Notas sobre la computación cuántica

Notes on quantum computing

Ricardo Rosenfeld
Facultad de Informática, Universidad Nacional de La Plata, Argentina. CAETI, Universidad Abierta Interamericana (UAI), Argentina.

DOI *https://doi.org/10.59471/raia2026243*
Enviado: agosto 2026. **Aceptado**: octubre 2026. **Publicado:** noviembre 2026
Como citar: Rosenfeld, R. (2026). Notas sobre la computación cuántical, *Revista Abierta de Informática Aplicada, 10(1)*, 1-28 *https://doi.org/10.59471/raia2026243*

Resumen

Este artículo incluye una serie de notas con las que se pretende brindar al lector una primera aproximación a la computación cuántica. Se consideran las razones para estudiarla, la física y las matemáticas necesarias, los fundamentos teóricos, los modelos computacionales principales, características de los algoritmos y de la complejidad computacional, y una breve revisión de los orígenes y la evolución del paradigma. Se pone especial atención en las similitudes y diferencias entre la computación probabilística, que es el modelo de computación clásica de referencia en el contexto de la complejidad computacional, y la computación cuántica. Por razones de espacio no se describen algoritmos cuánticos representativos, que serán presentados en un próximo artículo.

PALABRAS CLAVE: computación cuántica, algoritmo, complejidad.

Abstract

This article includes a series of notes intended to provide the reader with an initial aproximation to quantum computing. It covers the reasons for studying the field, the necessary physics and mathematics, the theoretical foundations, the key computational models, characteristics of the algorithms and computational complexity, and a brief overview of the origins and evolution of the paradigm. Particular attention is paid to the similarities and differences between probabilistic computing, which is the standard classical model in the context of computational complexity, and quantum computing. Due to space constraints, representative quantum algorithms are not described, which will be presented in a subsequent article.

KEYWORDS: quantum computing, algorithm, complexity.

Este trabajo está bajo una Licencia Creative Commons Atribución 4.0 Internacional

INTRODUCCIÓN

En la región se observa un creciente interés por la *computación cuántica*, paradigma de computación alternativo al clásico basado en los principios de la mecánica cuántica. Dicho interés lo impulsan, entre otros factores, los importantes avances logrados en los últimos años en el desarrollo de las computadoras cuánticas, las cuales tendrían mayor poder computacional, en el sentido de la complejidad temporal, que las computadoras clásicas. Por tal razón, crece la demanda de contar con material en español que cubra los conocimientos necesarios, ciertamente novedosos para quienes provienen del escenario clásico. Y si bien dicho material ha crecido en el último tiempo, aún está lejos de resultar suficiente. Además, se encuentra mayormente disperso en artículos y cursos en línea, y se presenta con grados muy variados de formalidad, profundidad y enfoque.

Teniendo en cuenta esta situación, elaboré un libro introductorio sobre la computación cuántica, en español, a publicarse en los próximos meses. El libro está dirigido a los estudiantes de los últimos años de la carrera de ciencias de la computación, se centra en los aspectos algorítmico y de complejidad computacional, y destaca las similitudes y diferencias entre la computación probabilística, que es el modelo de computación clásica de referencia en el contexto de la complejidad computacional, y la computación cuántica. Esta última característica me parece sumamente ventajosa para la enseñanza de la computación cuántica, al explicitar los motivos por los que poseería mayor poder computacional que la computación clásica. En realidad, me parece ventajosa también para la enseñanza de la computación clásica, al clarificar el lugar que ocupan en ella los algoritmos probabilísticos, y para la enseñanza de la computación en general, al resaltar el papel que desempeña la aleatoriedad en la resolución algorítmica de los problemas.

Las notas que siguen contienen, en esencia, la introducción del libro referido, pero ampliada, sobre todo en lo que tiene que ver con los fundamentos teóricos de la información y las operaciones cuánticas. Por razones de espacio no incluyen algoritmos cuánticos representativos, que quedan para un siguiente artículo.

Sobre las razones para estudiar la computación cuántica

La razón fundamental para estudiar la computación cuántica es que para determinados problemas podría ofrecer una ventaja computacional muy significativa, en términos de la complejidad temporal, con respecto a la computación clásica. La evidencia más conocida en este sentido es el *algoritmo cuántico de Shor*, que resuelve el problema de factorización eficientemente, cuando los mejores algoritmos clásicos conocidos para factorizar requieren tiempo superpolinomial (la conjetura de que la factorización no admite algoritmos clásicos eficientes es aceptada por la mayoría de los investigadores, y constituye el fundamento de numerosos sistemas criptográficos). Otra evidencia muy conocida de ventaja computacional

temporal, menos espectacular, es el *algoritmo cuántico de Grover*, que acelera cuadráticamente las búsquedas no estructuradas en comparación con las resoluciones clásicas.

Un conjunto de problemas considerado en particular por los físicos para aprovechar el tipo de ventaja computacional referido es el de las simulaciones de los sistemas cuánticos, para avanzar en la comprensión y predicción del comportamiento de sistemas físicos complejos y de la mecánica cuántica en general. De hecho, la posibilidad de simular eficientemente sistemas cuánticos por parte de las computadoras cuánticas, cuya simulación mediante computadoras clásicas parece requerir una cantidad exponencial de recursos, constituyó la motivación inicial para el desarrollo de la computación cuántica.

Una segunda razón para estudiar la computación cuántica proviene de la teoría de la información cuántica. La información es un fenómeno físico, y por lo tanto resulta natural preguntarse cómo pueden almacenarse, transmitirse y procesarse los datos de los sistemas físicos que obedecen las leyes de la mecánica cuántica. Del estudio de estas cuestiones han surgido distintos protocolos de comunicación y aplicaciones criptográficas cuánticas, como así también importantes desarrollos de redes cuánticas.

Una de las aplicaciones de criptografía cuántica para destacar es la distribución cuántica de claves. La idea básica consiste en aprovechar el hecho de que en la mecánica cuántica, la medición de un sistema altera en general su estado. Esto permite detectar la presencia de un intruso que pretenda interceptar la transmisión de una clave, ya que su acción va a introducir perturbaciones en el canal de comunicación. Uno de los primeros protocolos de distribución cuántica de claves que se definieron fue el *protocolo BB84* de C. Bennett y G. Brassard. En la actualidad existen varios prototipos que se utilizan en aplicaciones reales a pequeña escala.

Otros dos motivos para encarar el estudio de la computación cuántica que cabe mencionar, corresponden a las teorías de la resolución de problemas y de la complejidad computacional. En el primer caso, porque la computación cuántica invita a desarrollar una *forma de pensar cuánticamente*, explotando nuevas posibilidades algorítmicas a partir de fenómenos característicos de la mecánica cuántica. Y en lo que tiene que ver con la teoría de la complejidad computacional, la idea es que tomando resultados de la computación cuántica podrían resolverse algunos problemas abiertos de la computación clásica. En este sentido, es razonable que la complejidad cuántica se analice con las mismas herramientas desarrolladas a lo largo de las últimas décadas para abordar la complejidad clásica: distintos modelos de computación, clases y jerarquías de complejidad, técnicas de prueba más de naturaleza estructural que con foco en problemas particulares, etc. Todo ello apuntando a relacionar componentes clásicos y cuánticos por medio de enunciados condicionales, de modo tal que de avances en un escenario se puedan lograr avances en el otro.

Sobre la física y las matemáticas necesarias

A diferencia de la computación clásica, basada en la física clásica, la computación cuántica se basa en los principios de la *mecánica cuántica*, teoría que desde hace más de un siglo constituye la descripción fundamental de los fenómenos físicos.

Informalmente, la mecánica cuántica puede pensarse como un sistema operativo sobre el que se ejecutan las distintas teorías físicas (a excepción de la relatividad general, cuya unificación con la mecánica cuántica continúa siendo uno de los principales problemas abiertos de la física teórica). Y desde un punto de vista matemático, especialmente útil para comprender las diferencias entre la computación clásica y la computación cuántica, puede interpretarse como una generalización de la teoría de las probabilidades, en la que las probabilidades de los posibles resultados de una medición no se asignan directamente sino que se obtienen como el cuadrado de los módulos de amplitudes complejas.

Afortunadamente, son muy pocos los conocimientos de física que se necesitan para comprender los principales resultados de la computación cuántica. En particular: los parámetros físicos de un sistema cuántico no se describen, en general, mediante valores definidos, sino por medio de una función de onda que asigna amplitudes a los distintos resultados posibles de la medición del sistema; recién tras su medición, el sistema adopta un estado compatible con el resultado obtenido (se dice que la función de onda *colapsa*); y esto no es un mero formalismo matemático, ya que las amplitudes pueden interferir entre sí efectivamente, dando lugar a efectos observables a través de experimentos.

Con respecto a las matemáticas que se requieren para estudiar la computación cuántica, el área principal es el *álgebra lineal*, en el marco de los *números complejos*. Más específicamente, los contenidos matemáticos que deben abordarse giran en torno a las nociones asociadas a los espacios vectoriales complejos de dimensión finita dotados de un producto interno, conocidos como *espacios de Hilbert*, y a los operadores lineales unitarios.

Una apropiada asimilación de esta base matemática facilita sobremanera la comprensión del cálculo subyacente en la algorítmica cuántica, dado que se pueden establecer distintas correspondencias entre las miradas algebraica y algorítmica. Por ejemplo:

- La correspondencia entre un vector complejo, expresado mediante una combinación lineal de los vectores de una base ortonormal de un espacio de Hilbert, y un estado cuántico.

