UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

Máster en filosofía teórica y práctica

Trabajo Fin de Máster

SOBRE LA COMPUTACIÓN CUÁNTICA

Dr. Carlos Ruiz Jiménez

Tutor: Dr. Jesús Zamora Bonilla

Abril de 2021

"I want to talk about the possibility that there is to be an *exact* simulation, that the computer will do *exactly* the same as nature".
(Feynman 1982, p. 468)

"Quantum computation (...) will be the first technology that allows useful tasks to be performed in collaboration between parallel universes".
(Deutsch 1997, p. 195)

"Is our universe a polynomial or an exponential place?".
(Aaronson 2005a)

"La construcción de un ordenador cuántico es un gran desafío tecnológico. Es algo que no tenemos, no está aquí, y va a tardar mucho tiempo en llegar".
(Cirac 2019, m. 35)

En recuerdo

En julio del año en curso presenté mi trabajo fin de master. Cuando preparaba el texto para su publicación en la web me llegó la noticia del fallecimiento del profesor Jacinto Rivera de Rosales. Me había evaluado vía telemática una presentación sobre Kant y Schelling que incluyo en esta web. Cursé con él la interesante asignatura *Interpretaciones de la Modernidad*, y aprendí mucho con su docencia y su copioso material audiovisual. Una gran pérdida, como la del primer profesor que tuve en el máster, Julio Armero, del que guardaré un grato recuerdo, y de cuya asignatura introductoria a la filosofía de la ciencia aprendí mucho, recibiendo numerosos y oportunos comentarios de ánimo. Sentí mucho también su temprana e inesperada pérdida.

Un recuerdo emocionado para ellos.

Madrid, noviembre, 2021.

Resumen

En este escrito se hace un recorrido por la historia del desarrollo de la computación cuántica, repasando las ideas filosóficas asociadas. Se dan los conceptos básicos de teoría computacional y de mecánica cuántica necesarios para la comprensión del mismo, y se describen los principales algoritmos cuánticos y los caminos que se están buscando para lograr su difícil materialización: la construcción de los ordenadores cuánticos escalables. Se analiza el sintagma *supremacía cuántica*, o supuesta superioridad de cálculo y transmisión de información con respecto a la informática clásica, meta a la que aspiran muchas de las grandes empresas tecnológicas del mundo, cuya publicidad a menudo genera gran confusión. Este reto podría hacer tambalear los cimientos de la nueva sociedad digitalizada, al suponer una amenaza para los intercambios telemáticos de información. También se trata el interesante debate que genera esta clase de computación en la teoría de la complejidad computacional, en torno a la llamada *tesis de Church-Turing extendida*, y en torno a los límites de las explicaciones clásicas de la teoría cuántica, ya que su desarrollo material está relacionado con la abstrusa frontera entre lo clásico y lo cuántico, en donde yacen asuntos de indudable interés epistemológico y ontológico.

Abstract

In this text we take a tour through the history of the development of quantum computing, while reviewing the associated philosophical ideas. The basic concepts necessary for grasping both; the theory of computation, and quantum mechanics; are provided. In addition, we describe the most relevant quantum algorithms, as well as the paths to achieve their difficult implementation that are underway: the building of scalable quantum computers. The syntagm *quantum supremacy* is analised -the supposed calculational and information-transfer superiority with respect to classical computation. This is a goal that many among the big technological corporations in the world aspire to, the publicity involved often giving rise to great confusion. This challenge could shake the foundations of the new digital society, as it poses a threat to the telematic exchanges of information. We also deal with the interesting debate that this kind of computation generates concerning the theory of computational complexity, about the so-called *extended Church-Turing thesis*, as well as about the limits of classical explanations of quantum theory, for its material development is related to the blurry boundary between classical and quantum, where tantalising issues of undoubted epistemological and ontological interest exist.

Índice general

INTRODUCCIÓN

Como es sabido, a partir del año 1900, con la introducción del *cuanto* por Max Planck, la ciencia dio un vuelco ontológico. Al contrario que su prima, la teoría de la relatividad, que había caracterizado al espacio y al tiempo como formas de lo real, desafiando al mismísimo Kant, la teoría cuántica venía de nuevo a dar la razón al idealismo del de Königsberg. La realidad se escapaba de las garras de la ciencia, que volvía a tener que conformarse con el estudio de los fenómenos. Así, las ondas electromagnéticas devinieron de nuevo partículas, los *fotones* que le valieron el Nobel a Einstein, pero más sorprendente aún sería que las propias partículas de la materia microscópica fueran reinterpretadas como ondas, como hizo Louis de Broglie con el *electrón*. Más adelante vendría la definición dinámica de Schrödinger y Dirac, la interpretación probabilística de Born o el nuevo formalismo de Heisenberg, que dio el golpe definitivo al realismo con su *principio de incertidumbre*. Todo este cuerpo teórico y fenoménico fue sintetizado epistemológicamente por la llamada *Escuela de Copenhague*, impulsada por Bohr, y el mismo Heisenberg, con una clara influencia de la filosofía positivista de los inicios del siglo XX[1], cuya principal aportación exigía aceptar una *dualidad onda-corpúsculo* en la naturaleza. Esta interpretación ortodoxa de la mecánica cuántica es la que ha perdurado, con pocos cambios, hasta nuestros días. Mas adelante, el matemático John von Neumann, precisamente el futuro teórico de la arquitectura de los nuevos ordenadores, apuntalaría la nueva lógica no conmutativa que imperaba en el mundo microscópico, dando, como los tiempos demandaban, una axiomatización rigurosa a la teoría cuántica(von Neumann 1932)[2].

[1] Así lo cree, por ejemplo, Popper, defensor del realismo, para el que el positivismo fue el coladero del subjetivismo en la física (Popper 1956). Más controvertida es la tesis de Forman, que sitúa el epicentro de la génesis histórica de las ideas en la República de Weimar, precisamente en la renuncia al positivismo, por una cuestión más política (de renuncia al poder), que epistemológica, y asocia el desarrollo de la teoría cuántica al existencialismo (Forman 1971). Quizás lo más acertado sea no vincular la teoría estrechamente con un movimiento filosófico, sino con una confluencia de varios en torno al antirrealismo (Jammer 1974)

[2] No tan rigurosa. A la postre la parte dedicada a la imposibilidad de las llamadas *variables ocultas*, clavo ardiendo del realismo, contenía una *petición de principio*. Parece que la primera que se dio cuenta de esto fue una alumna de Emmy Noether, Grete Hermann, en 1935. Poca una figura femenina parece para esos tiempos en esos temas, aparte de que el neokantismo imperante en los ambientes germanohablantes, y el prestigio del húngaro, enterraron la cuestión hasta que en los cincuenta y los sesenta David Bohm y John Bell desenterraran en cierta medida el realismo como posibilidad (Smolin 2019, p. 118).

Pero la nueva teoría, con su mochila de nueva matemática (matrices, funcionales, números complejos, operadores...), con su excesiva axiomatización, su carácter probabilístico e idealista (renuncia a conocer la supuesta naturaleza de la realidad), no convencía a muchos miembros de la comunidad científica, que se caracterizaba por sus tendencias realistas. Así, físicos como los mismos Schrödinger o Einstein, pusieron de manifiesto varias paradojas que se derivaban de sus resultados. Esto abrió un debate, de carácter ontológico, del que salieron interpretaciones alternativas a la de Copenhague, como la de la *onda-piloto* de de Broglie-Bohm, o los *universos paralelos*, de Everett. Sin embargo, la disidencia se fue apaciguando precisamente con la llegada, en la segunda mitad del siglo XX, de una de las consecuencias materiales de la teoría cuántica, el *láser*, con el que se pudieron diseñar experimentos que empezaran a desechar muchas de las interpretaciones realistas alternativas a la ortodoxa. Ya se podían comprobar en el laboratorio hechos como que una partícula solitaria podía a veces actuar exactamente como si estuviera interfiriendo consigo misma, como si se hubiera desdoblado.

No obstante, parte de la comunidad científica sigue hoy día demandando más pruebas que ayuden a entender esta teoría. De hecho, David Deutsch, uno de los fundadores de la computación cuántica, sigue defendiendo la teoría de Everett (Deutsch 1997), y el reciente premio Nobel Roger Penrose se ganó también una mala fama entre la ortodoxia cuántica al especular sobre la naturaleza gravitatoria del devenir clásico de los fenómenos cuánticos, relacionándolo además, sin mucho éxito, con el funcionamiento cerebral (Penrose 1989), lo que por otra parte dio alas a las teorías pseudocientíficas que siempre han acompañado a la mecánica cuántica. En cualquier caso, sigue siendo la teoría física en la que nadie acaba de estar del todo bien instalado. Feynman afirmó tener la certeza de que nadie entiende la mecánica cuántica (Feynman 1965, p. 129), aunque la interpretación ortodoxa caló en la comunidad científica hasta el punto de acallar cualquier voz discrepante, por desprecio o marginación. El operacionalismo se impuso, y "**shut up and calculate!**" fue la consigna (Mermin 1989, p. 199), aunque físicos como John Bell intentaran compaginar física y filosofía, al menos en su tiempo libre: "**I am a Quantum Engineer, but on Sundays I have principles**" (Gisin 2002, p. 199). En las últimas décadas solo se ha modificado ligeramente la interpretación de Copenhague, eliminando la dualidad que existía entre evolución y medición de los sistemas físicos, por medio de un artificio denominado *decoherencia*, según el cual, la pérdida de las características cuánticas de los sistemas no se produce debido a un observador en un acto de medición, sino en general por una interacción con el entorno macroscópico que, lamentablemente, es imposible de asir.

Es este contexto el responsable de que haya florecido el afán por el desarrollo material de la *computación cuántica*. En primer lugar, desde el punto de vista filosófico, se trataba de buscar una salida a una colisión epistemológica que ya Feynman consideraba inevitable en 1960 (Feynman 1960). Por un lado, el mundo atómico, con sus reglas cuánticas, su lógica no conmutativa y su reversibilidad, que cada vez quería crecer más. Por otro, el mundo clásico, macroscópico, irreversible, con su lógica tradicional y el desarrollo computacional, que buscaba incansablemente la miniaturización. El desarrollo material de una *máquina de Turing cuántica universal* (Benioff 1980; Feynman 1982; Deutsch 1985), vendría a eliminar definitivamente muchos de los recelos de los críticos del armazón ontológico y epistemológico que alrededor de la teoría cuántica se ha construido en los últimos cien años, puesto que se haría más palpable el potencial de la nueva lógica, en la velocidad de computación, en cada consulta por *Internet* o en cada operación bancaria a distancia. Más aún, desde el punto de vista filosófico, se volvería a entronizar el *noúmeno*.

En segundo lugar, desde el punto de vista sociológico, y quizás el motivo por el cual empresas como *Google*, *IBM*, *Intel* y otras estén apostando por invertir en estos desarrollos materiales, había que adelantarse a la amenaza que constituye la implementación de un ordenador de estas caraterísticas para el *statu quo* de la seguridad informática. La capacidad que tendría la lógica cuántica para desencriptar comunicaciones sería inimitable, aparte de abrir la posibilidad de nuevas formas de criptografía (Bennett y Brassard 1984). El portador material de los misterios de la cuántica podría hacer cosas como ganar siempre en un juego de cara/cruz o descubrir un as de oros entre cuatro cartas tapadas con total certeza con un solo gesto (Shor 1994; Grover 1996; Meyer 1999). Se ha dado en llamar *supremacía cuántica*, al alcance de este logro, y es tanta la impaciencia por llegar a él, que hasta una empresa como *Google* dio un paso en falso en 2019, deslizando que lo había logrado, cuando en realidad parece que todavía está lejos de conseguirlo. La revolución sería dramática, y no quedaría ningún secreto, ni ningún trilero, a salvo del poder que tendría tal materialización. Es por esto, y por las dificultades prácticas que están surgiendo en su construcción, por lo que hay quien piensa que este logro será inalcanzable ('t Hooft 1999; Levin 2003; Goldreich 2004; Kalai 2016).

En este trabajo se repasa la historia del desarrollo de la computación cuántica en las últimas décadas. Es un repaso histórico de las reflexiones, pero al hacer una historia de la reflexión también hemos querido hacer alguna reflexión sobre esa historia, dada la naturaleza del fin al que está destinado, que no es otro que un trabajo de un máster en filosofía. Al tratarse de un tema con muchas aristas, se han tenido que dejar de lado, o tocar solo tangencialmente, algunos otros relacionados, como el de la incompletitud de los

sistemas formales, o los de la complejidad y criptografía clásicas. Espero, no obstante, que esto no haya menoscabado demasiado el texto. El itinerario ha pasado en primer lugar por recordar brevemente, en el capítulo 1, los inicios de la teoría computacional, de los principales conceptos cuánticos implicados, y las pretensiones que tuvieron los primeros físicos y científicos computacionales para el desarrollo de esta rama de la ciencia. En el capítulo 2 se han repasado los conceptos básicos involucrados en la algorítmica cuántica, como el de paralelismo masivo y la supremacía, deteniéndonos en el algoritmo de Grover, por la importancia que tiene en orden a pensar la teoría en el nuevo contexto de la complejidad computacional. Siguiendo esta línea, en el capítulo 3, dedicado a la información y a la comunicación cuánticas, se ha presentado el algoritmo de Shor, su importancia en la nueva criptografía, y las novedosas formas de comunicación que pueden surgir a partir de las reglas de la mecánica cuántica. El capítulo 4 se ha ocupado del estado actual de puesta en marcha de estas tecnologías, con especial atención a la publicidad que las envuelve, dentro del enfoque social de los estudios tecnológicos, y a las controversias involucradas en estos nuevos desarrollos. Por último se dan unas breves conclusiones.

