LOS PRINCIPIOS BÁSICOS DE UNA COMPUTADORA CUÁNTICA

Palabras clave: computación cuántica, entrelazamiento.
Keywords: *quantum computation, entanglement.*

Resumen: El procesamiento, almacenamiento y transmisión de la información están fundamentalmente limitados por las leyes de la física. En este artículo se introducen los principios básicos de la computación cuántica, un paradigma que reemplaza los bits clásicos por sistemas cuánticos (qubits) capaces de exhibir superposición y entrelazamiento. Se analiza cómo este cambio en la codificación de la información desafía la Tesis de Church-Turing Extendida, habilitando la ejecución de algoritmos cuánticos —como el de Shor— que prometen resolver problemas matemáticos complejos con una eficiencia que se cree inalcanzable para las supercomputadoras clásicas. Asimismo, se discute el estado del arte de la tecnología cuántica actual, caracterizada por la era NISQ (dispositivos ruidosos de escala intermedia). A través de los conceptos de supremacía, ventaja y utilidad cuántica, se ofrece una perspectiva crítica sobre los recientes hitos experimentales, los desafíos inherentes a la corrección de errores y el impacto disruptivo que estas tecnologías tendrán en la sociedad, la industria y la seguridad informática en los próximos años.

Holik, Federico[1,*]; Roncaglia, Augusto J. [2,3]

[1]Instituto de Física La Plata (IFLP, CONICET-UNLP), 1900 La Plata, Argentina.
[2]Universidad de Buenos Aires, Facultad de Ciencias Exactas y Naturales, Departamento de Física, Ciudad Universitaria, 1428 Ciudad Autónoma de Buenos Aires, Argentina.
[3]CONICET - Universidad de Buenos Aires, Instituto de Física de Buenos Aires (IFIBA), Ciudad Universitaria, 1428 Ciudad Autónoma de Buenos Aires, Argentina.

*E-mail: holik@fisica.unlp.edu.ar

Basic principles of a quantum computer

Abstract: The processing, storage, and transmission of information are fundamentally constrained by the laws of physics. This article introduces the basic principles of quantum computing, a paradigm that replaces classical bits with quantum systems (qubits) capable of exhibiting superposition and entanglement. We analyze how this shift in information encoding challenges the Extended Church-Turing Thesis, enabling the execution of quantum algorithms—such as those of Shor and Grover—that promise to solve complex mathematical problems with an efficiency unattainable by classical supercomputers. Furthermore, we discuss the state of the art of current quantum technology, characterized by the NISQ (Noisy Intermediate-Scale Quantum) era. Through the concepts of quantum supremacy, advantage, and utility, we offer a critical perspective on recent experimental milestones, the inherent challenges of error correction, and the disruptive impact these technologies will have on society, industry, and cybersecurity in the coming years.

INTRODUCCIÓN

Las tareas de almacenar, procesar y transmitir grandes volúmenes de información, juegan un rol clave en las sociedades del Siglo XXI. El procesamiento de datos se encuentra a menudo en la base de actividades relacionadas a la infraestructura crítica de muchos países.

La teoría de la información tuvo su primera formulación sistemática en los trabajos de Claude E. Shannon, durante los años '40 del siglo pasado (Holik, Federico. 2016). El carácter distintivo de su abordaje consistió en que logró dar un tratamiento matemático de distintos aspectos relacionados al concepto de información. Este giro metodológico permitió un abordaje cuantitativo a la tarea ingenieril de la transmisión de la información, permitiendo definir cantidades clave, tales como la de flujo de información a través de un canal.

En la práctica, toda tarea de almacenamiento, procesamiento o transmisión de información, se lleva a cabo por medio de algún dispositivo físico, y esto hace que dichas tareas, en última instancia, queden supeditadas a las leyes de la física. A modo de ejemplo, podemos almacenar información en libros, en nuestros cerebros, o en unidades de almacenamiento digitales, tales como, por ejemplo, *pendrives*. De forma análoga, en la actualidad procesamos, almacenamos y transmitimos información utilizando computadoras programables, tales como *laptops* o *celulares*. Las leyes de la física imponen restricciones a la manera en que podemos manipular la información. Un ejemplo sen-

cillo consiste en el hecho de que, a partir de la teoría de la relatividad especial, no es posible transmitir información a una velocidad mayor a la de la luz. Otro ejemplo no tan evidente se encuentra relacionado con el procesamiento de la información: para ello debemos invertir energía, que, a su vez, se disipa en forma de calor. Para tener una idea de la dimensión de este problema, es importante tener en cuenta que las supercomputadoras –como las que utilizan las grandes empresas tecnológicas en la actualidad– consumen grandes cantidades de energía para realizar sus actividades de procesamiento de datos, y suelen utilizar también grandes volúmenes de agua para su refrigeración. Esto ha despertado debates acerca de la huella de carbono que dejan los servidores que se utilizan para correr algoritmos de inteligencia artificial (Observatorio, 2024).