- La correspondencia entre la proyección de un vector sobre otro, perteneciente a una base ortonormal, y la medición de un estado cuántico.

- La correspondencia entre una composición de operadores lineales unitarios y una secuencia de operaciones cuánticas, especificadas mediante matrices unitarias.

Sobre los fundamentos teóricos

En la computación cuántica, el análogo al bit de la computación clásica es el *bit cuántico* o *cúbit*. Como ocurre con el bit, un cúbit puede estar en el estado 0 o en el estado 1, pero a diferencia del bit, también puede estar en un estado de *superposición* de ambos, con una amplitud compleja asociada a cada uno.

Así como la implementación de un bit requiere algún componente que pueda estar en uno de dos estados (por ejemplo dos niveles de voltaje), la implementación de un cúbit también lo requiere, pero con el agregado de que debe contemplar además una superposición de ambos. Una opción se basa en el uso de electrones. Orbitando alrededor de un átomo, un electrón puede estar en un *estado fundamental* o en un *estado excitado*, y la iluminación del átomo, con una determinada energía y en un determinado período de tiempo, puede provocar que el electrón pase de un estado al otro o se quede *a mitad de camino* entre las dos alternativas.

Para introducir gradualmente los fundamentos teóricos principales de la información y las operaciones cuánticas, en lo que sigue consideramos primero el escenario con un solo cúbit y después el escenario con múltiples cúbits.

Escenario con un solo cúbit

Utilizando la *notación de Dirac*, o *notación bra-ket*, los estados 0 y 1 de un cúbit, identificados como *estados base*, se representan con los *kets* $|0\rangle$ y $|1\rangle$, respectivamente. Por su parte, un estado de superposición se representa mediante la combinación lineal:

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

donde los coeficientes α_i son amplitudes complejas que satisfacen la ecuación:

$$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

Cuando se *mide* un cúbit, su estado *colapsa* a $|0\rangle$ con probabilidad $|\alpha_0|^2$ o a $|1\rangle$ con probabilidad $|\alpha_1|^2$. De esta manera, la medición de un cúbit no revela sus amplitudes. Dicha información se mantiene *oculta*. Lo máximo que puede obtenerse es información estadística sobre la relación entre ellas.

Otra representación de un estado $\alpha_0|0\rangle + \alpha_1|1\rangle$ es el vector de amplitudes (α_0, α_1), más comúnmente utilizado en la forma de vector columna:

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

útil para los cálculos matriciales asociados a la operatoria cuántica. Y una tercera alternativa, gráfica, apropiada para la interpretación geométrica de los algoritmos cuánticos, es la Esfera de Bloch, esfera unitaria sobre cuya superficie cada punto, extremo de un vector unitario con

origen en su centro, representa un estado cuántico. En la figura 1 mostramos la Esfera de Bloch y la representación sobre su superficie de algunos estados cuánticos.

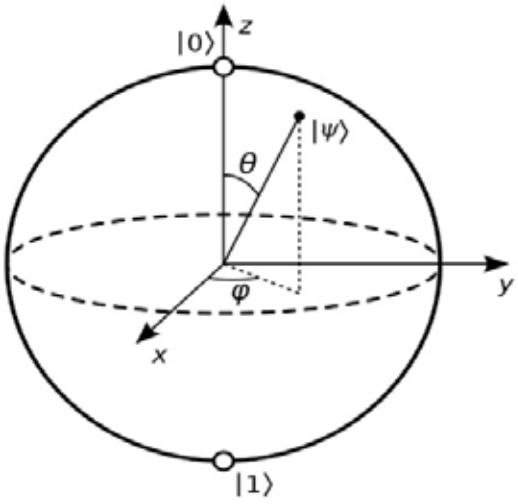


Figura 1. *La Esfera de Bloch y algunos estados cuánticos representados sobre su superficie.*

El estado $|0\rangle$ se representa mediante el extremo positivo del eje z de la esfera, es decir el punto $(0, 0, 1)$, o el polo norte tomando el eje z como el eje de rotación (es el eje estándar), mientras que el estado $|1\rangle$ se representa mediante el extremo negativo del eje z de la esfera, es decir el punto $(0, 0, -1)$, o el polo sur. Con respecto al estado $|\psi\rangle$, la combinación lineal que lo expresa es:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\,\mathrm{sen}\,\frac{\theta}{2}|1\rangle$$

con $0 \leq \theta \leq \pi$ y $0 \leq \varphi < 2\pi$, y el punto que lo representa es $(\mathrm{sen}\theta\cos\varphi,\ \mathrm{sen}\theta\,\mathrm{sen}\,\varphi,\ \cos\theta)$. La interpretación geométrica correspondiente es la siguiente: la probabilidad de que al medir un cúbit en el estado $|\psi\rangle$ se obtenga $|0\rangle$ es tanto mayor cuanto más cerca del polo norte se encuentre el punto que representa $|\psi\rangle$, y análogamente, la probabilidad de que se obtenga $|1\rangle$ es tanto mayor cuanto más cerca del polo sur se encuentre dicho punto. Más precisamente: al medir un cúbit en el estado $|\psi\rangle$, si $|\psi\rangle$ se representa por encima del ecuador de la Esfera de Bloch (la circunferencia punteada en la figura 1), es más probable que colapse a $|0\rangle$; si se representa por debajo del ecuador, es más probable que colapse a $|1\rangle$; y si se representa sobre el ecuador, las probabilidades de que colapse a $|0\rangle$ o $|1\rangle$ son iguales.

En particular, para representar gráficamente un estado cuántico con amplitudes reales (con las que ya se manifiestan las particularidades de la computación cuántica), basta el plano R^2, utilizando la circunferencia unitaria. En este caso, cada punto de la circunferencia, extremo de un vector unitario con origen en su centro, representa un estado cuántico. La figura 2 muestra la representación de algunos estados cuánticos con amplitudes reales.

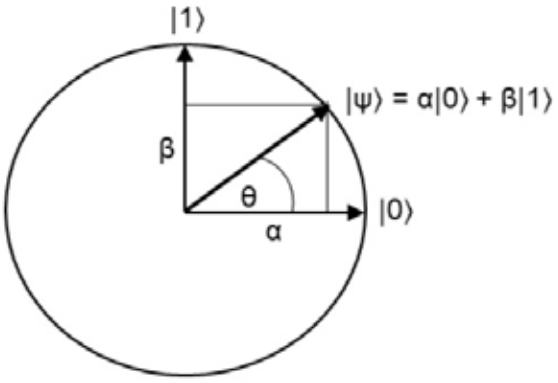


Figura 2. *Representación de algunos estados cuánticos con amplitudes reales.*

El estado $|0\rangle$ se representa con el extremo positivo del eje x de la circunferencia, es decir el punto $(1, 0)$; el estado $|1\rangle$, con el extremo positivo del eje y, es decir el punto $(0, 1)$; y el estado $|\psi\rangle$, con el extremo del vector unitario que se obtiene sumando α veces el vector unitario correspondiente a $|0\rangle$ y β veces el vector unitario correspondiente a $|1\rangle$. Siendo α y β dos números reales que satisfacen la igualdad:

$$\alpha^2 + \beta^2 = 1$$

existe un único ángulo θ, con $0 \leq \theta < 2\pi$, que cumple:

$$\alpha = \cos\theta \ , \ \beta = \text{sen}\theta$$

Así, $|\psi\rangle$ se puede expresar alternativamente como:

$$|\psi\rangle = \cos\theta\,|0\rangle + \text{sen}\theta\,|1\rangle$$

que satisface la interpretación geométrica mencionada anteriormente, basada en la relación entre los resultados de las mediciones y las distancias entre las representaciones, lo cual puede verificarse fácilmente.

Sea con amplitudes complejas o con amplitudes reales, la variedad de estados por los que puede pasar un cúbit es infinita. Más aún, el espacio de estados de un sistema de cúbits crece exponencialmente con su cantidad. Esta es la razón por la que el aprovechamiento de la información oculta en los cúbits, es decir la información previa a su medición, constituye la principal motivación de la algorítmica cuántica.

El conjunto $\{|0\rangle, |1\rangle\}$ que utilizamos para representar los estados de un cúbit y realizar mediciones sobre él constituye una *base de medición*, o directamente una *base*. Se la denomina *base* Z, por el eje de la Esfera de Bloch sobre el que se representan $|0\rangle$ y $|1\rangle$. También se la conoce como *base estándar* y *base computacional*. La base Z no es la única que existe. De hecho, cualquier par de estados cuánticos que se representan en la Esfera de Bloch mediante dos puntos opuestos constituye una base, lo que quiere decir que la cantidad de bases es infinita. En términos del álgebra lineal, dichos pares de estados cuánticos se corresponden con bases ortonormales del espacio de Hilbert C^2. Realizar

mediciones sobre un cúbit empleando distintas bases permite caracterizar su estado de una manera más completa.

Los estados de un cúbit evolucionan mediante *operaciones cuánticas*, denominadas en particular *puertas cuánticas* cuando los algoritmos cuánticos se describen mediante circuitos cuánticos (usaremos en general esta denominación). Toda puerta cuántica, digamos U, es *lineal* y *preserva la normalización de los estados cuánticos*, lo que quiere decir que aplicada sobre un cúbit en un estado $\alpha|0\rangle + \beta|1\rangle$:

- Se calcula de la siguiente manera: $U(\alpha|0\rangle + \beta|1\rangle) = \alpha\, U|0\rangle + \beta\, U|1\rangle$.
- Produce un estado $\gamma|0\rangle + \delta|1\rangle$ que cumple $|\gamma|^2 + |\delta|^2 = 1$.