En cuanto a la bibliografía utilizada, sobre las bases de la computación cuántica hemos usado el informe recopilatorio de dos profesores de la Complutense, *Information and computation: Classical and quantum aspects* (Galindo y Martín-Delgado 2002), y el convertido ya en clásico texto *Quantum Computation and Quantum Information* (Nielsen y Chuang 2010). Nuestras reflexiones y datos históricos se han apoyado principalmente en dos libros de naturaleza diferente, dada la bipolaridad del tema tratado, uno desde el punto de vista de un científico computacional, *Quantum computing since Democritus*, de Scott Aaronson, y otro desde la perspectiva de un físico, de Jonathan Dowling, que fue uno de los expertos mundiales en computación cuántica, *Schrödinger's killer app : race to buid the world's first quantum computer* (Aaronson 2013a; Dowling 2013). Aaronson tiene además multitud de publicaciones libres en Internet, y un blog dedicado al tema. También autores clásicos del tópico, como Richard Feynman, David Deutsch o Seth Lloyd, tienen libros sobre esta materia que se han consultado (Feynman 1996; Deutsch 1997; Lloyd 2007). Aparte, muchos otros autores nos han ayudado en este recorrido, especialmente con material en Internet, artículos o conferencias, desde Charles Bennet o John Preskill a Juan Ignacio Cirac.

Capítulo 1

FUNDAMENTOS

1.1. ¿Hay más espacio al fondo? El germen de la computación cuántica

1.1.1. El computador probabilístico

El afamado físico Richard Feynman fue de los primeros en darse cuenta de la problemática que surgía en la progresiva miniaturización de los componentes computacionales. Cuando uno intentara diseñar componentes a nivel molecular, ya no se enfrentaría a un simple problema de escala, sino a las leyes de la mecánica cuántica (Feynman 1960, p. 36). Gordon Moore, uno de los fundadores de *Intel*, estableció en 1965 una ley de proporcionalidad con el tiempo de la sucesiva disminución en el tamaño de los transistores, sugiriendo que se doblaría cada dos años el número que podría caber en un procesador. Esta reducción lleva consigo un aumento de la velocidad de procesamiento, cosa que todos hemos experimentado en los últimos años, dado que los componentes están cada vez más juntos y las señales deben recorrer menos espacio. Hoy en día existen microprocesadores de unos pocos nanómetros, un orden de magnitud más pequeño que nuestro fatídico virus SARS-CoV-2, y los ingenieros predicen que todavía hay algo de margen. No obstante, más temprano que tarde se llegará a los dominios de la física cuántica, en donde ya no solo se tendría el ubicuo problema práctico de la disipación de energía de los mecanismos físicos, sino que la propia indeterminación cuántica dejaría su sello, en forma, por ejemplo, de *efecto túnel*, por el que las partículas son capaces de atravesar barreras de potencial que clásicamente les estarían vedadas. Recordando una bella imagen de Ortega, la materia pasaría a ser "alma" (Ortega y Gasset 1947, p. 81). Incluso la lectura de la información, que todo ordenador debe hacer en cada paso de computación, podría estar limitada por el *principio de indeterminación* de Heisenberg. Feynman, poniendo en juego patrimonio propio, animó a la juventud a superar los retos nanotecnológicos, que eclosionarían unos lustros después. Más adelante, en 1981, vendría su disquisición acerca de la insuficiencia

de los ordenadores clásicos en las simulaciones físico-cuánticas y la propuesta de simulador cuántico, recogidas en sus famosas conferencias sobre computación (Feynman 1996), impartidas en el CalTech entre 1983 y 1986.

En estas famosas conferencias, Feynman hace un repaso, a su modo, de muchos de los tópicos de la teoría computacional de su siglo. En cuanto al tema que nos va a ocupar en este trabajo, debemos prestar especial atención en primer lugar a los tópicos de la disipación computacional y la reversibilidad. En este sentido, su aportación consiste en clarificar conceptos, dándoles su impronta personal, dado que ya había muchos trabajos anteriores al respecto (Landauer 1961; Bennett 1973; Fredkin y Toffoli 1982; Bennett 1982). Recordemos que, cuando falleció, se podía leer en la pizarra de su despacho "**what I cannot create I do not understand**". Él mismo reconoce que su interés en el tema le venía inspirado por su colega Edward Fredkin (Feynman 1982, p. 467), y que también se trataba en parte de poner en claro algunas de las ideas de Charles Bennett, al que cita a menudo. La inquietud principal de Feynman era cómo una computación irreversible clásica podía simular de verdad, no ya un sistema cuántico, sino una física clásica local, causal y reversible. Él no se contentaba, tengamos en cuenta, con una analogía, o con un intento de imitación, que es lo que básicamente se hace en los centros de cálculo con los modelos sobre algún aspecto de la naturaleza, no, él, siguiendo a mi juicio un realismo ingenuo que acecha a muchos de los grandes físicos, buscaba cómo lograr una simulación *exacta*. Como este era un callejón sin salida, por la inabarcable capacidad de memoria que se requeriría, fue más allá. Creyó que la clave estaba en simular directamente una teoría cuántica de la que tampoco tenía sólidos cimientos epistemológicos. Como muchos físicos de ayer y hoy, ateniéndose al mentado imperativo del *¡calla y calcula!*, había alcanzado hitos importantes en la teoría cuántica (nada menos que la inclusión en ella de la teoría electromagnética, un Nobel compartido le valió el logro), sin acabar de explicarse bien sus fundamentos y sin salir de la perplejidad que supone pensar en términos clásicos sus fenómenos. Estaba convencido, no obstante, de que la naturaleza era esencialmente mecanocuántica y, por tanto, focalizó sus reflexiones sobre la computación en la simulación de una verdadera probabilidad computacional, para lo que era menester diseñar un *computador probabilístico* (Feynman 1982, p. 472), cuyas puertas en sus entrañas dieran siempre varias posibilidades de salida a una única entrada. En teoría, su conjetura de afirmar que un computador cuántico debería ser exponencialmente más rápido para realizar simulaciones químicas ya ha sido probada, como afirma el profesor Seth Lloyd en el resumen de un famoso artículo: "**Feynman's 1982 conjecture, that quantum computers can be programmed to simulate any local quantum system, is shown to be correct**" (Lloyd 1996, p. 1073). En la práctica, la simulación exacta a la que se refería Feynman nos parece

que todavía está por ver. Actualmente, los ingenieros químicos de *IBM* y *Google* son los que se dedican a este sueño imposible de Feynman, aunque de momento sus simulaciones no vayan más allá del estudio de unas cuantas moléculas.

1.1.2. La termodinámica de la información

Aunque Feynman no lo nombre, Rolf Landauer había mostrado que no se disipaba energía en las operaciones reversibles, sino en los efectos del borrado de la información, que cuesta $k_{\mathrm{B}}T\ln 2$ por bit funcionando a una temperatura ambiental T (Landauer 1961, p. 187). Así, la irreversibilidad termodinámica se relacionaba con la irreversibilidad computacional, con la pérdida del pasado por causa de los operadores lógicos. Como veremos, la evolución cuántica pura no olvida el pasado. Los operadores lógicos que se definen en el contexto de la computación cuántica deben ser reversibles por principio, lo que estableció un nuevo nexo de unión entre la computación cuántica, nacida en los ochenta, y la llamada *termodinámica de la información*, que se había gestado en los últimos años de la Segunda Guerra Mundial, gracias a autores como Claude Shannon (Shannon 1948) en los prestigiosos laboratorios *Bell*, de cuyo seno había salido el transistor apenas un año antes. Shannon definió una clase de entropía aplicada a la información, que luego fue generalizada por el matemático húngaro Alfréd Rényi.

Pero incluso en el caso de poder realizar solamente computaciones reversibles, en la práctica se gasta inevitablemente energía al computar. Evidentemente, los sistemas físicos son limitados, y hay que reinicializar los estados. El ruido introduce errores en los bits, que normalmente se corrigen haciendo redundancias, que luego hay que borrar. En todo computador debe haber un *diablillo* de Maxwell poniendo orden. Aunque este ente se empeñe en corregir errores, al final su capacidad de almacenar errores tiene un límite. Por tanto, tendrá que vaciarse, transmitiendo entropía al exterior en mayor medida que la que ha disminuído gracias a su labor, y siempre se cumplirá el segundo principio de la Termodinámica y, por tanto, habrá aumento de entropía y gasto energético. En cualquier caso, la cota inferior que establece el principio de Landauer de gasto de energía no es algo que preocupe, de momento, a los ingenieros, puesto que las disipaciones de calor de nuestros ordenadores son unos cuantos órdenes de magnitud mayores. La constante de Boltzmann, k_{B}, medida en una unidad energética macroscópica como el *julio*, es del orden de 10^{-23}. De hecho, en la naturaleza las cifras de disipación tampoco se acercan. Nuestras neuronas tienen una pobre eficiencia energética, como diez órdenes de magnitud por encima del límite de Landauer, y el copiado de ADN, que sería más eficiente, solo

llega a un gasto energético por bit dos órdenes de magnitud mayor (Bennett 1982, p. 907).

Aparte del límite de tamaño y de las cuestiones termodinámicas, el siguiente paso era el diseño teórico de un ordenador que usara las reglas de la mecánica cuántica como herramientas de cálculo. Para cualquier circuito computacional irreversible, en donde se pierda la información de algún bit por el camino, siempre se puede diseñar uno funcionalmente equivalente que sea reversible. No hay más que guardar la información que se fuera a borrar y añadirla a la salida. Pero antes de abordar el diseño de algoritmos cuánticos, repasemos brevemente algunos tópicos de computación y teoría cuántica.

1.2. Orígenes computacionales

1.2.1. La lógica conservativa

Como es sabido, cualquier ordenador se puede entender como una *máquina de Turing universal*. Una máquina de Turing es un dispositivo imaginario que ideó en 1936 el matemático inglés para simular procesos computacionales. Consistía, *grosso modo*, en un cabezal que podía actuar sobre una banda de papel parcelado, regido por una unidad de control, que podía encontrarse en diferentes estados según el cabezal escribiera, borrara, leyera, se moviera a derecha o izquierda o se parase. Así se pasaba de una situación o configuración inicial a una final en un número finito de pasos, que se podían diseñar con las *tablas de máquina*, describiendo así un procedimiento general o algoritmo. El adjetivo universal se basa en considerar una máquina como programable para cualquier algoritmo. Esta idea matemática se complementa físicamente con la llamada *tesis de Church-Turing*, que defiende que si un algoritmo puede ser implementado materialmente de cualquier manera, por ejemplo, en un ordenador personal, entonces existirá un algoritmo equivalente diseñado para una máquina universal de Turing que realizará exactamente la misma tarea. En esta tesis radicó de hecho el desarrollo del computador en los años cuarenta, de la arquitectura de von Neumann y del proyecto *ENIAC* (Nielsen y Chuang 2010, p. 4).

Más adelante, en los setenta, se demostró la equivalencia polinomial entre las máquinas de Turing y los circuitos booleanos lógicos (Galindo y Martín-Delgado 2002, p. 378). Dicho de otra forma, un problema decidible está en la clase de problemas **P**, es decir, puede resolverse en un tiempo polinómico en **n**, dada una cadena de entrada de longitud **n**, sí y sólo sí existe una familia asociada de circuitos polinómicos que lo resuelven. Todos los problemas en la clase **P** tienen, por tanto, circuitos polinómicos, pero la inversa no es cierta, hay circuitos polinómicos para problemas indecidibles. Esto justifica que trabaje-

mos con circuitos y puertas lógicas, por ser más generales, antes que con las máquinas de Turing, o esos archiveros locos que describe Feynman (Feynman 1996, p. 5).