La teoría de la información cuántica puede definirse como aquella teoría de la información que surge a partir de la hipótesis de que los componentes de los dispositivos que utilizamos para procesar, transmitir y almacenar información, sean sistemas cuánticos. A modo de ejemplo, encontramos sistemas cuánticos cuando estudiamos la naturaleza a escala atómica y subatómica. Los átomos, protones, fotones, electrones, y otras partículas subatómicas, se rigen por leyes físicas que se engloban dentro de la teoría cuántica. Y estas leyes del mundo subatómico difieren en gran medida de las leyes de la física clásica, como veremos a continuación. También es posible producir estados cuánticos de la materia utilizando muchas partículas elementales. Esto ocurre, por ejemplo, ciertos materiales que se conocen como *superconductores*, los cuales, al ser enfriados a temperaturas lo suficientemente bajas –en algunos casos, cercanas al cero absoluto–, pueden dar lugar a corrientes eléctricas que involucran muchos electrones, y que se comportan colectivamente de acuerdo a las leyes de la física cuántica (Nobel Prize, 2025).

En este artículo nos concentramos en **qué ocurre con el procesamiento de la información si los componentes de los procesadores fueran capaces de utilizar las propiedades peculiares de los sistemas cuánticos.** En otras palabras, nos dedicaremos a delinear los aspectos fundamentales de lo que se conoce como teoría de la computación cuántica, la cual se puede definir como aquella teoría de la computación que surge de suponer que los componentes de las computadoras son sistemas cuánticos. Los resultados de las investigaciones de las últimas décadas en esta área sugieren que, si fuera posible construir computadoras cuánticas lo suficientemente grandes y que tengan protocolos de corrección de errores incorporados, sería posible obtener una aceleración en ciertas tareas que se creen muy costosas para las computadoras comunes o clásicas. Sorprendentemente, ya hay en la actualidad prototipos de computadoras cuánticas disponibles comercialmente, los cuales son utilizados para realizar tareas de investigación y desarrollo.

Comenzaremos primero discutiendo cuáles son las diferencias principales entre la información cuántica y la información clásica, para entender en qué sentido los sistemas cuánticos son diferentes a los clásicos, y qué impacto tiene esto en la codificación de la información. Luego, discutiremos la idea general de lo que sería una computadora cuántica programable, ilustrando las ideas básicas del campo de investigación. A partir de allí, haremos una breve sinopsis de algunos algoritmos cuánticos que, se cree, presentan ventaja respecto de los algoritmos clásicos conocidos. Finalmente, resumimos el estado del arte de la computación cuántica y sus perspectivas de desarrollo a futuro.

■ INFORMACIÓN CLÁSICA VS INFORMACIÓN CUÁNTICA

En los dispositivos estándar, tales como laptops, tablets, y celulares, la información se almacena en bits. Por ejemplo, uno puede codificar un mensaje (escrito en castellano) como una cadena de ceros y unos como la siguiente: “00010101”. Es por eso que nos referimos a estos dispositivos como digitales, en el sentido de que la información se codifica en términos de cadenas de ceros y unos. En estos dispositivos, la medida de información es el bit, y se le suele llamar bit físico al dispositivo físico que se utiliza para almacenar dicha información. Desde el punto de vista lógico, un bit puede tomar dos valores, cero, o uno. Por lo tanto, para instanciar físicamente un bit, necesitamos un sistema físico con dos estados claramente distinguibles, en los cuales representar los estados cero o uno. En las computadoras clásicas modernas, los transistores existen en estados de “encendido” (voltaje alto, 1) o “apagado” (voltaje bajo, 0) con el fin de realizar operaciones lógicas.

En los dispositivos clásicos, la información se procesa aplicando operaciones lógicas. Ejemplos de estas son el “y”, el “o”, y el “no”. A partir de estas operaciones lógicas elementales, es posible realizar operaciones más complejas. En general, es posible describir cualquier función booleana (es decir, cualquier función que mapee cadenas de ceros y unos en cadenas de ceros y unos) en términos de una combinación adecuada de las operaciones lógicas elementales. Por ejemplo,