En términos geométricos, las puertas cuánticas se corresponden con rotaciones sobre la superficie de la Esfera de Bloch, o sobre la circunferencia unitaria cuando las amplitudes son reales. Las puertas cuánticas de un cúbit más conocidas son:

Puerta I o puerta identidad. Su definición es:

$$I|0\rangle = |0\rangle \;\; , \;\; I|1\rangle = |1\rangle$$

Puerta X o puerta NOT. Su definición es:

$$X|0\rangle = |1\rangle \;\; , \;\; X|1\rangle = |0\rangle$$

es decir que actúa como la puerta lógica NOT considerando los estados base. En el caso de un estado de superposición, su efecto es el intercambio de sus amplitudes:

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle = \beta|0\rangle + \alpha|1\rangle$$

Puerta Y. Su definición es:

$$Y|0\rangle = i\,|1\rangle \;\; , \;\; Y|1\rangle = -\,i\,|0\rangle$$

Puerta Z. Su definición es:

$$Z|0\rangle = |0\rangle \;\; , \;\; Z|1\rangle = -\,|1\rangle$$

Las puertas X, Y y Z se conocen como *puertas de Pauli*. De acuerdo a su definición, cuando se aplican dos veces seguidas sobre un cúbit lo vuelven a su estado original, es decir que son *reversibles*. En realidad, todas las puertas cuánticas son reversibles, dado que se corresponden con los operadores lineales unitarios de los espacios de Hilbert. Por lo mismo, toda puerta cuántica cuenta con una puerta cuántica *inversa* que cancela su efecto, pudiendo ser incluso la misma, como es el caso de cada una de las puertas de Pauli. Otras puertas cuánticas muy comunes son:

Puerta S o puerta de fase. Su definición es:

$$S|0\rangle = |0\rangle \;\; , \;\; S|1\rangle = i\,|1\rangle$$

Puerta T. Su definición es:

$$T|0\rangle = |0\rangle \ , \ T|1\rangle = e^{i\pi/4}|1\rangle$$

Puerta $R_2(\theta)$. Su definición es:

$$R_2(\theta)|0\rangle = \cos\theta\,|0\rangle + \text{sen}\,\theta\,|1\rangle \ , \ R_2(\theta)|1\rangle = -\,\text{sen}\,\theta\,|0\rangle + \cos\theta\,|1\rangle$$

que se corresponde con una rotación de un ángulo θ sobre la circunferencia unitaria del plano R^2 (se aplica a partir de un estado cuántico con amplitudes reales). La última puerta cuántica que vamos a presentar desempeña un papel fundamental en la computación cuántica:

Puerta H o puerta de Hadamard. Su definición es:

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

es decir que a partir de un estado base produce un estado de superposición. Al igual que las puertas de Pauli, la puerta de Hadamard coincide con su puerta cuántica inversa. Veámoslo, por ejemplo, para el caso en que se aplica sobre el estado $|0\rangle$:

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

De esta forma, a partir de un estado de superposición, la puerta de Hadamard produce un estado base. Esto se explica por el hecho de que mientras las amplitudes correspondientes a $|0\rangle$ *interfieren* constructivamente, aumentando su probabilidad, las amplitudes correspondientes a $|1\rangle$ interfieren destructivamente, anulándose mutuamente. En la figura 3 representamos dicha situación.

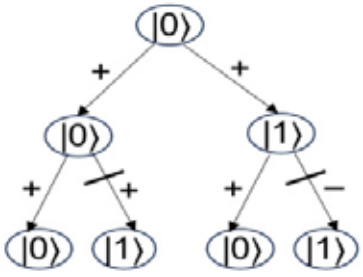


Figura 3. *Representación de dos aplicaciones seguidas de la puerta de Hadamard a partir de $|0\rangle$.*

Como muestra la figura 3, los dos caminos que conducen a $|0\rangle$ producen amplitudes positivas para $|0\rangle$, por lo que interfieren constructivamente. En cambio, los dos caminos que conducen a $|1\rangle$ producen amplitudes de signos opuestos para $|1\rangle$, por lo que interfieren destructivamente y se cancelan mutuamente.

Las puertas cuánticas se representan con matrices unitarias, lo que es natural teniendo en cuenta la correspondencia entre las puertas cuánticas y los operadores lineales unitarios y la relación entre estos y las matrices unitarias. De esta manera, las propiedades de la representación de las puertas cuánticas se pueden determinar a partir de las propiedades de los operadores lineales unitarios.

Para representar la aplicación de una puerta cuántica, como así también una secuencia de puertas cuánticas, se utiliza la multiplicación de matrices. Por un lado, la aplicación de una puerta cuántica sobre un cúbit en un estado $|\psi\rangle$ se representa mediante la multiplicación de una matriz de 2×2 que representa la puerta cuántica, por un vector columna de dimensión 2 que representa el estado $|\psi\rangle$, de la que se obtiene otro vector columna de dimensión 2 que representa el nuevo estado del cúbit. Por otro lado, una secuencia de puertas cuánticas $U_1, \ldots, U_k$ se representa mediante la multiplicación de matrices de 2×2 correspondientes $U_1, \ldots, U_k$ en el orden $U_k, \ldots, U_1$, la cual produce otra matriz de 2×2 que también representa una puerta cuántica.

Por ejemplo, en las igualdades siguientes mostramos la representación matricial de los estados $|0\rangle$ y $|1\rangle$, de las puertas X, Z y de Hadamard, y de la aplicación de dichas puertas cuánticas sobre ambos estados, incluyendo el resultado:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$Z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad Z|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

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

y en las siguientes, la representación de la secuencia de puertas cuánticas HXH, también con el resultado (la asociatividad de la multiplicación de matrices permite omitir paréntesis):

$$HXH = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}$$
$$\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Escenario con múltiples cúbits

De lo descripto antes se deriva que un registro cuántico de n cúbits puede encontrarse en un estado de superposición de hasta 2^n estados base. Por ejemplo, dos cúbits pueden estar en un estado base $|00\rangle$, $|01\rangle$, $|10\rangle$ o $|11\rangle$ o en un estado de superposición $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, empleando la notación de Dirac. Con vectores columna dichos estados se representan, respectivamente, del siguiente modo (la Esfera de Bloch no sirve en este escenario):

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

Siguiendo con un estado de dos cúbits, dado $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ se cumple:

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

y si se miden los cúbits, se obtiene el estado $|ij\rangle$ con probabilidad $|\alpha_{ij}|^2$, con i y j variando en el conjunto $\{0, 1\}$. La representación de los estados cuánticos y el comportamiento de las mediciones se pueden generalizar sin dificultad cuando se tienen tres, cuatro, o más cúbits.

Es con múltiples cúbits donde se aprecia realmente el poder computacional de la computación cuántica, al permitir procesar simultáneamente mucha información. Sin embargo, esta no es la diferencia fundamental con la computación clásica, dado que un registro clásico de n bits, procesado por un algoritmo probabilístico, también puede pensarse en un estado de superposición de hasta 2^n estados clásicos, cada uno con una probabilidad de ocurrencia específica. La diferencia esencial entre ambos paradigmas radica en la capacidad de los algoritmos cuánticos de producir interferencias constructivas y destructivas mediante un manejo apropiado de las amplitudes de los estados cuánticos, posibilidad con la que no se cuenta en la computación probabilística, donde los distintos caminos computacionales se excluyen mutuamente.

Al igual que la base $\{|0\rangle, |1\rangle\}$ para un cúbit, la base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ para dos cúbits se denomina *base Z*, y lo mismo ocurre con las bases para más cúbits cuyos estados se representan con cadenas de bits. Pero ahora, con múltiples cúbits, una medición puede abarcar todos los cúbits del registro cuántico considerado o parte de ellos. Por ejemplo, dados dos cúbits en el estado:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}|01\rangle + \frac{\sqrt{3}}{4}|10\rangle + \frac{1}{4}|11\rangle$$

midiendo los dos cúbits se obtiene $|00\rangle$ con probabilidad $|1/\sqrt{2}|^2 = 1/2$, colapsando el estado a $|00\rangle$, y midiendo sólo el primer cúbit se obtiene $|0\rangle$ con probabilidad $|1/\sqrt{2}|^2 + |1/2|^2 = 3/4$, colapsando el estado a:

$$\frac{2}{\sqrt{6}}|00\rangle + \frac{1}{\sqrt{3}}|01\rangle$$

Se cumple que la probabilidad de obtener, midiendo los dos cúbits, el estado $|xy\rangle$, coincide con la probabilidad de obtener el estado $|x\rangle$ después de medir el primer cúbit y de obtener el estado $|y\rangle$ después de medir el segundo cúbit. Lo mismo ocurre midiendo primero el segundo cúbit y luego el primer cúbit. Y esto vale para cualquier cantidad de cúbits y cualquier alternativa de medición.

Repasando y generalizando lo definido en términos de un solo cúbit:

- Las puertas cuánticas son lineales, preservan la normalización de los estados cuánticos y son reversibles.
- Una puerta U de k cúbits se representa mediante una matriz unitaria U de $2^k \times 2^k$.

- Tanto la aplicación de una puerta U sobre un conjunto de k cúbits, cuyo estado se representa con un vector columna de dimensión 2^k, como una secuencia de puertas cuánticas U_1, …, U_h, se representan mediante la multiplicación de matrices (cuando intervienen puertas cuánticas de distinta cantidad de cúbits, previamente deben igualarse las dimensiones de las matrices que las representan, empleando apropiadamente productos tensoriales con matrices identidad).