La puertas lógicas son las unidades algorítmicas básicas en donde se realizan ciertos procedimientos con la información, recogiendo uno o varios bits de entrada y emitiendo los que procedan a la salida. Una puerta lógica clásica famosa sería la puerta binaria **AND**, cuyo resultado pierde información de entrada y, por tanto, es irreversible. La puerta monaria **NOT** sería sin embargo una puerta reversible y, por tanto, servirá también para circuitos cuánticos. Usualmente se representa así:

$$\begin{array}{c}\text{NOT}\\ A \;\text{—}\boxed{X}\text{—}\; \neg A = 1 \oplus A,\end{array} \tag{1.1}$$

en donde un bit en estado **0** se transformaría en uno en estado **1**, y viceversa. También se puede entender como la adición módulo 2 (binaria), representada por el símbolo $\oplus$, de un bit en estado **1**. La mayoría de las puertas binarias son irreversibles, pero siempre se puede completar la información de salida con uno o varios bits testigos, de control o *ancillae*, de forma que se conviertan en puertas reversibles (Bennett 1973, p. 525). Por ejemplo, el **OR** exclusivo, **XOR**, equivalente a la suma de dos bits, es una puerta irreversible, pero se puede completar de la siguiente forma,

$$\begin{array}{c}\text{CNOT}\\ \begin{array}{ll} A & \text{—}\bullet\text{—}\; A \\ B & \text{—}\oplus\text{—}\; A \oplus B. \end{array}\end{array} \tag{1.2}$$

Es decir, la puerta invierte el segundo bit solo si el primer bit está "encendido", de ahí la denominación de la puerta como **CNOT** (Controlled-Not). Aquí, el bit ancilla, A, nos sirve para recuperar la información del operador **XOR** que se escribe en el segundo bit, también denominado bit *diana*. Deutsch también la llamó *puerta de medición*, dado que si el bit de entrada B es **0**, su salida es una medida no perturbativa del valor del bit A (Deutsch 1989, p. 75). De hecho, cualquier circuito lógico clásico irreversible puede ser sustituido por un circuito equivalente de elementos reversibles utilizando la llamada *puerta de Toffoli* o **CCNOT** (Controlled-Controlled-Not):

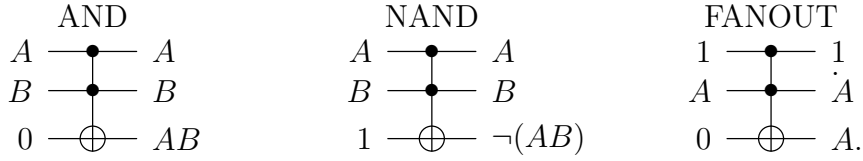
$$\begin{array}{c}\text{CCNOT}\\ \begin{array}{ll} A & \text{—}\bullet\text{—}\; A \\ B & \text{—}\bullet\text{—}\; B \\ C & \text{—}\oplus\text{—}\; C \oplus AB. \end{array}\end{array}$$

en donde denotamos $AB \equiv A \wedge B$ por abreviar. Es esta, como se ve, una puerta de tres

bits de entrada, ternaria, que por tanto podrán estar en 8 configuraciones distintas. Los dos primeros bits son de control y el ultimo es invertido cuando los dos primeros están encendidos. Conviene hacerse la tabla de verdad de esta puerta para ver de qué estamos hablando:

A	B	C	A′	B′	C′
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

En primer lugar, no solo es una puerta reversible, sino que ella misma es su inversa, $\mathbf{CCNOT}^2 = \mathbb{1}_8$, es decir, si se aplica dos veces la misma puerta se recupera el pasado. Además, si se observa la tabla, cuando el tercer bit de entrada está apagado, la salida en el bit diana simula un **AND**, que en esta ocasión será reversible, dado que tenemos en la salida la información de los otros dos bits de entrada, y así se pueden simular otras puertas clásicas, como las que pueden generar cualquier circuito, **NAND** y **FANOUT** (bifurcación o copia):



(1.3)

Este hecho se verbaliza diciendo que la puerta de Toffoli es *universal* en computación clásica, como también lo es la de *Fredkin*, famosa por implementar el computador de la bola de billar, que simula choques elásticos reversibles entre bolas de billar y las posibles salidas de estas (Fredkin y Toffoli 1982).

1.2.2. La máquina de Turing cuántica

Aunque Feynman fue el primero en apuntar que los computadores cuánticos serían más eficientes que los clásicos en simular los sistemas físicos, ya que la naturaleza según él era mecanocuántica, y reflexionaba sobre la forma de simular la probabilidad (Feynman 1982; Feynman 1986), las máquinas de Turing cuánticas habían sido antes introducidas en los trabajos de Paul Benioff (Benioff 1980; Benioff 1982), al que Feynman tampoco nombra. Ambos se basaban en definir hamiltonianos que rigieran la evolución de los componen-

tes físicos. El circuito lógico-cuántico propiamente dicho se debe, sin embargo, a David Deutsch (Deutsch 1989) y a sus desarrollos en los 90 (Yao 1993; Bernstein y Vazirani 1997).

Pero la motivación principal del cambio de paradigma computacional venía de los retos a los que se enfrentaba la tesis de Church-Turing con el desarrollo de la *teoría de la complejidad* en los setenta. Esta teoría trata de la cantidad de recursos que necesita un computador, especialmente en tiempo de cálculo y memoria de almacenamiento, para realizar un determinado algoritmo. Ya no se trataba solamente de la equivalencia entre algoritmos y máquinas de Turing, se requería también que esos algoritmos fueran *eficientes*, es decir, que pudieran ser incluídos en la ya aludida clase **P**, de problemas resolubles en tiempo polinómico respecto al tamaño de su cadena de entrada, o, en su defecto, al menos en un conjunto presumiblemente más amplio, la llamada clase **NP**, de algoritmos no deterministas resolubles en tiempo polinómico, que puede definirse como los problemas resolubles en tiempo polinómico con una ayuda, ejemplo o *testigo* de tamaño polinómico, como la comprobación de primalidad de un número. Es decir, son problemas cuyas soluciones positivas pueden ser verificadas en tiempo polinómico (existe también la clase complementaria, **coNP**, de los problemas cuyas respuestas negativas pueden ser chequeadas en tiempo polinómico). Así, la forma fuerte de la tesis de Church-Turing, con el requerimiento de eficiencia añadido, parecía no ser cumplida por las máquinas clásicas deterministas de Turing, frente a otros algoritmos de tipo probabilístico que se descubrieron, por ejemplo, en el contexto aludido de la primalidad (Solovay y Strassen 1977). Los algoritmos de la clase **NP** están relacionados con el mundo no determinista (y cuántico) por ser los que admiten subrutinas simultáneas y, aunque es patente que $\mathbf{P} \subseteq \mathbf{NP}$, el problema de que estas dos clases coincidan sigue estando abierto. Los expertos en computación creen, sin embargo, que $\mathbf{P} \neq \mathbf{NP}$, porque negarlo, según ellos, sería equivalente a afirmar que se puede automatizar la creatividad en matemáticas: "**The ability to check a proof would entail the ability to find one**" (Aaronson 2013a, p. 56). Conocer el método para verificar que una solución positiva de un problema es cierta equivaldría a resolver el problema, por muy difícil que fuera, por esto el problema $\mathbf{P} = \mathbf{NP}$ es el tercero de la lista de siete *problemas del milenio*, definidos en el año 2000 por el *Clay Mathematics Institute*, premiados con un millón de dólares.

Así, para dar cuenta de estas complicaciones en los supuestos de Church-Turing, Deutsch amplió la tesis a la afirmación de que cada sistema físico podía ser perfectamente simulado por un modelo universal de computador operando con medios finitos (Deutsch 1985, p. 99). Esta forma fuerte del principio no podía ser satisfecha por máquinas de Turing en la física clásica, debido, según él, a la continuidad de los estados de la dinámica

clásica. Y por un razonamiento análogo al de Feynman, basado en la evidencia del carácter mecanocuántico de la naturaleza, llegó a la conclusión de que en el contexto de la mecánica cuántica es donde se podía satisfacer ese principio más general. A pesar de su ejemplo de modelo cuántico universal de computación, que mostraba la eficiencia de la computación cuántica respecto de la clásica, la prueba de su ambiciosa conjetura sigue siendo un problema abierto. Aun así, las evidencias a favor de la eficiencia de la computación cuántica, encontradas en los noventa por autores como Peter Shor o Lov Grover (Shor 1994; Grover 1996), abrieron el camino experimental a los intentos de materialización de las máquinas de Turing o computadores cuánticos.

1.3. Características cuánticas

1.3.1. Superposición

Como es sabido, si la unidad de información clásica es el *bit*, a la unidad cuántica se le ha dado en llamar bit cuántico o *qubit*, término acuñado en 1995 por Benjamin Schumacher. Si clásicamente un estado de bit puede estar apagado, **0**, o encendido, **1**, cuánticamente puede estar en uno de los infinitos estados definidos por un vector en un espacio vectorial de dimensión finita, llamado *espacio de Hilbert*, y cuya norma o medida debe ser la unidad, reflejando el hecho de que la probabilidad de medir cualquier resultado debe ser la certeza absoluta. Estos vectores a menudo se denominan *kets*, por influencia del físico Paul Dirac. No vamos aquí a abusar del lenguaje matemático de que consta todo el formalismo de la mecánica cuántica, pero sí es preciso señalar que, al igual que en el análogo clásico, en este espacio se define la *base computacional* como $\{|0\rangle, |1\rangle\}$ para representar un qubit, que ya no será simplemente un 0 o un 1, sino que tendrá ciertas amplitudes de probabilidad, números complejos, cuyos módulos al cuadrado nos dan una medida de cuánto están siendo 0 y cuánto 1 en su evolución, y, en la medida, aquí sí como en el análogo clásico, nos proporcionará un 0 o un 1 en un azar regido por esas amplitudes.

Los estados cuánticos están representados por sus posibles valores según observables distintos, tanto continuos, como la posición o el momento lineal, como discretos. Los computadores cuánticos trabajan con observables discretos, específicamente los que toman dos valores principales, como el espín de una partícula material (de espín 1/2, como el electrón o el protón), la polarización respecto a un eje, los niveles energéticos de un átomo de hidrógeno o el sentido de una corriente. De esta forma se recupera la forma de la lógica binaria computacional. Tanto los observables como las puertas lógicas son representadas matemáticamente como matrices que actúan sobre esos vectores estados.

Es importante señalar que los estados cuánticos se clasifican en dos grandes grupos. El llamado estado cuántico *puro* es una superposición *coherente*. Por ejemplo, para un quibit podría ser una superposición de los dos estados de la base, $|0\rangle$ y $|1\rangle$, es decir, el sistema no se encuentra en uno u otro estado, sino en los dos, simultáneamente[1]. Si hacemos pasar este estado, a veces también llamado *función de onda*, por puertas lógicas que le perturben, en la evolución seguirá comportándose como si existieran simultáneamente las dos alternativas, y solo en la medición, o, en su defecto, en la interacción con sistemas macroscópicos, en el llamado tradicionalmente *colapso* de la función de onda, la naturaleza decidirá cuál de las alternativas mostrar, eliminando las demás. La experiencia cotidiana con objetos macroscópicos, en donde es prácticamente imposible mantener un estado puro para algún observable, hace que nos resulte chocante esta interpretación, pero en los estados microscópicos o, mejor dicho, con pocos grados de libertad[2], la naturaleza parece comportarse de esta forma, y cualquier interpretación alternativa choca con la evidencia del experimento.

El otro tipo de estados que se define en mecánica cuántica es el estado cuántico no puro, o *mezcla*, que constituye la versión clásica de nuestro conocimiento sobre el estado cuántico. En este caso el estado ya no es representado por un vector sino por una matriz, la *matriz densidad*, que nos da idea únicamente de la probabilidad de que ese estado se encuentre en $|0\rangle$ o en $|1\rangle$, pero ahora no se puede decir que simultáneamente. A esta versión clásica se llega porque se ha perdido la información cuántica del sistema, y solo se puede decir que está en una combinación de estados puros cuánticos. Se dice que ese estado (clásico) es una superposición *incoherente*, ya que no tenemos información de sus fases relativas, que constituyen esencialmente su característica cuántica (Ballentine 1998, pp. 50-54). El estado puro representa así un estado sobre el que un observador tiene información maximal. Por cierto, y en contra de un gran número de interpretaciones relativistas, no se trata de un concepto metafísico, el estado es una propiedad objetiva del mismo, que no depende del conocimiento del observador. Otra cosa es que otro observador no posea ese conocimiento maximal, pero eso es algo que también ocurre en la física clásica

[1]Me parece oportuno comentar que en la traducción del lenguaje matemático al verbal se cometen siempre algunos abusos, pérdidas de información o malentendidos. Las afirmaciones sobre *existencias* simultáneas de las distintas alternativas de los sistemas cuánticos no se basan en ninguna referencia ontológica, puesto que ello conllevaría una contradicción con los postulados de la teoría. En realidad se trata de alternativas regidas por la matemática de los números complejos, es decir, que aunque se dice que un sistema *existe* en dos estados simultáneamente, en realidad uno se refiere siempre a la referencia formal del concepto. El resto es elección interpretativa, metafísica. La interpretación ortodoxa que se está exponiendo aquí se cuida mucho de hacer referencias ontológicas.

[2]Los experimentos en el nivel mesoscópico hacen sospechar que es más correcto hablar de grados de libertad, es decir, de complejidad del sistema, que de su tamaño, aunque la relación es evidente.

(García Alcaine 1998)[3].

1.3.2. Unitariedad/Reversibilidad

La evolución de los sistemas en mecánica cuántica debe conservar la probabilidad, es decir, en todo momento el sistema, al ser medido, deberá tener un valor unidad de probabilidad de encontrar el *observable*, o magnitud física, que se estudie, en cualquiera de los estados de la base en la que se represente. Matemáticamente esto se traduce en que los operadores que representan las puertas lógicas, o las perturbaciones al sistema, deben conservar la norma (isometrías), y ser *unitarios*. Una de las consecuencias de este hecho es la comentada reversibilidad de los sistemas cuánticos en evolución, es decir, a partir de los valores posteriores a la perturbación, se deben encontrar los valores correspondientes que el sistema tenía en el pasado. Por esta razón, puertas lógicas clásicas irreversibles como la **AND** no tienen versiones cuánticas exactas.