una función que representa un cálculo matemático, no puede ser otra cosa más que un mapa que asigna cadenas de ceros y unos en cadenas de ceros y unos. En principio, cualquier tarea que realice una computadora clásica se puede reducir a esta descripción. En los dispositivos actuales, lo que se hace es representar estas operaciones lógicas utilizando circuitos electrónicos. En particular, las compuertas lógicas clásicas se implementan utilizando transistores. El chip de una computadora clásica disponible actualmente puede tener del orden de miles de millones de transistores, los cuales, a su vez, tienen un tamaño del orden de unos pocos nanómetros (es importante recordar aquí que un nanómetro es la mil millonésima parte de un metro). De esta forma, combinando muchísimas operaciones elementales sencillas de forma adecuada, las computadoras actuales pueden realizar tareas muy complejas, tales como procesar videos, entrenar y correr modelos de inteligencia artificial (como Chat GPT o Deep Seek), o realizar simulaciones numéricas necesarias para investigaciones científicas. de un bit -es decir, un dispositivo físico con dos estados perfectamente distinguibles- usáramos un sistema cuántico, podríamos tener otros estados que no están disponibles en el caso clásico. **Al equivalente cuántico del bit se lo denomina qubit, una abreviatura de quantum bit.** Un qubit puede estar no sólo en los estados cero y uno, sino que también puede existir en lo que se conocen como estados de superposición. Para ilustrar esta idea, utilizaremos la notación de Dirac de la siguiente forma. Los estados cero y uno del qubit, se representan matemáticamente por los símbolos $|0\rangle$ y $|1\rangle$, respectivamente. A diferencia del bit clásico, un qubit puede acceder a estados de superposición como:

$$|\text{Psi}\rangle = (1/\sqrt{2})(|0\rangle+|1\rangle) \qquad (1)$$

En un estado como el de arriba, si se realizara una medición del estado del qubit, el resultado podría ser cero, o uno, con una probabilidad del cincuenta por ciento cada uno.

Desde el punto de vista formal o matemático, **la teoría cuántica representa a los estados cuánticos por medio de vectores en un espacio vectorial.** Esto permite reflejar adecuadamente la física de estados de superposición como el de la ecuación (1). Si un qubit se encuentra en el estado de arriba, no podemos afirmar que esté en el estado cero, o uno. Diremos que se encuentra en los dos al mismo tiempo, o en una superposición de ambos. Por cómo son las leyes de la física cuántica, en ese caso, sólo podemos afirmar que, en caso de realizar una medición, es decir, en caso de que queramos retribuir la información acerca del qubit, la probabilidad de observar cero es 50% y la probabilidad de observar uno es 50%. De forma análoga, es posible preparar al qubit en estados con 30% de probabilidad de observar cero y 70% de observar uno, 60% y 40%, y todas las combinaciones probabilísticas posibles. En consecuencia, a diferencia del caso clásico en el cual hay solamente dos estados accesibles, en el caso cuántico hay infinitas posibilidades: cero, uno, y todos los posibles estados de superposición que se puedan concebir. El carácter aleatorio de las mediciones cuánticas, hace que el modelo de computación cuántica sea inherentemente probabilístico.

Pero las diferencias no terminan aquí. En la computadora cuántica, es posible producir estados de dos qubits de forma tal que estos queden correlacionados en formas que no tienen análogo clásico. Consideremos el siguiente ejemplo. Con un ordenador cuántico de dos qubits, podríamos preparar al primer qubit en cero, y al segundo en uno, obteniendo así el estado que representamos como $|01\rangle$. De forma análoga, también podríamos preparar al primer qubit en uno y al segundo en cero, obteniendo $|10\rangle$. Lo distintivo respecto a la computación clásica, es que en el caso cuántico podemos además producir un estado superposición de estos dos:

$$|\text{psi}\rangle = (1/\sqrt{2})(|01\rangle + |01\rangle) \qquad (2)$$

En tal estado, si medimos ambos qubits, obtendremos "01" o "10" con la misma probabilidad (cincuenta por ciento). En otras palabras, si medimos el primer qubit y obtenemos un cero, siempre vamos a obtener el valor opuesto en el segundo qubit, es decir, un uno. viceversa. Pero estas opciones aparecen con la misma probabilidad. Estos estados de superposición de múltiples qubits se conocen como *entrelazados*, y representan estados correlacionados de un procesador cuántico. En principio, es posible producir estados entrelazados de tantos qubits como queramos (Bub, Jeffrey. 2017).

Vimos que en las computadoras clásicas la información se codifica en cadenas de ceros y unos, y que las operaciones lógicas se representan por funciones booleanas (AND, OR, XOR, NOR, etc). Una primera diferencia que introduce la computación cuántica es que la información se codifica en términos de vectores en un espacio de Hilbert, los cuales permiten representan estados de superposición y entrelazados. ¿Cómo se representan matemáticamente las operaciones lógicas en la computadora cuántica? Esto se hace usando funciones que transforman vectores en vectores, lo que se conoce en la jerga matemática como *transformaciones lineales*. Dada la necesidad de que se mapeen estados en estados, es necesario que estas transformaciones lineales tengan asociadas también lo que se conoce como *matrices unitarias*.

Más allá de los detalles matemáticos, lo que es relevante para este artículo es que las características descriptas arriba hacen que la computación cuántica dé lugar a un modelo de computación que es diferente al clásico. De conjunto, el carácter estocástico de los procesos de medición, junto con la posibilidad de preparar a los qubits en estados de superposición y entrelazarlos entre sí, hacen que la computación cuántica pueda formularse tomando como base una descripción formal basada en un cálculo matricial que da lugar a probabilidades de resultados, en vez de la descripción determinista basada en funciones booleanas del caso clásico.