Las puertas cuánticas de más de un cúbit más conocidas son:

- *Puerta CNOT o puerta X controlada.* Su definición es:

$$CNOT|00\rangle = |00\rangle \ , \ CNOT|01\rangle = |01\rangle \ , CNOT|10\rangle = |11\rangle \ , \ CNOT|11\rangle = |10\rangle$$

es decir que actúa sobre dos cúbits aplicando una puerta X sobre el segundo cúbit sólo si el estado del primer cúbit es $|1\rangle$. El primer cúbit se identifica como el *cúbit de control*, y el segundo cúbit, como el *cúbit objetivo*. Así, la puerta CNOT sólo puede modificar el estado del cúbit objetivo, acción que se puede definir como el XOR entre dicho estado y el estado del cúbit de control (por eso a la puerta CNOT se la conoce también como el XOR cuántico).

A partir de un estado de superposición, la puerta CNOT intercambia las amplitudes de los estados $|10\rangle$ y $|11\rangle$:

$$\begin{aligned} &CNOT(\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle) \\ &= \alpha\, CNOT|00\rangle + \beta\, CNOT|01\rangle + \gamma\, CNOT|10\rangle + \delta\, CNOT|11\rangle \\ &= \alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \delta|10\rangle = \alpha|00\rangle + \beta|01\rangle + \delta|10\rangle + \gamma|11\rangle \end{aligned}$$

La puerta CNOT también se puede definir con el cúbit objetivo en primer lugar y el cúbit de control en segundo lugar. Y también se puede aplicar sobre cúbits no contiguos. En realidad, todas las puertas cuánticas de más de un cúbit cuentan con esta posibilidad.

Puerta CCNOT o puerta de Toffoli. Su definición es:

$$CCNOT|000\rangle = |000\rangle \ , \ CCNOT|001\rangle = |001\rangle \ , \ CCNOT|010\rangle = |010\rangle \ , \ CCNOT|011\rangle = |011\rangle$$
$$CCNOT|100\rangle = |100\rangle \ , \ CCNOT|101\rangle = |101\rangle \ , \ CCNOT|110\rangle = |111\rangle \ , \ CCNOT|111\rangle = |110\rangle$$

es decir que actúa sobre tres cúbits y su comportamiento es similar al de la puerta CNOT. En detalle, aplica una puerta X sobre el tercer cúbit, el cúbit objetivo, sólo si los estados del primer y segundo cúbit, los cúbits de control, son $|1\rangle$. Al igual también que la puerta CNOT, la puerta de Toffoli se puede definir alternativamente con operaciones lógicas: la modificación eventual del estado del cúbit objetivo se puede especificar mediante el XOR entre dicho estado y el AND de los estados de los cúbits de control, de lo que se deriva que la puerta de Toffoli computa de manera reversible el AND y el NAND de los estados de los cúbits de

control, según el estado del cúbit objetivo sea $|0\rangle$ o $|1\rangle$, respectivamente (por eso a la puerta de Toffoli se la conoce también como el *AND y el NAND cuánticos*). Cabe notar que como consecuencia de esto último, al ser la puerta lógica NAND una puerta lógica universal, se puede concluir que los algoritmos cuánticos pueden simular los algoritmos clásicos.

A partir de un estado de superposición, la puerta de Toffoli intercambia las amplitudes de los estados $|110\rangle$ y $|111\rangle$. Por ejemplo:

$$\text{CCNOT}\left(\frac{\sqrt{3}}{4}|100\rangle + \frac{\sqrt{5}}{4}|101\rangle + \frac{\sqrt{3}}{4}|110\rangle + \frac{\sqrt{5}}{4}|111\rangle\right)$$
$$= \frac{\sqrt{3}}{4}\text{CCNOT}|100\rangle + \frac{\sqrt{5}}{4}\text{CCNOT}|101\rangle + \frac{\sqrt{3}}{4}\text{CCNOT}|110\rangle + \frac{\sqrt{5}}{4}\text{CCNOT}|111\rangle$$
$$= \frac{\sqrt{3}}{4}|100\rangle + \frac{\sqrt{5}}{4}|101\rangle + \frac{\sqrt{3}}{4}|111\rangle + \frac{\sqrt{5}}{4}|110\rangle = \frac{\sqrt{3}}{4}|100\rangle + \frac{\sqrt{5}}{4}|101\rangle + \frac{\sqrt{5}}{4}|110\rangle + \frac{\sqrt{3}}{4}|111\rangle$$

La ubicación de los cúbits de control y el cúbit objetivo puede ser variada, característica en verdad de toda puerta cuántica controlada con cualquier cantidad de cúbits de control y cúbits objetivo.

Puerta SWAP. Su definición es:

$$\text{SWAP}|00\rangle = |00\rangle \ , \ \text{SWAP}|01\rangle = |10\rangle \ , \ \text{SWAP}|10\rangle = |01\rangle \ , \ \text{SWAP}|11\rangle = |11\rangle$$

es decir que actúa sobre dos cúbits intercambiando sus estados. En el caso de un estado de superposición, la puerta SWAP intercambia las amplitudes de los estados $|01\rangle$ y $|10\rangle$.

Puerta U controlada. A partir de cualquier puerta cuántica U se puede definir una puerta cuántica controlada, que intuitivamente se asocia a la instrucción condicional de la computación clásica. La puerta U controlada más simple es CU, de un cúbit de control y un cúbit objetivo (por ejemplo, CZ, CH, etc). Se define del siguiente modo:

$$\text{CU}|00\rangle = |00\rangle \ , \ \text{CU}|01\rangle = |01\rangle \ , \ \text{CU}|10\rangle = |1\rangle\text{U}|0\rangle \ , \ \text{CU}|11\rangle = |1\rangle\text{U}|1\rangle$$

El caso más general es C^kU, con $k \geq 1$, de uno o más cúbits de control y uno o más cúbits objetivo. Un ejemplo muy conocido de puerta cuántica controlada de un cúbit de control y dos cúbits objetivo es la *puerta de Fredkin (o puerta CSWAP, o puerta SWAP controlada)*, definida de la siguiente manera:

$$\text{CSWAP}|000\rangle = |000\rangle \ , \ \text{CSWAP}|001\rangle = |001\rangle \ , \ \text{CSWAP}|010\rangle = |010\rangle \ , \ \text{CSWAP}|011\rangle = |011\rangle$$
$$\text{CSWAP}|100\rangle = |100\rangle \ , \ \text{CSWAP}|101\rangle = |110\rangle \ , \ \text{CSWAP}|110\rangle = |101\rangle \ , \ \text{CSWAP}|111\rangle = |111\rangle$$

o sea que aplica una puerta SWAP sobre los dos cúbits objetivo sólo si el cúbit de control es $|1\rangle$.

Como ejemplo de representación matricial en el escenario con múltiples cúbits, en las siguientes igualdades se muestra la aplicación de la puerta CNOT a partir de cada uno de los estados de base de dos cúbits:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Sobre los modelos computacionales

La aplicación de las operaciones cuánticas se organiza a través de un *modelo computacional cuántico*. Los principales modelos computacionales cuánticos son la *máquina de Turing cuántica* y el *circuito cuántico*, análogos, respectivamente, a la máquina de Turing clásica y al circuito booleano. Las máquinas de Turing cuánticas se utilizan esencialmente en el área de la complejidad computacional, en tanto que los circuitos cuánticos constituyen el modelo computacional habitual para describir los algoritmos cuánticos. En las próximas dos subsecciones describimos las características principales de ambos modelos.

La máquina de Turing cuántica

Las especificaciones iniciales de la máquina de Turing cuántica (MTC) aparecieron en trabajos de P. Benioff y D. Deutsch entre los años 1980 y 1985, y su formalización definitiva, en artículos de D. Deutsch y R. Jozsa y de E. Bernstein y U. Vazirani casi una década más tarde (años 1992 y 1993). Las primeras publicaciones planteaban la cuestión de si la unitariedad impuesta por la mecánica cuántica constituía una limitación. La reversibilidad por sí sola no lo era, como había demostrado C. Bennett a comienzos de la década de 1970, describiendo cómo simular de manera eficiente una máquina de Turing determinística (MTD) irreversible con una MTD reversible. Pronto se determinó que la unitariedad no implicaba limitación alguna, consecuencia de lo cual quedó establecido que las MTC eran al menos tan poderosas computacionalmente como las máquinas de Turing probabilísticas (MTP), las máquinas de Turing clásicas más generales.

En el caso más general, una MTC puede efectuar mediciones intermedias y finales y con bases arbitrarias, y puede manejar estados *puros* y *mixtos*. Precisando esto último: todos los estados cuánticos que hemos utilizado se denominan *estados puros*, y constituyen un caso particular de los estados cuánticos más generales, denominados *estados mixtos*. Un estado mixto es un estado cuántico probabilístico que representa una distribución de probabilidades sobre estados puros (se puede establecer una analogía entre los estados puros y mixtos de la computación cuántica y los estados determinísticos y probabilísticos de la computación clásica). Se prueba que sin perder poder computacional, a una MTC le alcanza con manejar únicamente estados puros, y realizar mediciones sólo al final y con la base Z. En particular, cuando el algoritmo implementado resuelve un problema de decisión, la obtención de un resultado $|1\rangle$ se interpreta como una aceptación, y la obtención de un resultado $|0\rangle$, como un rechazo de la cadena de entrada procesada.