Así, las puertas lógicas de nuestros circuitos cuánticos también pueden estar representadas por operadores que actúan como matrices unitarias $2^n \times 2^n$, siendo n el número de bits entrantes. Por ejemplo, la puerta clásica **NOT** monaria que definimos en (1.1) está representada por una de las llamadas matrices de Pauli, σ_x. Pero hay otras puertas cuánticas sin contrapartida clásica, como la puerta de **Hadamard** que mezcla los estados equiprobablemente, creando superposiciones cuánticas. Es por este hecho por lo que el recientemente fallecido profesor Dowling sugería olvidarse del físico-matemático Jacques Hadamard, a quien está dedicada, y llamarla **CAT**, por ser creadora de "gatos" de Schrödinger con qubits (Dowling 2013, p. 97). No vamos a profundizar en el sinnúmero de puertas cuánticas que existen, pero baste decir que, como en computación clásica, también existe un *conjunto universal de puertas cuánticas*, que reproducen todas las demás (Barenco et al. 1995). Este conjunto, como en el análogo clásico, no es único. De hecho, la puerta con análogo clásico de Toffoli y esta puerta de Hadamard constituyen un conjunto universal de puertas cuánticas (Shi 2003). Lo que sí es relevante es que en la epistemología asociada a la computación cuántica no es tan importante el marco lógico concreto como otras consideraciones que analizaremos posteriormente: "**unlike classical computation, where one needs to engineer specific classical logic elements such as AND, OR and NOT, the precise form of the interactions hardly matters in the quantum case**" (Deutsch 1997, p. 214).

[3] A partir de consideraciones como estas se desarrolló la última interpretación de la mecánica cuántica, la llamada *bayesiana*, que no es más que reescribir la regla de Born y las consideraciones de Bohr en términos de inferencia probabilística. David Mermin o Christopher Fuchs son algunos de sus defensores (Caves, Fuchs, y Schack 2002).

1.3.3. Entrelazamiento

Cuando se tratan sistemas de varios qubits, las bases computacionales se amplían, ya que, para n qubits, deben contener 2^n estados. Por ejemplo, para dos qubits, la base computacional es $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, en donde el estado $|01\rangle$ representa, por ejemplo, el hecho de que el primer qubit se encuentra en un valor **0** y el segundo en un valor **1**. El estado general del sistema será un vector ahora en un espacio de cuatro dimensiones, y cada proyección sobre las direcciones de la base computacional representará la amplitud de probabilidad que posee cada una de las alternativas que define esta base. En este contexto, es muy importante diferenciar entre dos clases de estados posibles: los separables y los entrelazados.

Un estado cuántico *separable* de dos qubits, por ejemplo, es el que se puede poner como producto[4] de un estado del primer qubit por otro estado del segundo qubit, cada uno en su espacio de dos dimensiones, con sus amplitudes de probabilidad asociadas a $|0\rangle$ y a $|1\rangle$. Esto se traduce en que, operatoriamente, se pueden tratar los dos qubits de forma independiente, sin que afecte la medida sobre uno al estado del otro. Un estado *entrelazado*, como los llamados *estados de Bell*, no está definido de forma disyuntiva en los espacios correspondientes a los dos qubits por separado, y las acciones sobre uno afectarán al otro. Teniendo en cuenta que los dos qubits pueden estar separados espacialmente, estados como este tienen unas propiedades bastante singulares. Por ejemplo, en el estado llamado *singlete de espín*, la medida de un valor de **0** en el primer qubit implica automáticamente que el segundo qubit tiene el valor **1** con total probabilidad, y viceversa. Hechos como este sirvieron de excusa a Einstein para hablar de *acciones fantasmales a distancia* e intentar refutar la completitud de la mecánica cuántica con uno de sus famosos *Gedankenexperimente* (Einstein, Podolsky, y Rosen 1935). Desde entonces, a este sorprendente hecho se le conoce como *paradoja EPR* (por las iniciales de los autores del artículo). El estado singlete es el que utilizaron más adelante Bohm y Aharonov para hacer más gráfica esta paradoja con un observable discreto como el espín (en EPR se utilizaban variables continuas) (Bohm y Aharonov 1957). Hay que decir que desde los años ochenta del pasado siglo los experimentos sugeridos por Einstein ya no son solo *mentales*, sino que se pueden comprobar en el laboratorio. Se vienen dando evidencias experimentales de que la mecánica cuántica en efecto sigue esas leyes que a Einstein tanto le preocupaban. A destacar son figuras como Alain Aspect, de la Univesidad de París, o Anton Zeilinger, de Viena,

[4]Se trata del producto *tensorial*, definido para manejar operativamente vectores de dos espacios diferentes que actúan conjuntamente.

que en la década pasada logró demostrar el entrelazamiento, usando como observable la polarización de fotones, a través de los nada desdeñables 143 km que separan las islas de *La Palma* y *Tenerife* (Clauser y Shimony 1978; Aspect, Grangier, y Roger 1982; Zeilinger 2012). Allí también se hicieron, como veremos, experimentos diseñados para demostrar la seguridad que ofrecería la criptografía cuántica. De hecho, las bases teóricas en las que se basaron estos experimentos, para diferenciar una teoría realista local, como la que quería Einstein, y una teoría no local como es la mecánica cuántica, fueron establecidas en los sesenta por un brillante físico teórico, John Bell, en unas famosas desigualdades (Bell 1964), que constituyen uno de los más importantes legados a lo que se puede conocer como *filosofía experimental*[5].

Como curiosidad técnica, decir que la puerta a dos qubits más importante en este contexto es la versión cuántica de la representada en (1.2), puerta **CNOT** (**ENT**, de *entanglement*, para Dowling). Es la puerta lógica cuántica capaz de generar el entrelazamiento, que constituye una de las ventajas, alguno dirá simples diferencias, de la computación cuántica frente a la clásica.

1.3.4. No clonado

En los años ochenta del pasado siglo se pretendía violar la causalidad relativista por medio de las propiedades de las partículas cuánticas, pero pronto se vio que este límite causal era más férreo de lo que se pretendía. La no localidad cuántica nada tenía que ver con la localidad relativista. Una de las líneas de investigación era precisamente el entrelazamiento, pues parecía apuntar a que se podía mandar información a distancia instantáneamente. Sin embargo, el azar intrínseco de la teoría impedía cualquier intento. Aunque al conocer el estado de una partícula se conociera instantáneamente el estado de otra lejana, la medida local no dejaba de ser una medida cuántica, con una probabilidad asociada, no se podría diseñar de antemano el mensaje, pues solo se conocía en el acto de medir. Este hecho está relacionado con el *teorema de no clonación*, una consecuencia muy simple de la linealidad de la mecánica cuántica que, sin embargo, no fue desvelada hasta que William Wootters y Wojciech Zurek publicaron una breve reseña en la revista *Nature* (Wootters y Zurek 1982). Su simplicidad desconcertó a la comunidad científica, que no entendió cómo pudo pasar inadvertido durante tantos años. Aunque normalmente se atribuye a los anteriores autores el logro, ese mismo año Dennis Dieks llegaba al mismo resultado, en una carta a *Physics Letters*, en donde se afirmaba la imposibilidad de

[5]Las pretensiones de Bell eran también de índole realista, es decir, esperando algún hecho que refutara la teoría cuántica, pero su inesperada muerte hizo que no pudiera asistir a los resultados experimentales más concluyentes.

transmisión de información a partir del entrelazamiento EPR (Dieks 1982).

En las adaptaciones de la puerta de Toffoli (1.3) vimos la puerta **FANOUT**, capaz de copiar un bit clásico. En el mundo cuántico las cosas cambian. De acuerdo con las propiedades unitarias y lineales de la mecánica cuántica, este teorema lo que afirma es que no es posible hacer una copia o clonación de un estado cuántico *arbitrario*. El teorema tiene una grave desventaja relacionada con las lecturas y las copias de seguridad, pero sin embargo es de una gran importancia en la llamada *criptografía cuántica*. Además, hay que decir que el teorema no impide la copia exacta de un estado simple conocido. Es decir, sí hay una puerta capaz de clonar estados $|0\rangle$ o $|1\rangle$ como lo hace la puerta **FANOUT** clásica. Por tanto, dado un estado desconocido $\alpha|0\rangle + \beta|1\rangle$, sí podremos lograr estados de la forma $\alpha|00...0\rangle + \beta|11...1\rangle$ a partir de él, sin más que usar la puerta capaz de copiar estados singulares. Más aún, existen algoritmos de copia aproximados (Buzek y Hillery 1996). Y, como veremos, tampoco impide *teleportar* estados, ya que este caso no es una copia, al borrarse el estado original.

1.3.5. Decoherencia

Como se ha adelantado, un estado puramente cuántico, de superposición, es muy difícil de observar en la vida cotidiana con objetos macroscópicos de muchos grados de libertad. Dicho de otra forma, no se puede definir claramente la función de onda de un sistema con muchos grados de libertad. Ni siquiera es fácil aunque uno quiera prepararlo, porque la gran cantidad de partículas da lugar a numerosas interacciones con el ambiente. Los estados de superposición se transforman y pierden su coherencia. En este caso, ya no tendríamos un sistema formado por estados como $|0\rangle$ y $|1\rangle$, con sus correspondientes pesos o probabilidades de existencia simultánea, sino un sistema que, o bien estará en el estado $|0\rangle$, o bien en el estado $|1\rangle$, cada uno con su correspondiente probabilidad. Este fenómeno se conoce como *decoherencia*, y de alguna forma ha venido a sustituir al indeseado *colapso* de la función de onda, que constituía uno de los postulados de la mecánica cuántica.

Gran parte de la comunidad de físicos, especialmente a partir de los años ochenta, no estaban conformes con el hecho de que los objetos cuánticos tuvieran que comportarse de una forma cuando no son medidos (evolución), y de otra cuando lo son (medida), aceptando un cambio drástico de formalismo matemático, de una evolución unitaria, lineal y reversible, a una interrupción no lineal e irreversible. Aparte de esto, desde el punto de vista epistemológico, el colapso planteaba bastantes dudas, y dio lugar a diversas especulaciones, dado que la evolución física parecía estar a merced de un observador

(¿consciente? ¿tendría que ser doctor en física?, se preguntaba John Bell). Uno de los mayores promotores de la teoría de la decoherencia fue el físico polaco Wojciech H. Zurek. El papel que juega el entorno en esta selección de una rama de la función de onda frente a otras ha venido a justificar el término *darwinismo cuántico*, empleado a veces en los artículos (Zurek 2003, p. 759). Aunque operatoriamente en muchos artículos se sigue utilizando el colapso de la función de onda en la medición de los observables, la teoría de la decoherencia proporciona una alternativa teórica más cómoda, aunque tampoco guste a muchos, que consideran que es desviar, y no explicar, el problema. La coherencia se pierde por interacción con el entorno en unos tiempos no accesibles hoy en día a los laboratorios (por debajo de la llamada *unidad de Planck*), razón por la que supuestamente no vemos los efectos cuánticos en nuestro mundo cotidiano. Según esta teoría, no hay gatos vivos y muertos a la vez (Schrödinger tenía razón), ni lunas que dejan de existir cuando no se las observa. Es imposible mantener estados de superposición en situaciones macroscópicas de alta decoherencia.

Capítulo 2

PROGRAMACIÓN CUÁNTICA

2.1. ¿Supremacía cuántica?

El término supremacía cuántica fue acuñado por el físico teórico estadounidense John Preskill en 2011, y denota el supuesto poder superior de cálculo, en términos de complejidad computacional, que tendría un ordenador cuántico frente a uno clásico. Se supone así que los ordenadores cuánticos tendrían el poder de abordar, con eficiencia polinómica, problemas en el dominio de la clase **NP**, que no podrían ser abordados con la misma eficiencia por los ordenadores clásicos (aunque sí se podrían verificar eficientemente en ellos). El ejemplo paradigmático es la factorización de números primos y el algoritmo de Shor, que supone una ganancia polinomial respecto a su contrapartida clásica exponencial. Sin embargo, como el mismo Preskill apunta, hay problemas para los que se sospecha que ni siquiera se podrían resolver con un ordenador cuántico. Dentro de los problemas **NP** existe un tipo de problemas especialmente complicados, los **NP-completos**, como el problema de satisfacibilidad booleana (SAT) o la coloración de grafos. No existen algoritmos no exponenciales conocidos para este tipo de problemas, es decir, no se va mucho más allá de la simple verificación de muchos casos, la solución por *fuerza bruta* o de *caja negra*[1]. Y tampoco se han descubierto tantos algoritmos como para presumir de que en un futuro cercano se descubra alguno. Los teóricos de la computación sospechan que los límites de esta están más relacionados con el diseño de estos algoritmos eficientes que con el soporte material en el que se basen (Aaronson 2008, p. 19). En su artículo, Preskill retoma los argumentos de Feynman sobre las simulaciones, y sus perspectivas son esperanzadoras. Mis dudas sobre la materialización final de estos ordenadores y sobre el lento avance de los resultados matemáticos que podrían impulsar aún más estos estudios me hacen ser cauto, y no creo que la pretendida supremacía cuántica esté tan cerca, pero igual mi "mente clásica"(?), como afirma Preskill, me esté jugando una mala pasada: "**Predictions are never**

[1]Tampoco la ortodoxia en matemáticas acepta como demostraciones de teoremas la comprobación de casos por ordenador, como se demostró en el teorema de los cuatro colores en 1976.

easy, but it would be especially presumptuous to believe that our limited classical minds can divine the future course of quantum information science" (Preskill 2013, p. 77). Aun así, es innegable que la versatilidad cuántica aporta una mejora intrínseca al diseño de estos algoritmos, pero muchos autores siguen discutiendo el término "supremacía". El doctor Juan Ignacio Cirac, por ejemplo, un físico teórico catalán, formado en Madrid, que se ha convertido en uno de los mayores expertos en computación cuántica del mundo, es de los que prefiere el término *inimitabilidad cuántica* (Cirac 2019, m. 2). Vamos a ver en este capítulo algunas de las ventajas y los inconvenientes que aporta el mundo cuántico a la teoría de la computación.