Pese a ser modelos de computación bastante diferentes entre sí, es importante remarcar que las computadoras cuánticas programables son capaces de computar la misma familia de funciones que las computadoras clásicas. Es decir, si es posible computar una cierta función F en una computadora clásica, entonces, es posible computarla también en una computadora cuántica, y vice versa. Como explicaremos en la siguiente sección, la diferencia viene dada en términos de eficiencia: se puede probar que existen problemas que pueden ser resueltos de forma eficiente en una computadora cuántica, mientras que se cree que a una supercomputadora clásica le llevarían cientos o miles de años (M. A. Nielsen and I. L. Chuang, 2000).

■ SUPREMACÍA CUÁNTICA Y ALGORITMOS CUÁNTICOS

La idea de construir computadoras cuánticas surgió con los trabajos de distintos físicos durante los años ‘80 del siglo pasado, con autores de la talla de Richard Feynmann y Yuri Manin. En particular, Richard Feynman propuso usar computadoras cuánticas para simular la dinámica de sistemas cuánticos de muchos cuerpos. Este problema no sólo es de interés en el ámbito de la física y de la ciencia básica, sino que es relevante en muchas aplicaciones comerciales. Para fijar ideas, es importante tener en cuenta que, tanto en la industria de medicamentos, así como en toda actividad industrial que requiera del desarrollo de nuevos materiales o compuestos químicos, es necesario hacer simulaciones de moléculas que tienen muchos átomos, o de átomos o moléculas con muchos electrones. La experiencia de décadas de investigación indica que este problema matemático es extremadamente duro para las supercomputadoras convencionales. En este marco, la hipótesis de Feynman sostiene que usar computadoras cuánticas, podría dar lugar a avances sustanciales en distintas aplicaciones industriales, así como en distintas ramas de la medicina.

La propuesta de Feynman está vinculada a lo que hoy se conoce como Tesis de Church Turing Extendida (TCTE), la cual puede formularse de la siguiente forma:

TCTE: “Toda función que pueda computarse con un dispositivo físicamente construible, puede ser simulada con precisión y de forma eficiente con una máquina de Turing probabilística”.

En la afirmación de arriba, el concepto de “máquina de Turing probabilística” hace referencia a un modelo de computación clásica no determinista. La palabra “eficiente”, hace referencia a la complejidad de cómputo, es decir, al hecho de que el problema se pueda resolver en una cantidad de pasos que crece polinomialmente con el tamaño de la entrada del problema. En palabras sencillas, decimos que un problema se puede resolver de forma eficiente si dicha resolución puede llevarse a cabo en un tiempo razonable para un ser humano a medida que el tamaño del problema crece.

Si la TCTE fuera cierta, implicaría que una computadora clásica podría simular de forma eficiente y precisa todo lo que pueda llegar a hacer una computadora cuántica. En la actualidad, la mayor parte de la comunidad científica especializada en este tema cree que la TCTE es falsa. Esto está vinculado al concepto de supremacía cuántica: la existencia de una tarea (o de un conjunto de tareas) que pueda ser realizada de forma eficiente por una computadora cuántica, pero que tenga un costo muy grande para toda supercomputadora clásica físicamente construible. Enumeramos a continuación algunos de los motivos que dan lugar a la afirmación o creencia de que la TCTE es falsa.

Un primer resultado importante está vinculado al problema de la factorización. Decimos, por ejemplo, que el número 7 es un factor del número 21, porque 21 = 3x7. En este ejemplo, 3 y 7 son factores de 21, del mismo modo en que 2 y 5 son factores de 40 (40 = 2x2x2x5). Para números pequeños, es fácil encontrar factores mentalmente. Si los números son más grandes, se pueden utilizar computadoras clásicas para resolver el problema de encontrar factores. El desafío matemático consiste en que, pese a los esfuerzos de los matemáticos por décadas, no ha sido posible encontrar ningún algoritmo clásico que permita resolver el problema de la factorización de forma eficiente. En términos sencillos, esto quiere decir que si nos dan un número entero muy grande (y lo suficientemente complejo), a las supercomputadoras de hoy podría tomarles cientos de años resolver el problema. Tan firme es la creencia en que el problema de la factorización es duro para las supercomputado-

ras clásicas, que existen algoritmos para proteger la información que se basan en la idea de que ningún hacker va a poder factorizar de forma eficiente con ninguna computadora disponible actualmente.