Como ocurre con las MTD y las MTP, existen MTC *universales eficientes*, en particular MTC con operaciones determinísticas reversibles más una única operación cuántica, identificada comúnmente como un *lanzamiento de moneda cuántica*, capaces de simular cualquier MTC M con un error $\varepsilon > 0$ en tiempo polinomial con respecto al tiempo de M, el tamaño de las cadenas de entrada y el valor $1/\varepsilon$. En lo que hace específicamente a similitudes entre las MTC y las MTP:

- Las MTC pueden verse como una extensión de las MTP, con transiciones determinadas por amplitudes en lugar de probabilidades y con computaciones reversibles.
- Tanto las MTC como las MTP se suelen ejecutar varias veces, adoptando como respuesta la más frecuente y aumentando así la confianza en el resultado.
- Los dos modelos son *discretos,* en el sentido de que las amplitudes (en el caso de las MTC) y las probabilidades (en el caso de las MTP) correspondientes a sus transiciones son eficientemente computables. En particular, se demuestra que para ejecutar una computación cuántica de T pasos con un error acotado por una constante, alcanza con representar las amplitudes con $O(\log T)$ bits de precisión.

Por otro lado, en lo que hace a las diferencias entre las MTC y las MTP, la más importante está dada por la operación con amplitudes de las primeras frente a la operación con probabilidades de las segundas: en una computación probabilística, la probabilidad de pasar de una configuración a otra es la suma de las probabilidades asociadas a todos los caminos posibles entre ambas, mientras que en una computación cuántica ocurre lo mismo con las amplitudes pero no con las probabilidades. Este contraste sería la razón del mayor poder computacional de las MTC.

El circuito cuántico

El circuito cuántico fue introducido por A. Yao en una publicación de 1993, siendo su antecedente más cercano las *redes computacionales cuánticas* definidas a fines de la década anterior por D. Deutsch. El propósito era constituir en la computación cuántica un modelo computacional análogo al circuito booleano de la computación clásica, teniendo en cuenta

su importante aporte al estudio de la complejidad computacional. Con respecto a esto último, en su mismo trabajo fundacional A. Yao probó que las funciones computables eficientemente con MTC también pueden computarse eficientemente con circuitos cuánticos: probó que dichas funciones se pueden computar con *circuitos cuánticos polinomiales*, es decir con circuitos compuestos por un número polinomial de puertas cuánticas en relación al tamaño de sus cadenas de entrada.

Las características fundamentales de los circuitos cuánticos son las mismas que mencionamos de las MTC. En efecto, los circuitos cuánticos tienen computaciones reversibles. Las amplitudes son eficientemente computables. Existe un modelo universal eficiente, en este caso compuesto por circuitos cuánticos basados en *conjuntos universales de puertas cuánticas*. Se manejan estados cuánticos puros y mixtos, pudiendo omitirse los últimos sin que se pierda poder computacional. Y las mediciones pueden ser tanto intermedias como finales y en distintas bases, pero pueden utilizarse sólo mediciones al final y con la base Z también sin alterar el poder computacional.

Otra similitud entre las MTC y los circuitos cuánticos vinculada con la complejidad computacional y los modelos clásicos análogos es la siguiente: así como las MTC tienen al menos el mismo poder computacional que las máquinas de Turing clásicas, los circuitos cuánticos tienen al menos el mismo poder computacional que los circuitos booleanos. Esta última relación se cumple por la posibilidad de transformar toda puerta lógica irreversible en una puerta lógica reversible equivalente de tamaño no mayor que un factor polinomial, y así también en una puerta cuántica equivalente con la misma característica de tamaño. En términos de circuitos: todo circuito booleano se puede transformar en un circuito cuántico equivalente a lo sumo polinomialmente mayor.

La figura 4 muestra un ejemplo de un circuito cuántico.

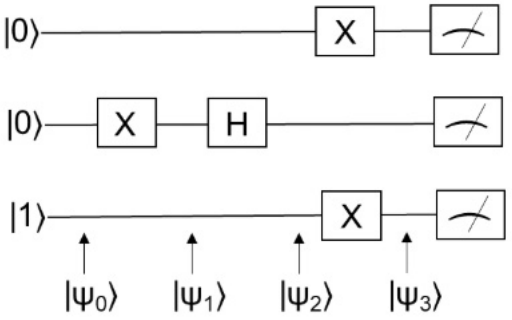


Figura 4. *Un ejemplo de un circuito cuántico.*

Con un registro cuántico de tres cúbits *preparado* en el estado $|\psi_0\rangle = |001\rangle$, el circuito cuántico de la figura 4 primero aplica una puerta X sobre el segundo cúbit, luego una puerta de Hadamard sobre el mismo cúbit, luego una puerta X sobre el primer cúbit y otra puerta X sobre el tercer cúbit, y finalmente mide los tres cúbits (la caja con el símbolo de un medidor analógico representa la medición de un cúbit). Se puede comprobar que los distintos

estados por los que pasa el circuito cuántico, identificados debajo de la fila inferior como se suele hacer, son:

$$|\psi_0\rangle = |001\rangle \ , \ |\psi_1\rangle = |011\rangle \ , \ |\psi_2\rangle = \frac{1}{\sqrt{2}} (|001\rangle - |011\rangle) \ , \ |\psi_3\rangle = \frac{1}{\sqrt{2}} (|100\rangle - |110\rangle)$$

y por lo tanto, tras la medición final se obtiene el estado $|100\rangle$ o el estado $|110\rangle$ con probabilidad $1/2$ en cada caso.

La representación gráfica de un circuito cuántico se interpreta de izquierda a derecha y de arriba hacia abajo (algunos autores utilizan la interpretación de abajo hacia arriba). En la primera columna se disponen los cúbits del registro cuántico preparados en sus estados iniciales, siendo entonces el cúbit superior el más significativo. Las filas representan las evoluciones de los cúbits, mediante cajas nombradas apropiadamente que corresponden a las puertas cuánticas utilizadas o a las mediciones finales.

A pesar de su simplicidad, el ejemplo anterior sirve para identificar las tres etapas que atraviesan las computaciones de los circuitos cuánticos, asumiendo mediciones sólo al final:

1. *Preparación*. Se prepara el estado inicial del registro cuántico. En general, si el registro cuántico tiene m cúbits, el estado inicial adopta la forma $|x\rangle|0^{m-n}\rangle$, donde $x \in \{0, 1\}^n$ es la cadena de entrada y los últimos $m - n$ cúbits en $|0\rangle$ son cúbits para cálculos auxiliares, conocidos como cúbits *ancilla*.

2. *Evolución.* Se aplican las puertas cuánticas una tras otra, de acuerdo a un orden establecido.

3. *Medición.* Se miden algunos o todos los cúbits del registro cuántico. Si en particular resuelve un problema de decisión, el circuito cuántico mide el primer cúbit y acepta o rechaza la cadena de entrada x según obtenga $|1\rangle$ o $|0\rangle$, respectivamente.

Para ilustrar cómo se representa una puerta cuántica controlada, en la figura 5 mostramos un fragmento de un circuito cuántico en el que a la aplicación de una puerta de Hadamard le sigue la aplicación de una puerta CNOT.

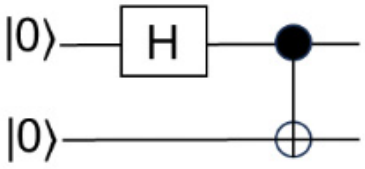


Figura 5. *Fragmento de un circuito cuántico con una puerta de Hadamard seguida de una puerta CNOT.*

Los componentes que integran la representación de una puerta cuántica de más de un cúbit se unen con líneas verticales. Con respecto, en particular, a la puerta CNOT, el círculo negro corresponde al cúbit de control y el círculo blanco, al cúbit objetivo (por lo dicho antes, el círculo negro no tiene que estar necesariamente en la parte superior). El lector puede comprobar sin dificultad que el estado producido por la secuencia representada en la figura 5 es:

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

Al igual que en el caso de las MTC, las ejecuciones de los circuitos cuánticos se suelen iterar varias veces para mejorar la probabilidad de obtener un resultado correcto. Asimismo, como en los circuitos booleanos, en los circuitos cuánticos se aplica el concepto de *familia uniforme*, que permite procesar cadenas de cualquier tamaño y considerar todos los circuitos cuánticos de la familia como parte de un único algoritmo.

Como ocurre con el repertorio de puertas lógicas de los circuitos booleanos, el repertorio de puertas cuánticas de los circuitos cuánticos se puede restringir a *conjuntos universales de puertas cuánticas*, que en este caso permiten simular, con un error arbitrario, cualquier puerta cuántica. Formalmente, un conjunto C de puertas cuánticas es un *conjunto universal*, si para toda puerta cuántica U de k cúbits, representada con una matriz U de $2^k \times 2^k$, y para todo error $\varepsilon > 0$, existe una secuencia de h puertas cuánticas $U_1, \ldots, U_h$ de C, representadas, respectivamente, con matrices $U_1, \ldots, U_h$ (cada una expandida apropiadamente hasta alcanzar la dimensión $2^k \times 2^k$), tal que para todo i, j entre 1 y 2^k se cumple:

$$| U_{ij} - (U_h \ldots U_1)_{ij} | \leq \varepsilon$$

Un conjunto universal de puertas cuánticas tiene que poder generar, naturalmente, superposiciones y entrelazamientos, pero esta capacidad por sí sola no asegura la universalidad. Por ejemplo, se prueba que las puertas cuánticas del *grupo de Clifford*, que son las puertas S, de Hadamard y CNOT, en conjunto tienen dicha capacidad, pero los circuitos cuánticos construidos exclusivamente con ellas pueden simularse de manera clásica.