La principal ventaja del cálculo con qubits es aportada por su capacidad de superposición, lo que da lugar a fenómenos de interferencia y entrelazamiento. Se puede decir que un qubit puede estar actuando de dos maneras distintas al mismo tiempo, como **0** y como **1**. Con dos qubits tendremos la posibilidad de seguir cuatro líneas de actuación a la vez, **00**, **10**, **01** y **00**. En general, con n qubits podremos simular 2^n actuaciones simultáneas. De forma que si tenemos, por ejemplo, doscientos setenta qubits, $2^{270} \approx 10^{81}$, podremos obtener un número de actuaciones mayor que el número aproximado de partículas de materia que se estima que hay en el universo observado ($\sim 10^{80}$). Es decir, con un ordenador ordinario deberíamos usar toda la materia del universo para igualar la potencia de cálculo de un ordenador cuántico de 270 qubits. ¿Por qué no pensar que un ordenador cuántico de solo 270 unidades de información puede simular cualquier cosa del universo conocido? Pues precisamente porque vivimos en un mundo clásico, una naturaleza que continuamente esta *midiendo* todo, una realidad tímida que al ser observada pierde su magia. La madre del cordero del diseño de algoritmos de programación cuántica es intentar medir después de haber aprovechado todas las ventajas que proporcionan los fenómenos ondulatorios, es decir, al final. Y rezar para que nada ni nadie observe el proceso antes de ese final del algoritmo. Como veremos, son muchos más los qubits que se necesitan, en la práctica, para combatir a tanto fisgón.

2.2. ¿Paralelismo masivo?

Por tanto, si bien es cierto que los sistemas cuánticos pueden estar en varios estados a la vez, y por ende aprovechar para realizar muchos trabajos simultáneamente, también lo es que el resultado final solamente puede ser uno de todos esos estados, es decir, que somos incapaces de medir el conjunto entero en el final del proceso. El hecho de que se puedan ejecutar varias órdenes de un algoritmo, o varios algoritmos, simultáneamente, se denomina *paralelismo*. Pero, no nos olvidemos, también existe un paralelismo clásico,

aunque sea más modesto. Nuestros ordenadores de sobremesa también hacen varias tareas a la vez, especialmente desde el desarrollo, a finales del pasado siglo, de la arquitectura de múltiples procesadores. Cualquier programador hoy en día se enfrenta a la tarea conocida como *abrir hilos*, en donde pueden diseñar algoritmos que funcionan en paralelo, pudiendo ser estos procesados compartiendo tiempo de trabajo o simultáneamente por varias unidades de control. La diferencia básica entre el paralelismo cuántico y el clásico es que en el primero lo que se abren no son tareas, o procesos, sino *alternativas* de los propios estados de computación, bifurcaciones de los estados en distintas evoluciones según las distintas amplitudes de probabilidad de las distintas configuraciones. Estas amplitudes de probabilidad están representadas en el formalismo por números complejos, lo que indica que van a manifestar su carácter ondulatorio. Se cree que precisamente este carácter es el que los hace potencialmente más fructíferos, aunque esto sólo haya sido demostrado de momento en un conjunto reducido de algoritmos.

El operador o puerta lógica de **Hadamard** es una de las puertas cuánticas de mayor utilidad, ya que realiza lo que se conoce como *paralelismo masivo*. Recibiendo un estado de n qubits, lo pone en superposición de 2^n estados. Esto hace que un estado se superponga en todas las alternativas que le brinda la base computacional, es decir, que viva todas las vidas posibles. De poderse realizar y comprobar todas las tareas de las distintas ramas de la función de onda simultáneamente, desde el punto de vista de la teoría de la complejidad computacional, supondría la equivalencia entre las clases **P** y **NP**, dado que se podría verificar eficientemente por fuerza bruta casi cualquier cosa. Pero, como ya se ha comentado, en la medición a la señal solo le estará permitido manifestar una de sus vidas. El problema de la igualdad entre las clases de complejidad **P** y **NP** sigue siendo un problema abierto, y, presumiblemente, lo seguirá siendo aunque se consiga la realización material de los computadores cuánticos.

2.3. Interferencia

La supuesta supremacía cuántica no parece radicar, por tanto, en el hecho del llamado paralelismo masivo cuántico, sino en los fenómenos de interferencia, que no tienen análogo clásico. El único momento en el que clásicamente la arquitectura de los ordenadores se pregunta por las interferencias de los distintos procesos es a la hora de la compartición de recursos, especialmente en la escritura de resultados en memoria. Clásicamente, este estilo de "interferencia" se intenta evitar. Todo lo contrario al caso cuántico. En el caso cuántico los fenómenos de interferencia se promueven. Son precisamente los aliados de las ganancias de recursos computacionales, las interacciones entre los distintos estados

simultáneos es lo que hacen poderosa a la computación cuántica dentro de la teoría de la complejidad (Galindo y Martín-Delgado 2002, p. 382). Un ejemplo es el famoso algoritmo de Grover (Grover 1996).

Una de las operaciones más brillantes que se usan en los circuitos cuánticos es la llamada *inversión sobre la media*. Si se tiene una sucesión finita de números reales, $\{a_i\}$, que pueden representar las distintas amplitudes de cada una de las ramas de un estado puro, y su media aritmética es m, siempre se puede elegir otra sucesión, $\{b_i\}/b_i = 2m - a_i$, que tendrá la misma media y nos proporciona un vector con las amplitudes invertidas respecto de ese valor medio, ya que $b_i - m = m - a_i$. Esta inversión se logra aprovechando las posibilidades de interferencia constructiva y destructiva que tiene la mecánica cuántica, por medio del operador unitario *difusión de Grover*, D_n, cuyos detalles quedan fuera del objetivo de este trabajo[2]. Como ejemplo, imaginemos un estado puro de dos qubits, definido por una probabilidad de $\sqrt{1/4}$ de encontrar a los dos qubits en posición **0** y de $\sqrt{3/4}$ de encontrar el primer qubit en estado **0** y el segundo en estado **1**, siendo las dos restantes posibles configuraciones, **11** y **10**, de probabilidad nula. Se puede representar este estado puro por el vector $|\psi\rangle = \sqrt{1/4}|00\rangle + \sqrt{3/4}|01\rangle$, cuya sucesión de números asociada sería $a_i = \{0.5, 0.866, 0, 0\}$, de media $m \simeq 0.3415$. Si se aplica a este estado la puerta de difusión de Grover a dos qubits, D_2, el estado queda transformado en en el estado $D_2|\psi\rangle = 0.183|00\rangle - 0.183|01\rangle + 0.683|10\rangle + 0.683|11\rangle$, que constituye el estado imagen especular del de entrada, como se puede ver por las amplitudes de probabilidad representadas en la figura 2.1, en donde se aprecia cómo unas amplitudes ganan (interferencia constructiva) y otras pierden (interferencia destructiva) en el proceso.

2.4. Buscando una aguja en un pajar

El algoritmo de Grover trata de jugar con estos efectos de interferencia, derivados de la superposición de estados, para localizar un elemento entre un conjunto de N elementos distribuidos con probabilidad uniforme, es decir, que la amplitud de probabilidad de encontrar al azar cada uno de esos elementos es $1/\sqrt{N}$. El ejemplo más claro nos lo puede proporcionar la búsqueda de un número de teléfono en una guía telefónica. El número lo sabemos de antemano, lo *conocemos*, pero tenemos que encontrarlo en la guía, es decir, debemos *reconocerlo*. Este es un problema de los llamados de *caja negra*, en el sentido que la manera más obvia de afrontarlo es ir eligiendo cada número, sin importar su estructura, e ir comparándolo con el que estamos buscando. Una función, llamada habitualmente

[2]Se puede ver con más detalle en el propio artículo de Grover (Grover 1996) o en el capítulo 6 de la referencia (Nielsen y Chuang 2010).

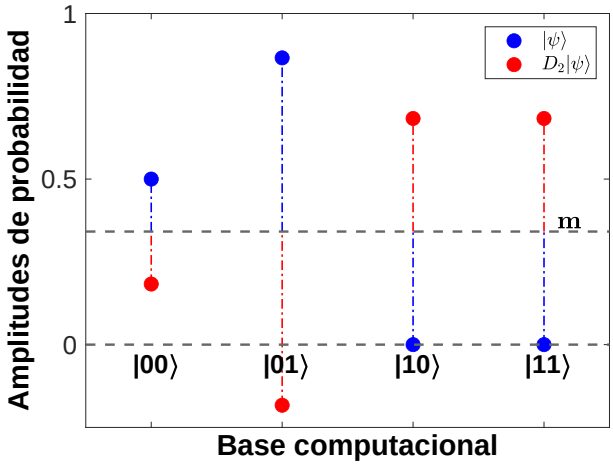


Figura 2.1: Ejemplo de actuación del *operador de difusión de Grover* a dos qubits, D_2, sobre el estado $|\psi\rangle = \sqrt{1/4}|00\rangle + \sqrt{3/4}|01\rangle$. Los puntos en azul y en rojo representan las amplitudes iniciales y las finales respecto de la base computacional. Se puede observar la inversión de las amplitudes iniciales con respecto a la media, $m \simeq 0,3415$, representada en línea horizontal discontinua.

oráculo, f, implementada en una transformación o puerta unitaria, U_f, se encarga de realizar la comprobación y devolver un valor de verdad o falsedad en cada caso. Esta solución por *fuerza bruta* nos haría comprobar toda la guía telefónica, sus N elementos, con lo que, en media, sería un problema a solucionar en $N/2$ pasos. En una base de datos estructurada u ordenada, es sabido que los algoritmos pueden alcanzar ganancias exponenciales, del orden de $\log(N)$, como en el caso de la *búsqueda binaria*. Lo que Grover demostró es que las leyes de la mecánica cuántica nos podrían dar, en estos problemas desestructurados, una ganancia, si no exponencial, sí considerable, y con su algoritmo cuántico se pasaría a una media del orden de $\sqrt{N}$ búsquedas, es decir, se produciría al menos una ganancia cuadrática[3].

Para la implementación del algoritmo de Grover bastan $n+1$ qubits para una búsqueda en una base de datos de $N = 2^n$ elementos (para que cuadre la igualdad, eventualmente se puede rellenar la lista con elementos espurios). De este modo, si clásicamente tuviéramos una media de 2^{n-1} búsquedas para encontrar un elemento conocido, cuánticamente se quedarían en $2^{n/2}$. Este algoritmo ha sido generalizado para otra clase de búsquedas y conteos, y, además, Bennett y otros demostraron que era óptimo, es decir, no hay otro

[3]Tampoco es moco de pavo. Aunque no sirva para diferenciar una clase de complejidad de otra, en un típico cálculo al margen (el *back-of-the-envelope calculation* típico de los físicos), el profesor Jonathan Dowling estima una diferencia de tiempo de búsqueda en la guía telefónica de Los Angeles de dos meses a menos de una hora, suponiendo la comprobación (u *oráculo*) de cada uno en un segundo (Dowling 2013, p. 189).

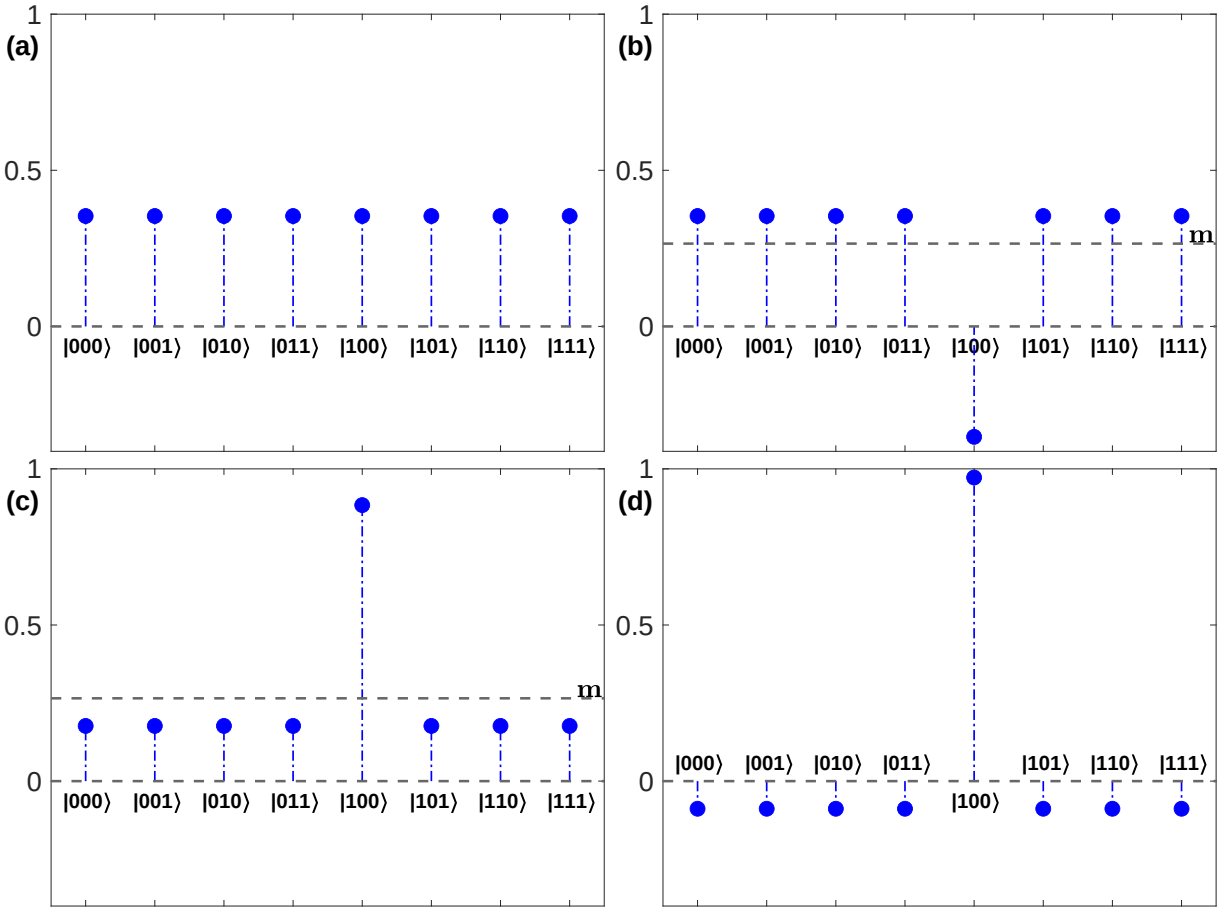


Figura 2.2: Identificación del elemento **100** en una base de datos de 8 elementos. Se representan las amplitudes de probabilidad de cada uno de los estados con respecto a la base computacional ($1/\sqrt{8}$ de amplitud, 1/8 de equiprobabilidad). (a) La puerta de Hadamard se encarga de crear una base de datos desestructurada, cuyas amplitudes de probabilidad son iguales. (b) El oráculo se encarga de invertir el estado a buscar, que queda ya marcado. (c) El difusor de Grover se encarga de hacer la inversión sobre la media, dejando el elemento a buscar con un 0.88 de amplitud ($\approx$ 77 % de probabilidad). (d) Repitiendo el proceso (b) y (c) se logra un 0.97 de amplitud ($\approx$ 94 % de probabilidad de encontrar el estado).