Es aquí donde la computación cuántica muestra su potencial revolucionario. Se sabe a ciencia cierta que si se pudiera construir una computadora cuántica lo suficientemente grande y tolerante a errores, sería posible resolver el problema de la factorización de forma eficiente (en tiempo polinomial con respecto al número de bits N del número en cuestión). Mientras que a una computadora clásica le llevaría mucho más tiempo (subexponencial en N) utilizando el mejor algoritmo conocido al momento. Es decir, que con una computadora cuántica, se podría factorizar un número entero muy grande y complejo en minutos o segundos (tarea que, como dijimos arriba, a las supercomputadoras actuales puede llevarles décadas). Esto es exactamente lo que permite hacer el algoritmo cuántico que lleva el nombre del científico de la computación Peter Shor. Utilizando este algoritmo, se podría quebrar el protocolo de encriptación conocido como RSA, el cual es utilizado ampliamente en el sector público y privado. Es decir, la mera posibilidad de que existan computadoras cuánticas podría llegar a poner en riesgo la seguridad informática de muchas instituciones. Este es un ejemplo de por qué la computación cuántica despierta tanto interés, y de por qué se invierten del orden de miles de millones de dólares a nivel mundial en esta área, ya sea para construir computadoras cuánticas, o para saber si los competidores son capaces de desarrollarlas, o no.

Es muy importante mencionar que el hecho de que no se conocen algoritmos clásicos que permitan resolver el problema de la factorización de forma eficiente, no implica necesariamente que no existan tales algoritmos. Al día de hoy, no existe una prueba matemática de que no existan algoritmos clásicos que permitan factorizar de forma eficiente. Esto quiere decir que, incluso si pudiéramos construir algún día computadoras cuánticas que puedan factorizar de forma eficiente números lo suficientemente grandes como para superar a cualquier supercomputadora clásica corriendo algoritmos clásicos que conocemos hoy, ello no constituía por sí solo una prueba de que la TCTE es falsa. Para demostrar su falsedad, sería necesario, además, demostrar que no existen algoritmos clásicos que permitan factorizar de manera eficiente. Este desafío teórico indica que, hoy por hoy, la falsedad de la TCTE es una hipótesis de trabajo relevante, pero que aún es necesario realizar más investigaciones para poder obtener una prueba de su falsedad.

Además del de Shor, otro algoritmo cuántico interesante es el de Grover. Este permite resolver un problema de búsqueda en una base de datos no estructurada. El aspecto ventajoso respecto es que permite una aceleración respecto del algoritmo clásico óptimo usado para resolver el mismo problema. Es importante mencionar que, a diferencia del algoritmo Shor, en el cual se obtiene una aceleración suprapolinomial respecto a los algoritmos clásicos conocidos, en el caso de Grover, la aceleración es cuadrática[1]. En palabras sencillas, esto quiere decir que, si a una computadora clásica le toman 1.000.000 pasos resolver el problema de búsqueda, a una computadora cuántica aplicando el algoritmo de Grover le tomaría solamente 1000. Es importante remarcar que el algoritmo de Grover tampoco constituye una prueba de que la TCTE sea falsa. El problema de búsqueda no estructurada tiene un costo exponencial para una computadora clásica. Dado que el algoritmo de Grover sólo permite una aceleración cuadrática, el problema sigue siendo exponencial para las computadoras cuánticas. En ese caso, la solución cuántica no da lugar a una resolución eficiente, la cual exige un costo polinomial.

Además del problema de la simulación, los algoritmos de Shor y Grover, existen también otras áreas en las cuales hay indicios de que las computadoras cuánticas podrían llegar a dar lugar a ventajas significativas respecto de los algoritmos clásicos. Estas investigaciones van desde la resolución de problemas de optimización, hasta la resolución de problemas de aprendizaje automatizado. Abordar estas investigaciones está más allá del alcance de este artículo corto e introductorio. Nos limitaremos a mencionar que, si bien se han obtenido resultados promisorios en los últimos años, es aún necesario que tengan lugar más desarrollos, tanto en materia de algoritmos, como de hardware cuántico, de forma tal de alcanzar el objetivo de obtener aplicaciones comerciales significativas o, más en general, de impacto social más allá de la investigación en física básica. Esta discusión nos lleva al problema de la siguiente sección: ¿Cuál es el estado del arte de la computación cuántica hoy?

■ ESTADO DEL ARTE DE LA COMPUTACIÓN CUÁNTICA EN LA ACTUALIDAD

Desde el punto de vista tecnológico, vivimos en un momento histórico apasionante en el siguiente sentido: ya existen prototipos de computadoras cuánticas, muchas de las cuales son accesibles al público general (The Quantum Insider, 2025). Estos prototipos son desarrollados por dis-

tintas empresas privadas, así como por universidades e institutos de investigación públicos.