Algunos de los conjuntos universales de puertas cuánticas más conocidos son:

- {todas las puertas cuánticas de un cúbit, CNOT}
- {T, puerta de Hadamard, CNOT}
- {S, puerta de Hadamard, puerta de Toffoli}
- {puerta de Hadamard, puerta de Toffoli}

La universalidad del último conjunto de puertas cuánticas revela la importancia de la puerta de Hadamard en la computación cuántica: siendo la puerta lógica de Toffoli universal para la computación clásica reversible, podemos concluir que la puerta de Hadamard es lo único que se necesita agregar a un conjunto universal de puertas lógicas reversibles para obtener un conjunto universal de puertas cuánticas.

La universalidad de dicho conjunto revela también que todo circuito cuántico puede simularse por medio de otro con puertas cuánticas definidas únicamente con números reales. Para ello basta incorporar en el circuito cuántico simulador un cúbit auxiliar, encargado de indicar en todo momento si se está procesando la parte real o la parte imaginaria de una amplitud.

Además del objetivo teórico de determinar por qué las computadoras cuánticas tendrían mayor poder computacional que las computadoras clásicas, el manejo de distintos

conjuntos universales de puertas cuánticas tiene varios objetivos prácticos: recurrir a las puertas cuánticas más convenientes según la tarea que se quiera realizar (por ejemplo, un diseño teórico), aprovechar los recursos disponibles (por ejemplo, una computadora cuántica con un repertorio específico de operaciones), priorizar propiedades que deban cumplirse (por ejemplo, la tolerancia a fallas), etc. Este ejercicio es comparable al de la elección, en la programación clásica, del lenguaje más adecuado de acuerdo al problema tratado.

Siguiendo con la analogía entre los lenguajes de programación y los conjuntos universales de puertas cuánticas, sería deseable que así como las transformaciones entre los programas escritos en distintos lenguajes de programación habituales de la computación clásica pueden realizarse eficientemente, también resultaran eficientes las transformaciones entre los conjuntos universales de puertas cuánticas. Afortunadamente esto se cumple, según el *teorema de Solovay-Kitaev*. Formulado por R. Solovay en 1995 y difundido por A. Kitaev en 1997, el teorema establece lo siguiente: dado un conjunto universal finito de puertas cuánticas, toda puerta cuántica puede simularse con un error $\varepsilon > 0$ por medio de una secuencia de $O((\log(1/\varepsilon))^c)$ puertas cuánticas de dicho conjunto, para alguna constante positiva c. De esta forma, todo circuito cuántico puede simularse eficientemente con un error arbitrario por otro, definido a partir de un conjunto universal finito de puertas cuánticas, lo que formaliza la existencia de un modelo universal eficiente en el marco de los circuitos cuánticos.

Sobre los algoritmos cuánticos

Podría pensarse que por el paralelismo asociado a las superposiciones, un algoritmo cuántico siempre aventajará a un algoritmo clásico, en el sentido de la complejidad temporal, para resolver un problema. Sin embargo esto no ocurre en general, sino sólo en el caso de determinados problemas con estructuras específicas. Sucede que aunque a lo largo de una computación puede existir un gran número de estados base superpuestos, y por lo tanto múltiples resultados posibles, tras la medición final se produce un único resultado, y así no toda la información obtenida puede recuperarse. Por eso, un aspecto central del diseño de los algoritmos cuánticos es el manejo de las amplitudes, para lograr interferencias deseadas. Como ya fue dicho, la idea es generar, antes de la medición final, interferencias constructivas y destructivas que aumenten la probabilidad de obtener un resultado correcto y disminuyan la probabilidad de obtener un resultado incorrecto.

Otra característica fundamental de la computación cuántica, sin equivalente en la computación clásica, es la generación de estados *entrelazados*. Un estado entrelazado de dos o más cúbits es aquel que no puede describirse únicamente a partir de los estados de los cúbits considerados aisladamente. Una consecuencia de esta característica es que los resultados de las mediciones parciales, es decir las mediciones realizadas sobre un subconjunto de cúbits, presentan correlaciones imposibles de reproducir clásicamente. Un ejemplo de entrelazamiento lo constituye el siguiente estado cuántico (uno de los cuatro *estados de Bell*), que ya mostramos anteriormente:

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

Notar que al medir uno de los cúbits, si se obtiene $|0\rangle$ se puede asegurar que al medir el otro también se obtendrá $|0\rangle$, y si se obtiene $|1\rangle$, que la medición del otro producirá $|1\rangle$.

El entrelazamiento desempeña un papel central en numerosas aplicaciones cuánticas, entre ellas la comunicación cuántica y la corrección de errores cuánticos. Los estados cuánticos no entrelazados se conocen como estados *separables*. Es fácil verificar que si todos los estados cuánticos fueran separables, los algoritmos cuánticos podrían simularse eficientemente por medio de algoritmos clásicos.

El entrelazamiento protagoniza la evolución de la mecánica cuántica casi desde su consolidación a fines de la década de 1920. En la década de 1930 se planteó un experimento mental, la *paradoja EPR* (por sus autores, A. Einstein, B. Podolsky y N. Rosen), para mostrar que la novedosa teoría física era *incompleta*: asumiendo la inexistencia de las influencias instantáneas a distancia (*localidad*), las fuertes correlaciones entre sistemas entrelazados sugerían la existencia de propiedades físicas predefinidas (*realismo*), no incluidas en la teoría. En la década de 1960, para analizar esta cuestión, J. Bell propuso un test basado en una ecuación, la *desigualdad de Bell*: si el test reflejaba una violación de dicha desigualdad, entonces las correlaciones observadas no podían explicarse mediante una teoría que satisficiera simultáneamente la localidad y el realismo, tal como predecía la mecánica cuántica. Desde entonces se llevaron a la práctica varios tests basados en el test de Bell, mostrando todos ellos violaciones de la desigualdad, y por lo tanto confirmando las predicciones de la mecánica cuántica. En los últimos años se han logrado importantes progresos en la comprensión del entrelazamiento, lo que ha permitido su uso en varias aplicaciones de la computación cuántica, entre otras disciplinas.

Como contrapartida, en la computación cuántica no es posible copiar arbitrariamente estados cuánticos, que es una capacidad elemental en la computación clásica. Más precisamente, no es posible clonar un estado desconocido. Este resultado se conoce como *teorema de no clonación,* y constituye una diferencia fundamental entre la computación clásica y la computación cuántica. El teorema fue formulado en 1982, por W. Wootters y W. Zurek e independientemente por D. Dieks.

Dicha limitación impone restricciones sobre las operaciones cuánticas que pueden realizarse, pero no parece alterar el poder computacional de la computación cuántica. Más aún, la misma restricción constituye una ventaja para las comunicaciones seguras: dado que al medir, un intruso puede ser detectado por la perturbación que produce, una alternativa que tiene para obtener información es copiar estados cuánticos, pero en general lo máximo que puede lograr en este sentido son copias imperfectas.

En la actualidad se conocen relativamente pocos algoritmos cuánticos que superen de manera sustancial a sus contrapartes clásicas, en términos de la complejidad temporal. Esta situación puede atribuirse no sólo a la dificultad inherente al diseño de algoritmos cuánticos, sino también al hecho de que nuestra intuición para el diseño de algoritmos se ha forjado durante décadas en el marco de la computación clásica. A ello se le suma que el diseño de

nuevos algoritmos cuánticos suele estar guiado por la expectativa de mejorar la eficiencia del mejor algoritmo clásico conocido para el problema en cuestión. Tres familias de algoritmos cuánticos que se destacan son:

- *Los algoritmos basados en la transformada cuántica de Fourier*. La transformada de Fourier es una herramienta matemática que permite cambiar la representación de la información, lo que facilita la resolución de determinados problemas. Su versión cuántica constituye el núcleo de muchos algoritmos, que en algunos casos proporcionan una aceleración muy significativa con respecto a los mejores algoritmos clásicos conocidos, como el *algoritmo de Shor*.

- *Los algoritmos de búsqueda no estructurada*. El ejemplo más representativo es el *algoritmo de Grover*, de aceleración cuadrática con respecto a los mejores algoritmos clásicos conocidos. La importancia de estos algoritmos cuánticos radica, sobre todo, en el hecho de que el esquema en el que se basan posee un ámbito de aplicación muy amplio.

- *Los algoritmos de simulación de sistemas cuánticos*. En algunos casos simulan de manera eficiente sistemas cuánticos para los que sólo se conocen simulaciones clásicas que requieren tiempo exponencial.

Sobre la complejidad cuántica

Se cumple que toda computación cuántica puede simularse clásicamente con un sobrecosto temporal exponencial, por lo que la computación cuántica no contradice la *tesis de Church-Turing* (las MTD pueden realizar todos los procedimientos de cálculo efectivo) ni tampoco la *tesis física de Church-Turing* (las MTD pueden simular todos los modelos computacionales físicamente realizables) aunque sí podría contradecir la *tesis fuerte de Church-Turing* (las simulaciones mencionadas en la tesis física por parte de las MTD son eficientes).

La clase de complejidad de los problemas que se resuelven con algoritmos cuánticos eficientes se denomina *BQP*. Es decir que BQP es la clase de complejidad análoga a la clase P de la complejidad determinística y a la clase BPP de la complejidad probabilística, teniendo en cuenta que la conjetura más aceptada es P = BPP, y que la computación probabilística es el modelo clásico de referencia en el contexto de la complejidad computacional.

