenemos

$$|\varphi_2\rangle = H|0\rangle \otimes |0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

Por último, aplicamos una puerta CNOT y obtenemos

$$|\varphi_3\rangle = \text{CNOT}\,\frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

El resultado es precisamente el estado entrelazado comentado en el apartado 3.1. Se trata de uno de los cuatro estados denominados pares de Bell, obtenidos aplicando el circuito anterior sobre cada uno de los cuatro estados básicos de dos cúbits: $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Estos estados se utilizan, por ejemplo, en el algoritmo de teleportación cuántica que veremos en el siguiente apartado.

Veamos ahora de dónde surge la potencia computacional de los ordenadores cuánticos. Supongamos para ello que tenemos una función $f : \{0,1\}^n \to \{0,1\}$ que, dada cualquier cadena de n bits, obtiene un bit. Supongamos también que tenemos un circuito cuántico que usa una transformación unitaria U_f para calcular dicha función del siguiente modo:

$$U_f(|x\rangle_n|0\rangle) = |x\rangle_n|f(x)\rangle.$$

Esto es, la transformación deja invariables los primeros n cúbits de entrada y devuelve en el cúbit $n+1$ el resultado de aplicar la función f sobre los mismos. Puede consultarse, por ejemplo, el libro de Nielsen y Chuang [12] para ver cómo construir esta transformación. Su «potencia» surge cuando el estado de entrada $|x\rangle$ es una superposición equiprobable como la obtenida en (5). En ese caso, teniendo en cuenta que se trata de una transformación lineal, el resultado será

$$U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (|x\rangle_n|0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} U_f(|x\rangle_n|0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_n|f(x)\rangle.$$

Podemos ver que, aunque la transformación se ha aplicado solo una vez para el estado en superposición, de algún modo la función se ha evaluado simultáneamente para los 2^n estados superpuestos. La posibilidad de almacenar 2^n estados usando solo n cúbits y de poder modificar todos esos estados a la vez se denomina *paralelismo cuántico*. Esa potencia computacional que crece exponencialmente con el número de cúbits es lo que permite abordar con ordenadores cuánticos determinados problemas intratables con ordenadores clásicos. No obstante, para poder aprovechar el paralelismo cuántico, los algoritmos deben modificar los estados superpuestos, de modo que, aprovechando la interferencia entre ellos, se incremente al máximo la probabilidad de obtener finalmente la solución correcta y se decremente la de medir soluciones incorrectas.

4. Algoritmos cuánticos

Siguiendo con el modelo de circuitos cuánticos, los algoritmos cuánticos son circuitos pensados para realizar una tarea o resolver un problema. En este apartado revisaremos uno de los más conocidos y, a pesar de su simplicidad, uno de los más llamativos. Se trata del algoritmo de teleportación cuántica, que ya ha sido utilizado en la práctica desde satélites en órbita [14]. Este algoritmo aprovecha la propiedad de que, dados dos cúbits entrelazados, los cambios sobre uno de los cúbits afectan al otro sin importar la distancia.

En la figura 7 está representado el circuito cuántico del algoritmo. Detallemos los pasos seguidos en el algoritmo. Sea $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ el estado del cúbit que Alice desea enviar a Bob ($|x\rangle$ en el circuito). Para

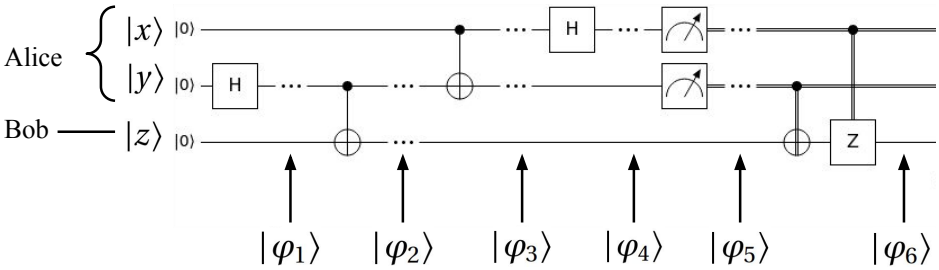


Figura 7: Circuito del algoritmo de teleportación cuántica.

poder enviarlo, necesitan repartirse dos cúbits entrelazados, que serán los cúbits $|y\rangle$ y $|z\rangle$ del circuito. Esto se consigue construyendo con estos cúbits un par de Bell, tal y como se ha descrito en el apartado 3.3. De este modo, en el estado $|\varphi_2\rangle$ los cúbits $|y\rangle$ y $|z\rangle$ se encontrarán en el siguiente estado:

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

En este punto, Alice se queda con uno de los cúbits entrelazados, $|y\rangle$, y Bob con el otro, $|z\rangle$. Ambos pueden entonces alejarse todo lo que quieran y, en cualquier momento, utilizar los cúbits entrelazados para llevar a cabo la teleportación de $|\psi\rangle$.