algoritmo cuántico que supere la eficiencia de $2^{n/2}$ iteracciones para encontrar un elemento en una base de datos totalmente desordenada (Galindo y Martín-Delgado 2002, p. 396). La razón se encuentra en los fundamentos de las reglas de la mecánica cuántica, concretamente en la *regla de Born*, que establece que las probabilidades son funciones cuadráticas de las amplitudes de los estados, cuya dependencia en las superposiciones va con $1/\sqrt{N}$ (Aaronson 2013a, p. 146). Vamos a explicar por encima en qué consiste su mecanismo.

En los estados con amplitudes constantes, como las superposiciones generadas por el operador de **Hadamard**, la aplicación de la puerta de Grover no da lugar a ningún cambio, es la identidad, ya que en este caso lo que hace es precisamente una reflexión sobre este

estado de probabilidad uniforme, cuyas amplitudes individuales coinciden con la media. Sin embargo, la idea de Grover fue implementar un oráculo para la función de búsqueda, la que *conoce* el elemento a buscar, de forma que se produjera una inversión sobre la amplitud de ese elemento[4]. Si después se hacía pasar al estado por una puerta que produjera una inversión sobre la media, como la comentada en la sección anterior, ya tendríamos la amplitud del elemento a buscar destacada sobre las demás, lo que garantizaría que, en la medida clásica del estado cuántico, el valor con más probabilidad sería el valor a buscar en la base de datos, y es en esta medida cuando se *reconocería* tal valor. Algo así como si, en un truco de cartomagia, el mago hiciera deslizar la carta buscada con un dedo oculto de forma que se destacara de las demás. En la figura 2.2 se esquematiza la búsqueda en una base de datos de ocho elementos, es decir, con tres qubits, $2^3 = 8$. El proceso del algoritmo de Grover comienza, en la figura 2.2(a), por la creación del estado de búsqueda totalmente desestructurado, es decir, en el que cada elemento tiene la misma amplitud de probabilidad de ser encontrado, $1/\sqrt{8}$. Es el estado puro de superposición que realizan las puertas de Hadamard. A continuación, en la figura 2.2(b), actúa el oráculo de localización del elemento a buscar, en este caso el estado **100**, que invierte su amplitud. En la figura 2.2(c) se realiza la inversión sobre la media a partir de la puerta de difusión de Grover, destacando ya claramente el elemento que se quiere reconocer. En este momento ya, si se midiera, se tendría una probabilidad de más del 70 % de encontrar el resultado buscado. No obstante, repitiendo de nuevo los pasos (b) y (c) se llega al estado óptimo de la figura 2.2(d), en donde la probabilidad de encontrar el elemento supera el 90 %. Pero ojo, si se hicieran más iteracciones del proceso, se perdería lo ganado, ya que el comportamiento es cíclico. De hecho, el número de iteracciones óptimo se puede comprobar que es la parte entera de $\pi\sqrt{N}/4$, es decir, en este caso de $N = 8$ elementos con dos iteracciones tenemos optimizado el problema. El caso de $N = 4$ curiosamente se resuelve con total certeza, es decir, con probabilidad igual a la unidad, con una sola consulta del oráculo.

Aunque los detalles más concretos del algoritmo están fuera de este análisis filosófico, debemos aclarar que se aprovechaba de los fenómenos cuánticos de interferencia, pero también de los de entrelazamiento. Sin embargo, es importante comentar que en el año 2000 se publicaron mejoras de este algoritmo que no necesitaban entrelazamiento para lograr la misma ganancia (Lloyd 1999). Recordemos que la obsesión contra la física cuántica de Einstein era, aparte de la incertidumbre y el antirrealismo, la no localidad. Este último aspecto se estaría evitando si uno se atuviera a los últimos algoritmos encontrados, y podría facilitar la construcción de artefactos cuánticos computacionales más concretos.

[4]Sin todavía haberlo *reconocido*, recordemos que el resultado solo se obtiene en la medida final.

Pero también conviene tener en cuenta que, como se ha visto, y en general, un algoritmo cuántico nos da el resultado buscado solamente en la medida final, y no podemos indagar en los resultados parciales que va almacenando en su recorrido. Además, es un resultado asociado siempre a una cierta probabilidad. Es esta una característica chocante de los ordenadores cuánticos. Nosotros no esperamos nunca que un ordenador clásico de sobremesa, o una calculadora, nos diera un resultado correcto solamente con cierta probabilidad. Es por esto por lo que conviene, para cerrar este capítulo, hacer una serie de reflexiones sobre la teoría de la computación probabilística y el sitio de la computación cuántica en el marco de la complejidad computacional.

2.5. Computación cuántica y complejidad

Como se ha dicho, el concepto de máquina de Turing es clave en el campo de la computabilidad. Dentro de su versatilidad, también están definidas las máquinas de Turing no deterministas, ya sean de tipo clásico, o cuántico, como la comentada máquina de Turing cuántica de Benioff-Deutsch. Dentro de la teoría de la complejidad hay un verdadero zoo de clases de problemas, pero las clases más importantes relacionadas con el azar son las clases **BPP**, **P/poli** y **BQP**. La clase **BPP** es la clase de problemas que son factibles de resolver, es decir, que se resuelven en tiempo polinómico, con un algoritmo clásico aleatorio cuyo resultado nos da una probabilidad de error acotada en 1/3. La clave de la definición es que $1/3 < 1/2$ (cualquier fracción menor que 1/2 valdría), de forma que si repetimos el algoritmo un número determinado de veces podemos hacer que el error sea tan pequeño como queramos. La llamada *cota de Chernoff* hace que la probabilidad de error disminuya exponencialmente con el número de repeticiones del algoritmo. Por supuesto, para no sobrepasar la caracterización de factibilidad, o de eficiencia, el número de veces que ha de repetirse el algoritmo no debe superar la dependencia polinomial en el tamaño de la cadena de entrada, por lo que se habla en estos casos aleatorios de tiempo polinomial *esperado*, salvo casos de pésima suerte[5]. Como una máquina de Turing determinista es un caso especial de una máquina de Turing (clásica) probabilística, los problemas de tipo **P** están incluidos en los problemas de la clase **BPP**: $\mathbf{P} \subseteq \mathbf{BPP}$. A partir de la demostración de que la verificación de la primalidad de un número se podía implementar eficientemente con un algoritmo determinista (Agrawal, Kayal, y Saxena 2004), se cree de hecho que las dos clases son la misma, pero de momento sigue siendo tan solo una conjetura. La sospecha de que $\mathbf{P} = \mathbf{BPP}$ equivale a afirmar que se puede *desaleatorizar* cada algoritmo

[5]No hay que alarmarse demasiado, como comenta con humor Scott Aaronson, la probabilidad de error se puede hacer tan pequeña como la probabilidad de que un asteroide impacte en medio del cálculo contra tu computadora (Aaronson 2013a, p. 78).

probabilístico, y según los teóricos de la computación se apoya en firmes evidencias.

Por otra parte, uno puede dejar libre la elección del algoritmo para cada longitud de la cadena de entrada, n, es decir, ayudarse de una cadena *consejo* en cada caso. Si esta cadena de ayuda al algoritmo depende polinómicamente de la cadena de entrada, estamos ante la clase de problemas **P/poli**. Son los problemas no uniformes, que desde los setenta, gracias a Leonard Adleman y otros, se sabe que al menos son tan poderosos como los problemas aleatorios, es decir, $\mathbf{BPP} \subset \mathbf{P/poli}$ (Aaronson 2013a, p. 87). De hecho, en 1982, Karp y Lipton probaron que si los problemas de tipo **NP** estuvieran contenidos en esta clase no uniforme, la llamada *jerarquía polinómica* colapsaría al segundo nivel[6] (Karp y Lipton 1982). Esto tiene como consecuencia que creer que existe una jerarquía recursiva infinita entre las clases de complejidad es equivalente a afirmar que los problemas **NP-completos** no se pueden resolver de manera eficiente por un algoritmo no uniforme. Como afirma Aaronson, esta clase de resultados de complejidad, en donde se relacionan dos supuestos no probados, puede parecer un simple ejercicio de onanismo intelectual[7], pero, para el tema que nos ocupa, las consecuencias de estos teoremas no son baladíes. En efecto, los teóricos de la teoría de la complejidad ven improbable el colapso de la jerarquía polinómica, lo que lleva a creer que en efecto no existen circuitos clásicos de tamaño polinómico que resuelvan problemas **NP-completos**, ni siquiera si se admiten algoritmos aleatorios, y esto nos lleva a la siguiente clase de complejidad, la complejidad cuántica, y a las diferencias entre la teoría clásica de la probabilidad y el azar cuántico.

Nos queda por tanto la clase **BQP**, que sería el conjunto de problemas resolubles eficientemente por una máquina de Turing cuántica con una probabilidad de error acotada en 1/3. Para empezar, en esta clase de problemas no se puede establecer jerarquía, los algoritmos de tipo **BQP** que llamen como subrutinas a algoritmos **BQP** no son más potentes que los propios **BQP**, es decir, $\mathbf{BQP}^{\mathbf{BQP}} = \mathbf{BQP}$. Esto se puede inferir de forma intuitiva por lo ya expuesto en este capítulo. Como ya se conocía desde Bennett en los 80, el secreto de la aleatoriedad cuántica está en *no calcular* o, mejor, dicho, la imposición

[6] *Grosso modo*, la jerarquía polinómica es la hipótesis de que existe una recursividad infinita entre las clases complementarias de complejidad, de modo que se pueda usar un tipo de problemas como oráculo, o subrutina, de sí mismos, con el uso de cuantificadores. En este contexto, el colapso al segundo nivel significa que las clases **NP** y **coNP** serían la misma si pudieran usar un oráculo **NP**, es decir, $\mathbf{coNP}^{\mathbf{NP}} = \mathbf{NP}^{\mathbf{NP}}$, contradiciendo la suposición de que la jerarquía es infinita.

[7] El teorema de Karp-Lipton viene a decir que si fuera verdad una cosa que nadie cree que es verdad sería verdad otra cosa que nadie cree realmente que sea verdad o, dicho de otra forma: "**if donkeys could whistle, then pigs could fly**" (Aaronson 2013a, p. 86). Aaronson, sin embargo, defiende estas cuestiones como cruciales en el pensamiento filosófico, y conjetura que la teoría de la complejidad computacional todavía no ha sido tan tenida en cuenta como la teoría de la computación en la filosofía (analítica) porque no ha tenido tiempo para entrar en la "**philosophical consciousness**" (Aaronson 2013b, p. 262).

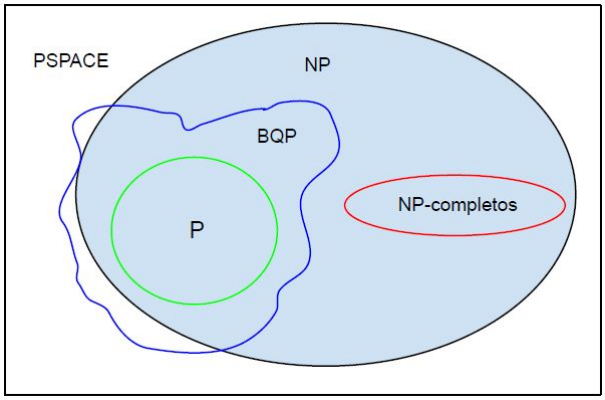


Figura 2.3: Esquema conjeturado de inclusividad de algunas clases de computación. El marco general se trata de la clase **PSPACE**, que incluye todos los problemas computables con recursos materiales clásicos limitados en espacio, aunque sin límite temporal, es decir, cuya cantidad de pasos de computación pueden depender exponencialmente de la longitud de la cadena de entrada. En ellos destacan los problemas **NP**, verificables en tiempo polinómico, representados en una elipse coloreada de azul. Dentro de esta elipse se encuentran los problemas difíciles, **NP-completos**, de contorno rojo, y los solubles en tiempo polinómico, **P**, de contorno verde. El contorno azul irregular representa la clase **BQP**, problemas que se podrían resolver en tiempo polinómico con una computadora cuántica sin errar demasiado. Su contorno irregular simboliza que esta clase de momento no encaja perfectamente en el puzzle, y por ahora su forma solo proviene de indicios.

de no medir hasta el final, dada la naturaleza del colapso de la función de onda cuántica. Por tanto, es inútil diseñar una rama con una subrutina que se deba medir en una parte intermedia del programa.