Al igual que lo que ocurre en la clase BPP, los algoritmos relacionados con la clase BQP son de error acotado, es decir que pueden responder erróneamente pero con una probabilidad de error acotada. Un umbral habitual es 1/3, que de todos modos se puede reducir de forma exponencial luego de algunas repeticiones independientes y adoptando el resultado más frecuente.

Se demuestra que la clase BPP está incluida en la clase BQP. Intuitivamente, existe una operación cuántica que permite simular un lanzamiento de moneda. También se demuestra la inclusión de BQP en la clase PSPACE. Históricamente, este fue el primer resultado

trascendente de la complejidad cuántica. Actualmente se conocen cotas superiores de BQP más precisas, como la clase PP.

No se sabe si dichas inclusiones son estrictas. En particular, que no se haya podido demostrar que existen problemas en BQP fuera de BPP, es decir que la computación cuántica tiene mayor poder computacional que la computación clásica, a pesar de la evidencia suministrada por algoritmos cuánticos como el algoritmo de Shor, se puede explicar entre otros motivos por el hecho de que P ≠ BQP implica P ≠ PSPACE, resultado este último que constituye un problema abierto de la complejidad clásica desde hace varias décadas.

Una de las principales razones para conjeturar que la clase BPP está incluida estrictamente en la clase BQP es la inexistencia, hasta el presente, de algoritmos probabilísticos eficientes para resolver la factorización y el logaritmo discreto, contrastando con la existencia de los algoritmos cuánticos eficientes de Shor para ambos problemas. Es cierto que esta evidencia no es cuantitativamente tan fuerte como, por ejemplo, la de que BPP no incluye a la clase NP. NP contiene miles de problemas que desde hace décadas se resisten a ser resueltos eficientemente por medio de algoritmos probabilísticos. Pero por otro lado, considerando en particular el problema de factorización, la evidencia se compensa cualitativamente por el hecho de que la factorización es uno de los problemas más antiguos y estudiados.

Tampoco se sabe cómo se relaciona BQP con NP. La búsqueda cuántica en el marco de un espacio de soluciones no estructurado no conduce a la inclusión de NP en BQP, pero esto no quiere decir que los problemas de NP no posean alguna estructura que permita resolverlos eficientemente mediante un algoritmo cuántico. De todos modos se cree que BQP no contiene problemas NP-completos, y por lo tanto que no incluye a NP. Una de las evidencias más importantes la constituye el algoritmo de Grover. Otra es que se prueba que si existe un lenguaje NP-completo en BQP, entonces la jerarquía polinomial PH colapsa, cuando la conjetura más aceptada es que no lo hace.

A propósito, no se sabe cómo se relaciona BQP con PH, mientras que se prueba que BPP $\subseteq$ PH. La conjetura más aceptada es que PH no incluye a BQP, y así, como NP $\subseteq$ PH, las clases BQP y NP serían incomparables. Otras clases de complejidad cuántica consideradas habitualmente son *QMA*, la contraparte cuántica de *NP y MA, y QIP,* la contraparte cuántica de *IP*.

La complejidad cuántica se estudia en términos de las MTC y también en términos de los circuitos cuánticos, modelos de poder computacional equivalente. Disponer de ambos modelos no sólo permite formular los enunciados de la manera más conveniente según el contexto, sino que además, a través de sus relaciones, podría facilitar el descubrimiento de nuevos resultados, lo mismo que se plantea en la computación clásica con los modelos análogos. La figura 6 muestra la relación de la clase BQP con las principales clases de complejidad clásica.

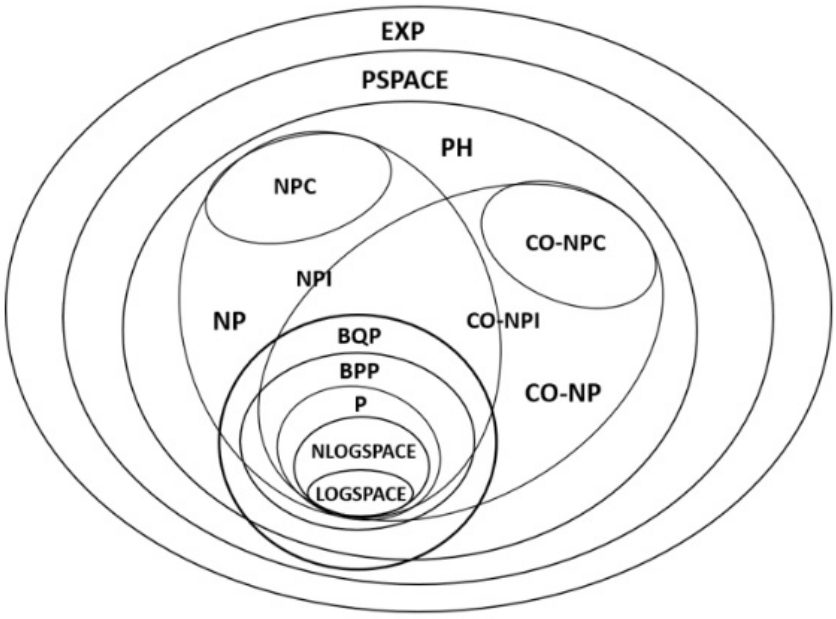


Figura 6. *La clase BQP y su relación con las principales clases de la jerarquía de la complejidad clásica.*

Sobre los orígenes y la evolución de la computación cuántica

La computación cuántica surgió a partir de la idea de estudiar la computación como un proceso físico. Entre las contribuciones fundamentales se encuentran el *principio de Landauer* (1961), mediante el cual R. Landauer relacionó la información con la termodinámica, y el trabajo de C. Bennett (1973), inspirado en dicho principio, en el que demostró que toda computación determinística puede realizarse de forma reversible con un sobrecosto temporal polinomial.

A partir de estas bases conceptuales, P. Benioff presentó el primer modelo cuántico de una máquina de Turing (1980), R. Feynman propuso utilizar computadoras cuánticas para simular eficientemente sistemas cuánticos (1982), y D. Deutsch introdujo el concepto de máquina de Turing cuántica universal (1985). Estas publicaciones establecieron los cimientos teóricos de la computación cuántica.

En la década siguiente, la teoría de la computación cuántica alcanzó una notable madurez. A. Yao formalizó el modelo de los circuitos cuánticos y probó la equivalencia entre su poder computacional y el de las máquinas de Turing cuánticas (1993). E. Bernstein y U. Vazirani desarrollaron el marco formal de la complejidad cuántica (1993). Los algoritmos de P. Shor (1994) y L. Grover (1996) mostraron ventajas concretas de la computación cuántica frente a la computación clásica para determinados problemas. Paralelamente, surgió la teoría de la información cuántica, impulsando desarrollos como la criptografía cuántica, la

teleportación cuántica y la corrección de errores cuánticos. Con respecto a esta última línea de trabajo en particular, los códigos de corrección de errores cuánticos de P. Shor, A. Steane y otros investigadores, y los *teoremas del umbral* (1995-1998), constituyeron un avance decisivo para la computación cuántica, al demostrarse que los efectos del ruido (alteraciones de los estados y las operaciones cuánticas causadas por las interacciones con el entorno o por imperfecciones de los dispositivos cuánticos) no representan un obstáculo insalvable para la construcción de computadoras cuánticas escalables.

Desde entonces, la computación cuántica ha mostrado un desarrollo continuo tanto desde el punto de vista teórico como experimental. Junto con la profundización en sus fundamentos y el descubrimiento de nuevos algoritmos, han surgido distintas líneas de investigación orientadas a hacer posible la construcción y el uso práctico de las computadoras cuánticas. Entre ellas:

- *La implementación física de cúbits.* En la actualidad existen diversas tecnologías, como cúbits superconductores, iones atrapados, átomos neutros, fotones y espines, cada una con ventajas y limitaciones con respecto a la escalabilidad, fidelidad de las operaciones y resistencia al ruido.

- *La construcción de computadoras cuánticas.* Entre los factores que impulsan su desarrollo se encuentra la progresiva ralentización de la *ley de Moore*, según la cual el número de transistores en un circuito integrado se duplica aproximadamente cada dos años, tendencia que durante décadas se tradujo en un aumento sostenido de la capacidad de cómputo. En la actualidad ya existen procesadores cuánticos con miles de cúbits físicos, pero la construcción de computadoras cuánticas universales, tolerantes a fallas y de gran escala, continúa siendo un importante desafío. La principal dificultad radica en la elevada sensibilidad de los sistemas cuánticos al ruido. Esta situación recuerda a la de los modelos analógicos, cuya potencial ventaja computacional se ve limitada por la acumulación de errores producidos por las imperfecciones físicas. Sin embargo, la corrección de errores cuánticos y la computación cuántica tolerante a fallas muestran que la computación cuántica presenta una diferencia fundamental comparada con dichos modelos. En efecto, los teoremas del umbral, ya mencionados, establecen que es posible realizar computaciones cuánticas arbitrariamente largas con una tasa de error controlada, siempre que las tasas de error de los componentes físicos se mantengan por debajo de determinados valores.

- *El desarrollo de lenguajes de programación, compiladores y plataformas de software para computadoras cuánticas*. Algunas de las herramientas más difundidas hoy día son Qiskit, Cirq, Q#, PennyLane y CUDA-Q. Estas herramientas permiten diseñar, optimizar, simular y ejecutar algoritmos cuánticos sobre distintos tipos de hardware.

- *La verificación y validación de programas y dispositivos cuánticos*. Se destacan actividades como la verificación formal de algoritmos y protocolos cuánticos, la certificación y el *benchmarking* de procesadores cuánticos, y distintos métodos para verificar resultados obtenidos mediante computadoras cuánticas cuando no se pueden reproducir eficientemente por medios clásicos.