Si incluimos el cúbit que queremos teleportar en posesión de Alice, obtenemos el estado

$$|\varphi_2\rangle = |\psi\rangle \otimes |yz\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle).$$

Para iniciar la teleportación, Alice aplica una puerta CNOT sobre sus dos cúbits, transformando el sistema global al estado

$$|\varphi_3\rangle = (\text{CNOT} \otimes I)|\varphi_2\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle),$$

que puede expresarse también como

$$|\varphi_3\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle \otimes (|00\rangle + |11\rangle) + \beta|1\rangle \otimes (|10\rangle + |01\rangle)].$$

Lo siguiente que debe hacer Alice es aplicar una puerta H sobre el cúbit $|\psi\rangle$, dejando el sistema en el siguiente estado:

$$\begin{aligned}
|\varphi_4\rangle &= (H \otimes I_2)\left(\frac{1}{\sqrt{2}}[\alpha|0\rangle \otimes (|00\rangle + |11\rangle) + \beta|1\rangle \otimes (|10\rangle + |01\rangle)]\right) \\
&= \frac{1}{2}\,[\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)] \\
&= \frac{1}{2}[|00\rangle(\beta|1\rangle + \alpha|0\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(-\beta|1\rangle + \alpha|0\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)].
\end{aligned}$$

En este punto, Alice mide sus dos cúbits y puede obtener con igual probabilidad cada uno de los estados básicos. En cada caso, el cúbit de Bob colapsará a un estado diferente dado por el cuadro 1.

Para completar la teleportación, Bob puede tener que realizar algunas transformaciones sobre el estado de sus cúbits que dependerán de los cúbits medidos por Alice. Por ello, Alice debe enviarle el resultado de su medición, y puede hacerlo por un canal clásico, puesto que solo necesita enviar dos bits de información. Las transformaciones que realizará Bob en ese punto para obtener en su cúbit el estado teleportado $|\psi\rangle$ pueden verse en el cuadro 2.

Podemos ver que la teleportación se ha producido y Bob acaba teniendo en todos los casos en el cúbit z el estado $|\psi\rangle$ inicialmente en posesión de Alice. Merece la pena comentar algunos aspectos del proceso.

Cuadro 1: Estado de los cúbits en $|\varphi_5\rangle$, tras la medición de Alice.

cúbits de Alice	**cúbit de Bob en** $|\varphi_5\rangle$
00	$\alpha|0\rangle + \beta|1\rangle$
01	$\beta|0\rangle + \alpha|1\rangle$
10	$\alpha|0\rangle - \beta|1\rangle$
11	$-\beta|0\rangle + \alpha|1\rangle$

Cuadro 2: Estado de los cúbits en $|\varphi_6\rangle$, tras completarse la teleportación.

cúbits de Alice	**cúbit de Bob en** $|\varphi_6\rangle$
00	$I(\alpha|0\rangle + \beta|1\rangle) \to \alpha|0\rangle + \beta|1\rangle$
01	$X(\beta|0\rangle + \alpha|1\rangle) \to \alpha|0\rangle + \beta|1\rangle$
10	$Z(\alpha|0\rangle - \beta|1\rangle) \to \alpha|0\rangle + \beta|1\rangle$
11	$ZX(-\beta|0\rangle + \alpha|1\rangle) \to \alpha|0\rangle + \beta|1\rangle$

Nótese que en ningún momento se ha comunicado información más rápido que la luz, puesto que los bits de Alice se han enviado por un canal clásico. Es cierto que ha sido necesario enviar esos dos bits, pero en realidad se han teleportado las dos amplitudes complejas asociadas a $|\psi\rangle$ con una precisión infinita. Para ello ha sido necesario destruir el estado inicial del cúbit x de Alice cuando esta lo ha medido. También se ha destruido el estado de los dos cúbits inicialmente entrelazados que han usado Alice y Bob como base para lograr la teleportación. Finalmente, en ningún caso estamos hablando de teleportación de materia, sino de información en forma de estado cuántico de un cúbit.