Otro aspecto relevante del momento actual, es que varios laboratorios y empresas han anunciado que sus prototipos pueden resolver tareas que a las supercomputadoras actuales les llevarían cientos o miles de años. En otras palabras, ya hay laboratorios de investigación que afirman que sus prototipos de computadoras cuánticas han alcanzado lo que se conoce como *supremacía cuántica*. Como ejemplos de proclamas de supremacía cuántica, podemos mencionar a la empresa Xanadú, la cual utilizando una arquitectura de computadora cuántica fotónica (aproximadamente 126 fotones) logró resolver el problema de muestreo bosónico Gaussiano (Madsen, 2022); Google, con su procesador Willow, que resolvió la simulación de muestreo de circuitos cuánticos aleatorios con una computadora de qubits superconductores, al mismo tiempo que presentó resultados alentadores en materia de corrección de errores (Google Quantum AI, 2025); la computadora Zuchonghzi 3.0, que resolvió la tarea de muestrear circuitos cuánticos aleatorios con 105 qubits superconductores (Dongxin Gao, 2025).

Sin embargo, es importante introducir algunos conceptos fundamentales, así como tener en cuenta algunas sutilezas, de forma tal de evitar extraer conclusiones apresuradas acerca del estado del arte de la computación cuántica hoy. Por un lado, los prototipos disponibles en la actualidad funcionan de forma imperfecta: tienen errores. Pese a algunos resultados promisorios, no se conoce aún ninguna forma efectiva de implementar algoritmos de corrección de errores en los prototipos de computadoras cuánticas existentes. Por otro lado, el tamaño de las computadoras cuánticas disponibles hoy es muy pequeño, y van de decenas a unos pocos cientos de qubits. Estos dos efectos combinados, hacen que sea imposible aplicar algoritmos tales como el de Shor o el de Grover, y resolver problemas significativos. Esto implica que, en particular, no es posible quebrar algoritmos de encriptación tales como RSA con los prototipos disponibles actualmente.

Llegado este punto, es importante introducir el concepto de *ventaja cuántica*. Se dice que se ha alcanzado la ventaja cuántica, en caso de que exista alguna tarea relevante desde el punto de vista comercial, o con impacto social, que pueda ser llevada a cabo por una computadora cuántica de forma eficiente, mientras que a cualquier supercomputadora clásica físicamente construible le resulte muy costoso. Hay acuerdo en la actualidad en que no hemos alcanzado aún la era de la ventaja cuántica, dado que ninguna de las pruebas de principio de aplicaciones comerciales ha dado lugar a una ventaja significativa y convincente respecto de los algoritmos clásicos conocidos. Existen muchas propuestas que van desde simulaciones de materiales complejos hasta la resolución de problemas de optimización de forma híbrida (es decir, combinando computación cuántica con computación de alto rendimiento HPC).

Por otro lado, es importante mencionar que aún las pruebas de supremacía cuántica tienen por delante muchos desafíos. A modo de ejemplo, consideramos el caso de la empresa Google Quantum AI y su computadora cuántica Sycamore. En el 2019, la empresa anunció que había podido resolver el problema que se conoce como muestreo de circuitos cuánticos aleatorios con Sycamore en unos pocos segundos (Arute, 2019). En su publicación, estimaron que la misma tarea le costaría a una supercomputadora clásica del orden de 10.000 años. Sin embargo, unos meses después, IBM anunció que había podido resolver la misma tarea en tres días con una supercomputadora clásica (Pednault E., 2019). Paralelamente, un equipo de investigadores de China resolvió con un algoritmo clásico el problema en unos pocos segundos (Y. A. Liu, 2021).

El ejemplo de Google con Sycamore es interesante, dado que ilustra la complejidad del problema. Por un lado, los experimentos de supremacía cuántica suelen depender de hipótesis que son difíciles de comprobar. Por otro lado, aún hay muchas cosas que se desconocen en el ámbito de la computación clásica: los algoritmos clásicos y las arquitecturas de computadoras clásicas están también en constante desarrollo, lo cual da lugar a una auténtica competencia entre estos dos tipos de tecnologías. Nuevos desarrollos en el campo de la computación clásica, podrían dar lugar a formas más efectivas de simular los experimentos en computadoras cuánticas en la actualidad.

Sin embargo, más allá de que los experimentos de supremacía cuántica puedan dar lugar a discusiones acaloradas entre los y las especialistas, hay acuerdo en que estamos en una etapa histórica en la que hay prototipos de computadoras cuánticas que realizan tareas que ponen en jaque a las capacidades de las computadoras clásicas más potentes disponibles en la actualidad. Se espera que los próximos años den lugar a nuevos desarrollos, cada vez más interesantes, y con el norte de buscar aplicaciones comerciales que den lugar a una ventaja significativa respecto a los algoritmos clásicos.

En este escenario, es también importante mencionar el concepto de utilidad cuántica. Se dice que se ha alcanzado la era de la *utilidad cuán-*

tica (IBM Quantum, 2023), cuando existan prototipos de computadoras cuánticas capaces de resolver problemas que tengan un interés en la investigación científica, y que sean muy duros para las computadoras clásicas. Es razonable afirmar que algunos experimentos actuales tienen un indudable interés académico. Pero es también importante aclarar que muchas proclamas de utilidad cuántica podrían ser desafiadas por el desarrollo de nuevos algoritmos clásicos en los próximos años.