Todo estos temas constituyen áreas de investigación muy activas. Existe bibliografía especilizada por medio de la cual se puede profundizar en ellos.

Observación final

Para que sea completa, aun una primera aproximación a la computación cuántica debe incluir la descripción de algunos algoritmos cuánticos representativos, que por razones de espacio postergamos para un siguiente artículo. Partiendo de una base sólida de fundamentos teóricos como los que abordamos en las secciones precedentes, los algoritmos cuánticos constituyen la mejor manera de ilustrar la *forma de pensar cuánticamente*, y las ventajas que tendría el modelo cuántico en comparación con el modelo clásico, considerando distintos aspectos computacionales.

Algunos ejemplos de algoritmos cuánticos que se suelen utilizar para ilustrar la combinación de la superposición y la interferencia son el *algoritmo de Deutsch* y el *algoritmo de Deutsch-Jozsa*, que determinan si una función booleana es constante o balanceada; el *algoritmo de Bernstein-Vazirani* y el *algoritmo de Simon*, que resuelven los problemas de la *cadena secreta* y de la *máscara secreta*, respectivamente; el *algoritmo de Grover,* cuyo propósito es realizar una búsqueda no estructurada; y el *algoritmo de Shor*, el cual permite factorizar un número natural.

Otras descripciones algorítmicas a las que se recurre habitualmente con fines didácticos son los protocolos de comunicación cuánticos, con los que se puede ejemplificar el uso de otros recursos cuánticos como el entrelazamiento y la medición en distintas bases. Algunos protocolos típicamente presentados para dicho propósito son la *codificación superdensa*, que permite transmitir dos bits mediante un cúbit a través de un canal de comunicación cuántico; la *teleportación cuántica*, protocolo con el se puede transmitir el estado de un cúbit por medio de dos bits a través de un canal clásico; el *juego no local CHSH*, en el que dos participantes reciben entradas binarias aleatorias y deben producir para ganar respuestas binarias que satisfagan una determinada condición; y el *protocolo BB84*, diseñado para acordar una clave secreta.

Todos los ejemplos de algoritmos y protocolos de comunicación cuánticos mencionados en esta sección figuran en las referencias que especificamos a continuación.

Referencias

Los contenidos del libro indicado en la introducción, cuyos contenidos se resumen en parte en este artículo, se basaron principalmente en las obras (Nielsen y Chuang, 2010), (Hughes, 2021) y (Wong, 2022). Las dos últimas son textos introductorios que permiten obtener, de cero, un grado de conocimiento sólido de los fundamentos de la computación

cuántica. Reúnen además material sobre herramientas de programación, corrección de errores cuánticos y hardware cuántico. La obra de M. Nielsen e I. Chuang, por su parte, es de referencia fundamental de la computación cuántica. Todas estas publicaciones abordan la complejidad cuántica con cierto detalle, pero para tratarla con mayor profundidad, para el desarrollo del libro base de este artículo se utilizaron sobre todo las obras (Arora y Barak, 2009), (Aaronson, 2013) y (Rosenfeld, 2026), y el artículo (Bernstein y Vazirani, 1993). De este artículo provino, además, la descripción de la máquina de Turing cuántica.

Otras fuentes fueron una wiki y tres cursos en línea de acceso libre. La wiki, de nombre *Qudos*, formó parte de los entregables de la tesis de grado (Tomatis y Miglierini, 2025). Con respecto a los cursos, dos de ellos, (Matuschak y Nielsen**,** 2019) y (Quantum SOAR, 2020), son cursos introductorios con propuestas de enseñanza innovadoras. El tercero, (Watrous, 2021), es de nivel superior.

Para profundizar en la complejidad cuántica se sugiere considerar el libro (Kitaev, Shen y Vyalyi, 2002). Para recorrer la historia de la mecánica cuántica, la obra de divulgación (Kumar, 2011). Y para conocer en detalle trabajos influyentes en el desarrollo de la computación cuántica, los siguientes artículos: (Benioff, 1980) y Feynman (1982), de los inicios de la disciplina; (Deutsch, 1985), (Deutsch, 1989), (Bernstein y Vazirani, 1993) y (Yao, 1993), sobre los modelos de computación cuántica y la complejidad cuántica; (Cleve, Ekert, Macchiavello y Mosca, 1993), (Deutsch y Jozsa, 1993), (Bernstein y Vazirani, 1993), (Simon, 1994), (Grover, 1996), (Shor, 1994), (Bennett y Weisner, 1992), (Bennett, Brassard, Crépeau, Jozsa, Peres y Wootters, 1993), (Clauser, Horne, Shimony y Holt, 1969) y (Bennett y Brassard, 1984), correspondientes, en el mismo orden, a los algoritmos y protocolos de comunicación cuánticos enumerados en la sección anterior; y (Barenco, Bennett, Cleve, DiVincenzo, Margolus, Shor, Sleator, Smolin y Weinfurter, 1995), (Kitaev, 1997) y (Shi, 2002), referidos a la universalidad en la computación cuántica.

Detallamos a continuación las referencias citadas:

Aaronson, S. (2013). *Quantum computing since Democritus*. Cambridge University Press.

Arora, S. y Barak, B. (2009). *Computational complexity: a modern approach*. Cambridge University Press.

Barenco, A., Bennett, C., Cleve, R., DiVincenzo, D., Margolus, N., Shor, P., Sleator, T., Smolin, J. y Weinfurter, H. (1995). *Elementary gates for quantum computation*. Physical Review, A, 52, 5, 3457–3467.

Benioff, P. (1980). *The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines***.** *Journal of Statistical Physics, 22, 5, 563-591.*

Bennett, C. y Brassard, G. (1984). *Quantum cryptography: Public key distribution and coin tossing*. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 175–179.

Bennett, C., Brassard, G., Crépeau, C., Jozsa, R., Peres A. y Wootters, W. (1993). *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*. Physical Review Letters, 70, 1895–1899.

Bennett, C. y Wiesner, S. (1992). *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*. Physical Review Letters, 69, 2881–2884.

Bernstein, E. y Vazirani, U. (1993). Quantum *complexity theory***.** *Proceedings of the 25th Annual ACM Symposium on Theory of Computing,* San Diego, California, USA, 11–20. ACM Press.

Bernstein, E. y Vazirani, U. (1997). *Quantum complexity theory*. SIAM Journal on Computing, 26, 5, 1411–1473.

Clauser, J., Horne, M., Shimony, A. y Holt, R. (1969). *Proposed experiment to test local hidden-variable theories*. Physical Review Letters, 23, 880–884.

Cleve, R., Ekert, A., Macchiavello, C. y Mosca, M. (1998). *Quantum algorithms revisited*. Proceedings of the Royal Society of London. A, 454, 1969, 339–354.

Deutsch, D. (1985). *Quantum theory, the Church–Turing principle and the universal quantum computer*. Proceedings of the Royal Society of London. Mathematical and Physical Sciences. A, 400, 1818, 97–117.

Deutsch, D. (1989). Quantum computational networks. Proceedings of the Royal Society of London. Mathematical and Physical Sciences, A, 425, 1868, 73–90.

Deutsch, D. y Jozsa, R. (1992). Rapid solution of problems by quantum computation. Proceedings of the Royal Society of London. A, 439, 553–558.

Feynman, R. (1982). *Simulating physics with computers*. International Journal of Theoretical Physics, 21, 467–488.

Grover, L. (1996). *A fast quantum mechanical algorithm for database search*. Proceedings of the 28th Annual ACM Symposium on Theory of Computing, Philadelphia, Pennsylvania, USA, 212–219. ACM Press.

Hughes, C. (2021). *Quantum computing for the quantum curious*. Springer.

Kitaev, A. (1997). *Quantum computations: algorithms and error correction*. Russian Mathematical Surveys, 52, 6, 1191–1249.

Kitaev, A., Shen, A. y Vyalyi, M. (2002). Classical and quantum computation. American Mathematical Society.

Kumar, M. (2011). Quantum: Einstein, Bohr y el gran debate sobre la naturaleza de la realidad. Editorial Kairós.

Matuschak, A. y Nielsen, M. (2019). Qu*antum computing for the very curious*. Quantum Country.

Nielsen, M. y Chuang, I. (2010). *Quantum computation and quantum information*. Cambridge University Press, 10th Anniversary Edition.

Quantum Soar (2025). *Introduction to quantum computing: complete course*. Quantum Soar.

Rosenfeld, R. (2026). *Computabilidad y complejidad computacional*. EDULP.

Shi, A. (2002). *Both Toffoli and Controlled-NOT need little help to do universal quantum computation*. Quantum Information and Computation, 2, 1, 41–59.

Shor, P. (1994). *Algorithms for quantum computation: discrete logarithms and factoring*. Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 124–134. IEEE Computer Society Press.

Simon, D. (1994). On *the power of quantum computation***.** *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science,* Santa Fe, New Mexico, USA, 1**16–123.** IEEE Computer Society Press.

Tomatis, F. y Miglierini, F. (2025). *Dos hojas de ruta para aprender computación cuántica*. Tesis de grado, Facultad de Informática, Universidad Nacional de La Plata.

Watrous, J. (2025). *Understanding quantum information and computation*. IBM Quantum Learning.

Wong, T. (2022). *Introduction to classical and quantum computing*. Rooted Grove.

Yao, A. (1993). Quantum *circuit complexity***.** *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science, Palo Alto, CA, USA, 352-361.* IEEE Computer Society Press.