Existen un conjunto de algoritmos cuánticos bien conocidos que sirvieron para demostrar el potencial de la computación cuántica. Estos son el algoritmo de Deutsch-Jozsa [3] que determina si una función es constante o equilibrada, o el algoritmo de Grover [8], que permite buscar información en secuencias de datos no ordenados. Pero sin lugar a dudas, el algoritmo cuántico más conocido y que sirvió para despertar el interés en la computación cuántica es el algoritmo de Shor [16], que permite factorizar grandes números enteros con un coste lineal y puede suponer una amenaza para los sistemas criptográficos actuales en el momento en que podamos construir ordenadores cuánticos con un número suficiente de cúbits [9, cap. 4]. Debido a ello, se están desarrollando nuevos sistemas criptográficos resistentes a la computación cuántica. No obstante, dado que la adaptación de todos los sistemas actuales a la criptografía postcuántica puede llevar más de una década, es urgente no solo desarrollarlos, sino también desplegarlos [9, cap. 4].

Por otro lado, el funcionamiento de los algoritmos comentados se basa en la existencia de ordenadores cuánticos sin errores. En la actualidad, y muy probablemente durante bastantes años, nos encontraremos en la denominada era *Noisy Intermediate-Scale Quantum (NISQ)*, en la que manejaremos unos pocos cientos de cúbits con ruido y puertas con fiabilidad reducida [13]. Para la obtención de un cúbit lógico sin ruido es necesario utilizar sistemas de corrección de errores que involucran cientos de cúbits físicos ruidosos. Dado que queda mucho tiempo para disponer de ordenadores cuánticos con los muchos miles de cúbits necesarios para implementar los algoritmos comentados, nuestra mayor esperanza a corto plazo es el desarrollo de algoritmos eficientes que permitan obtener soluciones aproximadas a problemas con aplicación práctica y rendimiento económico usando pocos cúbits. Entre ellos se encuentran los algoritmos cuánticos variacionales, que permiten utilizar sistemas híbridos que combinan un ordenador clásico con uno cuántico para resolver, por ejemplo, problemas de química cuántica con aplicaciones en farmacología o ciencia de materiales [9, cap. 3].

5. Conclusiones

A lo largo del artículo hemos podido constatar cómo los fundamentos matemáticos de la computación cuántica son sorprendentemente simples. Esto es así a pesar de que algunos de los fenómenos físicos en que se apoya, tales como el entrelazamiento o el efecto de la medida, supusieron un reto para algunas de las mentes más brillantes del siglo pasado, como Albert Einstein y Niels Bohr, y cuya interpretación sigue siendo polémica en la actualidad. Básicamente, la computación cuántica se basa en el álgebra lineal compleja con el uso, menos habitual, del producto tensorial. También hemos podido describir algunas de las propiedades que confieren toda su capacidad y poder computacional a los ordenadores cuánticos. Hemos descrito la superposición de estados cuánticos y el caso particular del entrelazamiento de varios cúbits. Hemos comentado cómo aprovechar el fenómeno de la interferencia. También hemos visto cómo el crecimiento exponencial de la información con el número de cúbits en ciertos casos y la posibilidad de transformar simultáneamente todos los estados en superposición pueden dar lugar a la potencia de cálculo exponencial del paralelismo cuántico para ciertos problemas. Finalmente, hemos visto cómo sacar partido de esas propiedades mediante el uso de circuitos cuánticos para poder llevar a cabo tareas sorprendentes y abordar problemas aparentemente intratables con ordenadores clásicos, tales como la factorización de grandes números enteros.

Referencias

[1] Bell, John Stewart. «On the Einstein Podolsky Rosen paradox». En: *Physics Physique Fizika* 1.3 (1964), págs. 195-200. ISSN: 0554-128X. https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195.

[2] Chong, Frederic T.; Franklin, Diana, y Martonosi, Margaret. «Programming languages and compiler design for realistic quantum hardware». En: *Nature* 549 (2017), págs. 180-187. ISSN: 1476-4687. https://doi.org/10.1038/nature23459.

[3] Deutsch, David y Jozsa, Richard. «Rapid solution of problems by quantum computation». En: *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439.1907 (1992), págs. 553-558. ISSN: 0962-8444. https://doi.org/10.1098/rspa.1992.0167.