La existencia de dispositivos imperfectos de escala intermedia, los cuales realizan tareas que representan un desafío para las supercomputadoras clásicas, en combinación con la inexistencia de protocolos de corrección de errores escalables, nos permiten afirmar que estamos en lo que se conoce como era NISQ, las cuales son las siglas en inglés de Noisy Intermediate Scale Quantum, para referirse a la existencia de dispositivos ruidoso de escala intermedia (The Quantum Insider, 2023). Uno de los objetivos principales de las investigaciones en la actualidad es desarrollar protocolos de corrección de errores escalables que den lugar a computadoras cuánticas programables tolerantes a errores, lo suficientemente grandes como para aplicar algoritmos como el de Shor y obtener una ventaja significativa en problemas con relevancia comercial.

■ CONCLUSIONES

La computación cuántica es un modelo de computación que se apoya en las propiedades peculiares de los sistemas cuánticos para resolver de forma eficiente problemas que se creen muy costosos para las computadoras clásicas más poderosas. Como tales, constituyen una apuesta tecnológica promisoria, que podría llegar a dar lugar a un cambio tecnológico disruptivo y con profundo impacto social, en caso de que sea posible que algunas de las propuestas de arquitecturas existentes se desarrollen en su pleno potencial.

Existen en la actualidad prototipos de computadoras cuánticas, los cuales están disponibles comercialmente. Si bien hay experimentos relevantes que muestran el potencial de estos prototipos y que desafían a las supercomputadoras clásicas existentes, aún no se ha alcanzado un estado de desarrollo tal que permita obtener ventajas comerciales significativas. A pesar de ello, los desarrollos de los últimos años sugieren que es razonable esperar que nuevos descubrimientos y avances permitan alcanzar una mejora significativa en la performance de esta tecnología en los próximos años.

En la actualidad, diversos grupos de investigación en Argentina se dedican al estudio de la física cuántica desde múltiples perspectivas. Una lista extensa se puede encontrar en "Mapa de la Cuántica en Argentina" (Mapa de la Cuántica en Argentina, 2025, AFA: https://gbosyk.github.io/mapa_cuantico_argentina/), hecho a partir de la información recabada por la Div. de Fundamentos de la Asociación Física Argentina. Destacan aquellos enfocados en la teoría de la información cuántica y sus aplicaciones tecnológicas.

En lo que respecta específicamente a la computación cuántica, el ecosistema local se divide en tres ejes fundamentales:

- **Hardware:** Desarrollo de prototipos de *qubits* y componentes físicos.
- **Teoría:** Investigación en los fundamentos teóricos del campo.
- **Software y Algoritmos:** Un puente vital donde se trabaja tanto en el diseño de algoritmos para dispositivos NISQ —buscando aplicaciones prácticas inmediatas— como en el software de testeo y control de hardware.

A pesar de que la computación cuántica es todavía una disciplina emergente, la inversión sostenida de los sectores público y privado a nivel global asegura un mercado consolidado y en plena expansión. Argentina cuenta con recursos humanos altamente calificados y capacidad instalada en laboratorios para insertarse competitivamente en distintos eslabones de esta cadena de valor. Esto permite no solo monitorear los avances a nivel mundial, sino también dar pasos concretos en materia de soberanía técnica. En relación a esta dirección estratégica, en el año 2022 el Ministerio de Ciencia, Tecnología e Innovación creó el Programa institucional de Fortalecimiento de la Ciencia y las Tecnologías Cuánticas destinado a promover la investigación científica, el desarrollo tecnológico y la formación de recursos humanos en el país. Este programa se basó en un Informe del estado de la situación elaborado por investigadores y representantes de distintas instituciones. A finales de 2025 tuvo lugar un acuerdo interuniversitario -que involucró a una decena de universidades nacionales y otras instituciones dedicadas a la investigación científica- diseñado para potenciar la formación de especialistas y la investigación aplicada, facilitando así la integración de estas tecnologías en el sector productivo nacional.

Agradecimientos: Los autores agradecen a Ariel Bendersky por las observaciones sobre algunos conceptos fundamentales de complejidad algorítmica abordados en este artículo.

■ GLOSARIO

Algoritmo de Grover: Algoritmo cuántico que permite buscar en una base de datos no estructurada con una aceleración cuadrática respecto al mejor algoritmo clásico posible.

Algoritmo de Shor: Algoritmo cuántico capaz de encontrar los factores primos de un número entero muy grande de forma eficiente, lo que amenaza algunos sistemas de encriptación actuales como RSA. Reduce la complejidad del tiempo subexponencial a polinómico, lo que permite factorizar números grandes en horas o días, en lugar de miles de años.