Por otra parte, se sabe que **BPP** $\subseteq$ **BQP**, lo que implica que cualquier cosa que se pueda hacer con una computadora probabilística clásica se puede hacer con una cuántica. De hecho, la puerta de **Hadamard** a un qubit simularía la tirada aleatoria clásica de una moneda. También se cree que la aleatoriedad cuántica es más difícil de *desaleatorizar* que la clásica, es decir, **P** $\neq$ **BQP**. Esto es así por el problema, resuelto por Shor, de la factorización eficiente con un algoritmo cuántico, que veremos con algo de detalle en el siguiente capítulo. De momento este problema es difícil para las computadoras clásicas, lo que lleva también a pensar, desde los años noventa del pasado siglo, que **BQP** $\neq$ **BPP**. En suma, parece que el azar cuántico es más potente que el clásico, aunque la relación de ambos con los problemas **NP** no está clara. En la figura 2.3 dejamos un pequeño esquema de inclusividad de las clases de complejidad más importantes. En el contorno de la clase **BQP** se mezclan hechos probados, como que las computadoras cuánticas pueden resolver problemas **NP**, que de momento no pertenecen a los problemas que puede solucionar en un tiempo polinómico una computadora clásica, como la conjetura de que las

computadoras cuánticas podrían incluso resolver algún problema que no fuera ni verificable en tiempo polinómico con una computadora clásica, es decir, que perteneciera a los problemas clásicos solo exponencialmente tratables en tiempo, **PSPACE**, pero no a los **NP**. También puede uno darse cuenta en este esquema el colapso que produciría el hecho improbable de que las clases **P** y **NP** fueran la misma.

Uno de los problemas cerrados en los noventa con más trascendencia filosófica es la inclusión de **BQP** en **PSPACE** (Bernstein y Vazirani 1993), ya que implica que una máquina de Turing clásica puede simular cualquier máquina de Turing cuántica, siempre que uno no tenga en cuenta su eficiencia, es decir, que aunque los recursos materiales de que disponga sean finitos, se permite que el cálculo sea en general lo lento que se quiera. Dicho de otro modo, la tesis de Church-Turing, en su forma más débil, sigue siendo válida, y solo se pone en entredicho, como ya se ha comentado, cuando uno reclama la eficiencia polinómica. El problema que sigue abierto es si la inclusión de **BPP** en **BQP** es propia, es decir, no se ha demostrado todavía si existen problemas resolubles eficientemente, con una cota aceptable de error, con una máquina de Turing cuántica, que no lo puedan ser clásicamente, aunque, como veremos en el siguiente capítulo, a partir de los algoritmos desarrollados desde finales de los ochenta por David Deutsch, Daniel Simon, Peter Shor y Richard Jozsa (Deutsch 1985; Simon 1994; Shor 1994; Jozsa 1997), se sospecha que en efecto así es.

Además, sigue sin estar probado que los problemas **NP-completos** puedan resolverse cuánticamente, y de momento se conjetura que $\mathbf{NP} \not\subset \mathbf{BQP}$. Ni siquiera, recordemos, se ha podido probar que $\mathbf{P} \neq \mathbf{NP}$, lo que daría pistas sobre la relación entre **NP** y **BQP**. Sin embargo, sí se ha probado que $\mathbf{NP} \not\subset \mathbf{BQP}$ cuando uno se ayuda de un oráculo que busca soluciones del problema a la manera del algoritmo de Grover explicado en este capítulo (Bennett et al. 1997) (en este caso el oráculo no identificaría un elemento, sino que diría si la solución encontrada es o no correcta). Esto daría, como se ha visto, una dependencia temporal de $2^{n/2}$ con la cadena de entrada, que seguiría siendo exponencial, aunque mejor que el 2^{n-1} de su contrapartida clásica. El resultado[8] indica que los algoritmos cuánticos no mejorarían polinómicamente a los clásicos en la resolución de problemas **NP-completos** por *fuerza bruta*, solo lo harían aprovechando la estructura propia del problema. Este límite cuántico, además, refleja el hecho de que, aunque en las superposiciones se pueden dar cálculos masivos en paralelo, jamás se podrán obtener todas las soluciones. Otros problemas, como la relación de la clase de computación cuántica con

[8]Parece que el trabajo de Bennett y otros fue en realidad liberado en 1994, por lo que el algoritmo de Grover, posterior, es el que vendría a confirmar la ganancia tan solo cuadrática en búsquedas por fuerza bruta, y no al revés (Aaronson 2005b, p. 5).

la jerarquía polinomial, siguen también abiertos. Con esto podemos ver la cantidad de caminos abiertos que tiene la teoría de la complejidad computacional, y especialemente con la entrada en el escenario de la computación cuántica. Se trata de una disciplina en ciernes, pero volveremos a ella esporádicamente más adelante.

Capítulo 3

COMUNICACIÓN CUÁNTICA

3.1. Información cuántica

El estudio de la información como magnitud comenzó en los años cuarenta del pasado siglo, gracias a la introducción de la unidad discretizada, el *bit*, por John Wilder Tukey, de los laboratorios *Bell*[1]. Allí también se consumó la primera teorización matemática de la información, por Claude Elwood Shannon (Shannon 1948). Pasaron casi veinte años hasta que se reconoció la naturaleza física de esa magnitud, que ayudaba a explicar paradojas como la del diablillo de Maxwell, ese ser que podía utilizar información privilegiada para burlar las leyes de la termodinámica, y otros más de veinte hasta que a finales del siglo XX se generalizara la unidad de información al *qubit*, que podía ocupar una posición intermedia a su antojo entre el **0** y el **1**. La conexión entre la computación y la física se ha ido consolidando desde entonces (Landauer 1991). El desarrollo de los algoritmos de *autómatas celulares*, esas cadenas discretas interrelacionadas por las leyes de la lógica, que pueden incluso simular los mismos comportamientos que las ecuaciones diferenciales que se discretizan en los cálculos de evoluciones físicas, ha llevado incluso a la idea de que hay que considerar a la naturaleza como un gran autómata celular, un supercomputador[2].

Esta idea, iniciada en los años sesenta por Edward Fredkin, entonces profesor del *Instituto Tecnológico de Massachusetts* (MIT), y Konrad Zuse, creador en los cuarenta del primer computador digital alemán, se asocia al sintagma *filosofía digital* u *ontología digital*[3], y han tenido entre sus defensores a científicos de la talla de Stephen Wolfram, creador

[1]En realidad, como en casi todo, sus raíces se remontan más allá. Quizás en el desarrollo del concepto de *entropía*, en torno a la segunda ley de la termodinámica, en el siglo XIX. Los protagonistas de este origen estadístico de la termodinámica serían el escocés Maxwell, el austriaco Boltzmann y el americano Gibbs.

[2]El magnífico relato *La última pregunta* de Isaac Asimov ya se planteaba, en 1956, la posibilidad de que el Universo se convirtiera en un gran computador capaz de invertir la entropía, asemejándolo a la divinidad.

[3]La corriente hunde sus bases en las alternativas al mecanicismo cartesiano, en la metafísica monadológica de Leibniz - precisamente el que formalizó la primera aritmética binaria -, cuyas sustancias son

del prestigioso software de cálculo *Mathematica*, el lógico-matemático Gregory Chaitin o el físico John Archibald Wheeler, cuya frase "**it from bit**" ha arraigado como lema en esta corriente de pensamiento. Se trata, cómo no, de nuevo de establecer puentes entre la física y la matemática, por esto a veces se les asocia con el sintagma *cuasiempirismo matemático*. Otros, sin dejar de estar en la línea de estas ideas, frente a los autómatas celulares, inclinan la balanza hacia la nueva mecánica cuántica y, recogiendo el testigo de Feynman, creen que no se pueden establecer isomorfismos entre los computadores clásicos y la naturaleza, pero sí los habría si se llegara a desarrollar un computador que obedeciera las reglas de la mecánica cuántica (Lloyd 2007, p. 51). De hecho, ven al qubit cuántico como el verdadero representante de una física que se ha demostrado indeterminista. La base discreta en la que en definitiva medimos los estados cuánticos de un qubit, vendría también a corroborar esta intuición, que se complementaría con la búsqueda de una discretización del propio espacio-tiempo relativista, en la anhelada unificación de la gravitación con la mecánica cuántica. Volveremos sobre este enfoque en la sección 4.4, por la relación que tiene con la propia admisión de la posibilidad de una computación cuántica.

En este capítulo insistiremos en esa brecha entre el mundo clásico y su unidad, el bit, y el mundo cuántico y su qubit, en el contexto de la transmisión de la información. Shannon nos demostró que el intercambio de información tampoco salía gratis energéticamente, ajustando a $kT \ln 2$ el gasto energético por bit a lo largo de un canal lineal en un ruidoso equilibrio térmico. Los estados que se pueden codificar con n bits clásicos son 2^n, pero con n qubits, como se ha visto, son potencialmente infinitos, dado que el qubit es un vector combinación lineal de los estados de la base con amplitudes arbitrarias. Pero el bit clásico era estable, y se podía copiar, generar *redundancias*, repeticiones de información contra errores. El qubit cuántico, sin embargo, es frágil, y, como se ha visto, no admite copia. Además, existe un límite, desvelado por el matemático ruso Alexander Holevo, según el cual, aunque cuánticamente se puedan manejar muchos más estados simultáneos que los correspondientes a n bits clásicos, en realidad la cantidad de información que se puede recuperar del sistema no puede exceder de n unidades clásicas (Holevo 1973).

Por tanto, estamos de nuevo en el punto de partida, y nos podemos preguntar en dónde radica la cacareada supremacía. Pero otra vez, la magia de la supuesta potencia superior de los computadores cuánticos residiría en el aprovechamiento de su capacidad de interferencia y entrelazamiento. De hecho, este último fenómeno parece ser la clave para los algoritmos de comunicación cuántica (Bennett y Shor 1998). La no localidad, que se

ahora reemplazadas por los nodos de conexión de los autómatas celulares, todo interrelacionado, a la postre, con todo. Fredkin aparece todavía detrás del sitio web digitalphilosophy.org.

deriva de las extrañas reglas de la mecánica cuántica, ayuda a esconder la información que clásicamente podría estar más expuesta. En estos enredos se fundamentan muchas de las ventajas de la seguridad en la transmisión de mensajes, la nueva criptografía, al mismo tiempo que sirven como herramienta para la corrección de errores. Asimismo, aparecen protocolos difíciles de imaginar en el mundo clásico, como la *codificación superdensa* y su corolario, la *teleportación*, de la que hablaremos a continuación.

3.2. Teleportación

La *codificación superdensa* aprovecha las propiedades del entrelazamiento cuántico para la transmisión de información entre un emisor (Alice) y un receptor (Bob)[4]. Si ambos comparten de antemano un par de qubits entrelazados, la magia de la mecánica cuántica haría que Alice solo necesitara un qubit para enviar dos bits de información a Bob (Bennett y Wiesner 1992).

Otro de los usos del entrelazamiento es la llamada *teleportación cuántica*, que fue demostrada experimentalmente a finales del pasado siglo cuando dos grupos experimentales independientes, liderados por Anton Zeilinger en Insbruck y Francesco De Martini en Roma, lograron copiar el estado cuántico de un sistema individual, como habían señalado las ideas de Charles Bennett y otros (Bennett et al. 1993; Bouwmeester et al. 1997; Boschi et al. 1998).

El nombre del fenómeno puede llevar a confusión, dado que el término a menudo es usado en ciencia ficción -la serie *Star Trek* sería un ejemplo- como la capacidad de transportar materia a distancia instantáneamente. El fenómeno cuántico aludido no transporta materia ni energía, y la transmisión de información que se da siempre lo es a una velocidad igual o inferior a la de la luz. No viola, pues, la causalidad relativista. Hay que recordar que, precisamente para salvaguardar esta causalidad, la condición lineal de la teoría cuántica prohíbe la copia de estados desconocidos, por lo que la "copia" mencionada tiene truco: el estado copiado acaba siendo desmantelado en origen.

Como es sabido, clásicamente podemos hacer copias de sistemas macroscópicos sencillos sin ningún límite, como demuestran a diario las cadenas de producción industrial. Basta conocer con detalle el diseño de un original. También, a diario, estamos *teleportando*

[4]En la literatura sobre criptografía se suelen usar siempre los mismos nombres en los ejemplos, siguiendo el orden del abecedario en las iniciales, y alternando sexos: Alice, Bob, Carol, Dave, Eve... esta última participante se suele reservar para el papel de espía o, en criptografía cuántica, simplemente el efecto del entorno. Adaptaciones al español habituales son Alicia, Benito o Eva.

información, cuando nos bajamos un artículo de *Internet*, por ejemplo. El problema de la transmisión cuántica es que no puedes *conocer* con detalle un original sin perturbarlo, y lo único que obtienes es un resultado de su gama de posibles valores superpuestos, ¿cómo transportar un estado cuántico a través de un canal clásico?. Ese problema fue precisamente, de nuevo, el que acabó siendo una ventaja. La ventaja respecto al mundo clásico es que en el dominio de la mecánica cuántica no hace falta conocer ese estado original para teletransportarlo, siempre que uno se ayude de un enredo cuántico establecido entre emisor y receptor. La desventaja, como se ha dicho, es que se trata de una copia que destruye el original y, además, debe ser única.