[4] Dirac, Paul A. M. «A new notation for quantum mechanics». En: *Mathematical Proceedings of the Cambridge Philosophical Society* 35.3 (1939), págs. 416-418. ISSN: 0305-0041. https://doi.org/10.1017/S0305004100021162.

[5] Einstein, Albert; Podolsky, Boris, y Rosen, Nathan. «Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?» En: *Physical Review* 47.10 (1935), págs. 777-780. ISSN: 0031-899X. https://doi.org/10.1103/PhysRev.47.777.

[6] Feynman, Richard P. «Simulating physics with computers». En: *International Journal of Theoretical Physics* 21.6-7 (1982), págs. 467-488. ISSN: 0020-7748. https://doi.org/10.1007/BF02650179.

[7] Gerbert, Philipp y Rueß, Frank. *The Next Decade in Quantum Computing—and How to Play*. Boston Consulting Group. 15 de nov. de 2018. URL: https://www.bcg.com/publications/2018/next-decade-quantum-computing-how-play (visitado 02-2021).

[8] Grover, Lov K. «A fast quantum mechanical algorithm for database search». En: *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*. 1996, págs. 212-219. https://doi.org/10.1145/237814.237866.

[9] Grumbling, Emily y Horowitz, Mark, eds. *Quantum Computing: Progress and Prospects*. National Academies of Sciences, Engineering, and Medicine. Washington, US: The National Academies Press, 2019. https://doi.org/10.17226/25196.

[10] Loceff, Michael. *A Course in Quantum Computing*. 2015. URL: https://lapastillaroja.net/wp-content/uploads/2016/09/Intro_to_QC_Vol_1_Loceff.pdf (visitado 02-2021).

[11] López Oliva, Vicente. *An introduction to Quantum algorithms*. Trabajo de Fin de Grado. Universitat Jaume I, 2020. URL: http://hdl.handle.net/10234/191725.

[12] Nielsen, Michael A. y Chuang, Isaac L. *Quantum Computation and Quantum Information. 10th Anniversary Edition*. Cambridge, UK: Cambridge University Press, 2010. https://doi.org/10.1017/CBO9780511976667.

[13] Preskill, John. «Quantum Computing in the NISQ era and beyond». En: *Quantum* 2, artículo 79 (2018). issn: 2521-327X. https://doi.org/10.22331/q-2018-08-06-79.

[14] Ren, Ji-Gang; Xu, Ping; Yong, Hai-Lin; Zhang, Liang; Liao, Sheng-Kai; Yin, Juan; Liu, Wei-Yue; Cai, Wen-Qi; Yang, Meng; Li, Li; Yang, Kui-Xing; Han, Xuan; Yao, Yong-Qiang; Li, Ji; Wu, Hai-Yan; Wan, Song; Liu, Lei; Liu, Ding-Quan; Kuang, Yao-Wu; He, Zhi-Ping; Shang, Peng; Guo, Cheng; Zheng, Ru-Hua; Tian, Kai; Zhu, Zhen-Cai; Liu, Nai-Le; Lu, Chao-Yang; Shu, Rong; Chen, Yu-Ao; Peng, Cheng-Zhi; Wang, Jian-Yu, y Pan, Jian-Wei. «Ground-to-satellite quantum teleportation». En: *Nature* 549 (2017), págs. 70-73. issn: 1476-4687. https://doi.org/10.1038/nature23675.

[15] Scherer, Wolfgang. *Mathematics of Quantum Computing. An Introduction*. Cham, CH: Springer, 2019. https://doi.org/10.1007/978-3-030-12358-1.

[16] Shor, Peter W. «Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer». En: *SIAM Review* 41.2 (1999), págs. 303-332. issn: 0036-1445. https://doi.org/10.1137/S0036144598347011.

[17] Sutor, Robert S. *Dancing with qubits. How quantum computing works and how it can change the world*. Birmingham, UK: Packt, 2019. isbn: 978-1-83882-736-6.

[18] Yanofsky, Noson S. y Mannucci, Mirco A. *Quantum computing for computer scientists*. Cambridge, UK: Cambridge University Press, 2008. https://doi.org/10.1017/CBO9780511813887.

[19] Yuan, Xiao. «A quantum-computing advantage for chemistry». En: *Science* 369 (2020), págs. 1054-1055. issn: 1095-9203. https://doi.org/10.1126/science.abd3880.