Bit: Unidad básica de la información clásica. Se representa físicamente en sistemas digitales con dos estados mutuamente excluyentes (0 y 1).

Entrelazamiento cuántico: Propiedad exclusiva de la mecánica cuántica por la cual dos o más sistemas quedan fuertemente correlacionados, de modo que el estado de uno no puede describirse de forma independiente del estado del otro, sin importar la distancia física que los separe.

Era NISQ (Noisy Intermediate-Scale Quantum): Término que describe la era actual de la computación cuántica, caracterizada por procesadores de tamaño intermedio (decenas a cientos de qubits) que son ruidosos y carecen de corrección de errores escalable.

Qubit (Quantum bit): Análogo cuántico del bit. Es un sistema físico de dos niveles que, gracias a las leyes de la mecánica cuántica, puede encontrarse en el estado 0, en el estado 1, o en cualquier superposición lineal de ambos simultáneamente.

Superposición: Principio cuántico que permite a un sistema físico existir en múltiples estados a la vez hasta el momento de ser medido.

Supremacía cuántica: El hito de demostrar experimentalmente que una computadora cuántica puede resolver un problema específico (sea o no de utilidad práctica) en un tiempo razonable, mientras que a la supercomputadora clásica más potente le tomaría cientos o miles de años.

Tesis de Church-Turing Extendida: Hipótesis fundamental de la informática teórica clásica que postula que cualquier cálculo realizable físicamente puede ser simulado de manera eficiente por una máquina de Turing probabilística clásica. La computación cuántica pone en duda la validez de esta tesis extendida.

■ BIBLIOGRAFÍA:

Arute, F., Arya, K., Babbush, R. et al. Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510 (2019). https://doi.org/10.1038/s41586-019-1666-5

Bub, Jeffrey. 2017. "Entrelazamiento cuántico e información". En Diccionario Interdisciplinar Austral, editado por Claudia E. Vanney, Ignacio Silva y Juan F. Franck. http://dia.austral.edu.ar/Entrelazamiento_cuántico_e_información

Dongxin Gao, Daojin Fan, Chen Zha, Jiahao Bei, Guoqing Cai, Jianbin Cai, Sirui Cao, Fusheng Chen, Jiang Chen et al. "Establishing a New Benchmark in Quantum Computational Advantage with 105-qubit Zuchongzhi 3.0 Processor." Phys. Rev. Lett. 134, 090601, 2025. DOI: https://doi.org/10.1103/PhysRevLett.134.090601

Google Quantum AI and Collaborators. Quantum error correction below the surface code threshold. Nature 638, 920–926 (2025). https://doi.org/10.1038/s41586-024-08449-y

Holik, Federico. 2016. "Teoría de la información de Claude E. Shannon". En Diccionario Interdisciplinar Austral, editado por Claudia E. Vanney, Ignacio Silva y Juan F. Franck. http://dia.austral.edu.ar/Teoría_de_la_información_de_Claude_E._Shannon

IBM Quantum (2023) What is quantum utility? IBM Quantum Blog. Recuperado de: https://www.ibm.com/quantum/blog/what-is-quantum-utility

Instituto para la Formación de la Educación, Tecnológico de Monterrey, Observatorio, 2024: "El Costo ambiental de la IA" tomado de https://observatorio.tec.mx/el-costo-ambiental-de-la-ia/

M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, 2000)

Madsen, L.S., Laudenbach, F., Askarani, M.F. et al. Quantum computational advantage with a programmable photonic processor. Nature 606, 75–81 (2022). https://doi.org/10.1038/s41586-022-04725-x

NobelPrize.org (2025) The Nobel Prize in Physics 2025. Recuperado de: https://www.nobelprize.org/prizes/physics/2025/summary/

Pednault E., Gunnels J., Maslov D., Gambetta J. (2019) On "Quantum Supremacy". IBM Research Blog. Recuperado de: https://web.archive.org/web/20191101012410/https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

The Quantum Insider (2025) Top Quantum Computing Companies. Recuperado de: https://thequantuminsider.com/2025/09/23/top-quantum-computing-companies/

Y. A. Liu et al., Closing the "quantum supremacy" gap: Achieving real-time simulation of a random quantum circuit using a new sunway supercomputer, in Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis (SC '21) (Association for Computing Machinery, 2021) p. 3.

The Quantum Insider (2023) What is NISQ Quantum Computing? Recuperado de: https://thequantuminsider.com/2023/03/13/what-is-nisq-quantum-computing/

■ NOTA

[1] La aceleración es cuadrática y óptima en el modelo tipo "oráculo" o "consulta a caja negra", sin embargo, en la práctica, este algoritmo tiene muchas limitaciones. A modo de ejemplo, la construcción del oráculo como un circuito cuántico puede ser complejo, difícil o incluso inviable para algunos problemas del mundo real, ya que puede requerir de un costo extra de procesamiento, anulando la ventaja cuántica.