El algoritmo de Bennett, *grosso modo*, funciona como sigue. Alice tiene una partícula, p, en un estado cuántico, $|\psi\rangle_p$, y quiere transmitir a Bob la información suficiente para que pueda copiar ese estado que tiene la partícula de Alice (y que ella no conoce). Para ello, una tercera participante, Carol, se ayuda de dos partículas entrelazadas, a y b, del mismo tipo que la partícula cuyo estado se quiere copiar, preparándolas en un estado singlete como el explicado en la subsección 1.3.3. Carol envía a Alice la partícula a y a Bob la b. A partir de este momento, las tres partículas se encuentran en un estado que resulta ser una combinación lineal de los cuatro estados entrelazados de Bell para las dos partículas de Alice, siendo los coeficientes cuatro estados posibles en los que queda la partícula de Bob, uno de ellos igual al original de la partícula p, y los otros simples rotaciones del mismo. Basta con que Alice mida el estado de su par de partículas pa y comunique a Bob cuál de los estados de Bell ha obtenido. Esta comunicación se hace a través de un canal clásico. Concretamente, Alice comunicará a Bob dos bits clásicos de información. Bob, dependiendo de la información transmitida por Alice, aplicará la operación (rotación) conveniente al estado de su partícula, b, para obtener el mismo estado en el que estaba la partícula p a teleportar, es decir, $|\psi\rangle_b$.

Se puede comprobar, por tanto, que en la teleportación cuántica, no se realiza un viaje, sino una reconstrucción de un estado. La partícula original no se encuentra ya en el estado teleportado, o incluso puede haber desaparecido. No hay duplicación. Además, se requiere un canal clásico en el proceso, para la comunicación entre Alice y Bob, con lo que no hay violación de causalidad alguna. Recalcar también que Alice no conoce el estado de su partícula, sólo va a conocer el resultado de una medición sobre el par de partículas pa. Por último, Alice tampoco tiene por qué conocer la ubicación de Bob, la teleportación no es un proceso direccional.

Como se ha comentado, este fenómeno ha sido comprobado ya experimentalmente va-

rias veces. Originalmente los estados enredados se lograban haciendo incidir un fotón en el rango energético del espectro ultravioleta contra ciertos cristales que los separan en dos fotones entrelazados con la mitad de energía, pero hoy en día se teleportan distintos tipos de estados cuánticos, como de electrones o iones. El interés principal de este fenómeno radica en su seguridad, cualquier interceptación mínima de la señal haría que el estado no pudiera ser trasladado, lo que lo hace una buena opción para transmisiones seguras de información. Esa fragilidad también es la razón por la cual es difícil la implementación de estos experimentos. Se ha conseguido la teleportación de fotones por debajo del Danubio, unos 600 m, a través de fibra óptica, estando el record en transmisiones por tierra en solo unos cientos de kilómetros. Un equipo liderado por un discípulo de Anton Zeilinger, Jian-Wei Pan, ha logrado, en 2017, teleportar estados a través de un satélite a más de 1000 kilómetros de distancia. De hecho, entre Pekín y Shanghái se están haciendo intentos de establecer lo que sería una red de Internet cuántica. También se han conseguido teleportaciones reversibles entre luz y materia, lo que podría servir para implementar algunas ideas sobre la construcción de repetidores cuánticos (Cirac et al. 1997).

3.3. Más allá de Eratóstenes

El problema de la factorización es uno de los más difíciles en teoría de la computación. Aunque no pertenezca a la clase **NP-completos**, si se cree que está incluído en los problemas **NP** de tiempo exponencial. Esto es así porque el algoritmo clásico más común para factorizar un número grande sigue siendo el de ir probando factores desde el 2 e ir haciendo divisiones entre los siguientes números impares para comprobar los posibles restos nulos de las mismas. Variantes de la clásica *criba de Eratóstenes* que se les enseña a los alumnos de Enseñanza Secundaria (ir desvelando números primos del 1 al N a base de ir tachando múltiplos a partir del 2 hasta la raíz cuadrada del número N). La idea de la cantidad de números primos menores que uno dado la da el *teorema de los números primos*, debido en inicio a una conjetura de Gauss, que situaba la cifra de números primos menores que x en torno a x dividido por su logaritmo natural, $x/\ln x$. En realidad, como un número compuesto debe poseer algún factor menor o igual a su raíz cuadrada, $\sqrt{x}$, se suele parar ahí la iteracción, aunque eso no ayuda a que el problema no siga siendo de tipo *fuerza bruta*. Si al número se le multiplica por diez, que es como añadir una cifra, la raíz cuadrada se hace el triple. Es decir, por cada cifra se triplica el número de iteracciones, lo que da lugar a una progresión geométrica o, lo que es igual, un crecimiento exponencial. Actualmente, con la ayuda del cálculo cooperativo de cientos de ordenadores clásicos en red, no se va más allá de poder factorizar números de unas 200 cifras, tarea que conlleva años. En realidad, clásicamente, con métodos como la *criba cuadrática* o la *criba general*

de cuerpos de números algebraicos (GNFS), se ha conseguido reducir el coste exponencial de la factorización a un coste superpolinómico (o subexponencial), pero el tiempo de cálculo para números con cientos de cifras sigue siendo del orden de eones (Pomerance 1996).

Aún así, todavía nadie ha demostrado que el problema de la factorización no pertenezca a la clase **P**, es decir, que no pueda existir un algoritmo clásico eficiente de factorización de números. La sensación de los expertos es que no existe, pero quizás detrás de esta intuición solo se halle un razonamiento corporativo con tintes ególatras: "**We have spent over 100 years looking for an efficient classical factoring algorithm with no success, and we are smart mathematicians, and so therefore it does not exist**" (Dowling 2013, p. 118). La seguridad de Internet, la seguridad del mundo, descansa sobre esta suposición. La cuestión es si se puede confiar verdaderamente en esta convicción. Por ejemplo, hasta el año 2002 también se creía que no había un algoritmo determinista eficiente para decidir, sin necesidad de dar sus factores, si un número era primo o no (los algoritmos que había eran de tipo aleatorio). Si el anterior se conoce como problema de la *factorización*, este se conoce como problema de la *primalidad*, y pasó de la clase **NP** (y, de hecho, de la **coNP**) a la **P**, gracias al trabajo de un profesor indio de ciencia computacional del Instituto de Tecnología de Kanpur, Manindra Agrawal, y a sus alumnos Neeraj Kayal y Nitin Saxena (este último ni siquiera había acabado el Grado) (Agrawal, Kayal, y Saxena 2004). Su trabajo, como se ha dicho, fue liberado en 2002, enviado a expertos como Carl Bernard Pomerance -que rápidamente dio el visto bueno-, y llegó a estar en la portada del *New York Times*[5]. Su algoritmo mejoraba la criba de Eratóstenes de $\sqrt{n}$ a tan solo un orden de $\log n$, usando bases de la aritmética modular, una generalización del llamado *pequeño teorema de Fermat*, al álgebra de polinomios. El mismo Pomerance, junto a otros colegas, había estado a punto de lograrlo en 1983. ¿Cuánta seguridad transmite, pues, la suposición de que el problema de factorización no puede estar en **P**?

De momento lo que sabemos, gracias a Peter Shor, es que el problema de la factorización está en **BQP**, es decir, sí que existe un algoritmo cuántico eficiente de error limitado para factorizar números en tiempo polinómico (Shor 1994). En realidad se basó en trabajos previos de Deutsch y Simon, encaminados a desentrañar la naturaleza periódica de una función, lo que los matemáticos engloban en los llamados *problemas de subgrupo oculto* (Deutsch 1985; Simon 1994). Adaptó la llamada *transformada de Fourier cuántica* de Deutsch, para descomponer una señal en sus modos de vibración, a funciones de números

[5] `https://www.nytimes.com/2002/08/08/us/new-method-said-to-solve-key-problem-in-math.html`

enteros. El algoritmo de Shor pretende factorizar un número entero cualquiera, N, a partir de un entero arbitrario, $a \in (1, N)$, cuyo *orden módulo* N hay que hallar. Es decir, hay que calcular el menor entero, r, tal que $a^r = 1 \bmod N$. Los detalles del proceso, y de sus mejoras, se escapan al própósito del trabajo, pero cabe destacar que se aprovechan tanto potencialidades puramente cuánticas, como el paralelismo masivo y los fenómenos de interferencia, como variaciones de algoritmos clásicos como el de Euclides del cálculo de un *máximo común divisor*, que ha resistido muy bien el tiempo. Una analogía en física muy útil de por qué los mecanismos cuánticos permiten obtener información sobre el periodo de funciones de forma más rápida que los clásicos serían los experimentos ondulatorios de *difracción de Bragg*, con los que se puede extraer información del periodo espacial de una red cristalina, formada por muchos átomos, a partir de la adecuada observación de la difracción de un solo fotón.

Gracias a que la transformada cuántica de Fourier no introduce entrelazamiento, el coste de la factorización por el algoritmo de Shor resulta polinómico en el número de bits de la entrada. Se estima que consigue al menos una mejora del orden de n^2 frente a sus contrapartidas clásicas exponenciales o subexponenciales: $2^{n/2}$ nos costaría un cálculo a partir del uso de la criba de Eratóstenes, o del orden de $2^{\sqrt[3]{n}}$ en las cribas actuales mejoradas. El secreto está en el uso del paralelismo masivo para los cálculos simultáneos de las potencias modulares y la interferencia destructiva que, al igual que en la magia de la búsqueda de Grover, nos desvela el periodo oculto que servirá para hallar los factores del número.

3.4. Criptografía cuántica

El intercambio secreto de información es un anhelo que se remonta a los orígenes de la historia del ser humano. Aunque no es propósito del trabajo repasar la historia de la criptografía, hay que decir que el cifrado certificado con una demostración formal de máxima seguridad sigue siendo el llamado *cifrado de Vernam*. El también llamado método de cifrado de un solo uso (*one-time pad*), desarrollado por Gilbert Vernam en 1917, sigue siendo el más seguro para intercambiar información codificada (Vernam 1926). Si Alice quiere enviarle a Bob una cadena binaria, p, solo tiene que encriptarla con el operador **XOR** (o suma binaria), por medio de otra cadena aleatoria de la misma longitud, k, que compartan ambos de antemano. Bob recibirá la cadena encriptada $c = p \oplus k$ y la desencriptará aplicando de nuevo el operador, $c \oplus k = p \oplus k \oplus k = p$. La clave compartida debe ser de un solo uso, o el método dejará de ser seguro. Shannon demostró en sus trabajos de los 40, a partir de las propiedades de la llamada *entropía de Shannon*, que

la criptografía segura requiere que emisor y receptor compartan una clave al menos tan larga como el mensaje que se quiere codificar[6]. A esta clase de criptografía se la conoce como *criptografía simétrica*.

Una mejora al esquema de Vernam la suponen los *cifradores de flujo*, que utilizan algoritmos deterministas para generar números pseudoaleatorios que funcionen como claves de un solo uso a partir de *semillas* de menor tamaño, habitualmente de 128-256 bits. Con esto se evita que la clave compartida entre Alice y Bob tenga que ser del mismo tamaño que el texto plano. El algoritmo pseudoaleatorio debe ser determinista, es decir, a partir de la misma semilla se debe generar la misma cadena en emisor y receptor, pero debe ser impredecible, en el sentido de que no se debe diferenciar de un número aleatorio puro. Esto, lógicamente, es conceptualmente, y en la práctica, muy complicado, y de nuevo aquí viene a echar una mano la teoría de la complejidad computacional, estrechamente relacionada con la tesis de Church-Turing fuerte. Un generador será verdaderamente pseudoaleatorio si la salida no se puede distinguir de un número aleatorio puro *en tiempo polinómico*. Así, la creencia en la robustez de estos generadores descansa de nuevo en la suposición de que $\mathbf{P} \neq \mathbf{NP}$. Si estas clases colapsaran, no podría haber generadores pseudoaleatorios, ya que si la salida fuera aleatoria pura, no podría existir, dado que el algoritmo se supone determinista, y si existiera tal generador, entonces podríamos averiguar su naturaleza en tiempo polinómico, y no sería válido (Aaronson 2013a, p. 98). Es más, uno de los generadores más famosos, el llamado *Blum Blum Shub*, basado en las propiedades de la factorización de números enteros, tiene como corolario que, si hubiera un algoritmo en tiempo polinomial capaz de distinguir su salida de una aleatoria pura, se podría factorizar cualquier número en tiempo polinomial (Blum, Blum, y Shub 1996). Clásicamente ya hemos visto que se cree que esto no es posible, así que de nuevo están relacionadas dos afirmaciones no probadas del todo, que niegan dos cosas que se creen imposibles.

Pero ya hemos visto que cuánticamente sí existe ese algoritmo de factorización en tiempo polinómico. Al menos en teoría, hasta que haya ordenadores cuánticos escalables, esa es una espada de Damocles también sobre los generadores pseudoaleatorios, si bien la factorización no es la única fuente de inspiración para el diseño de generadores pseudoaletorios, y se pueden desarrollar dentro del contexto de los autómatas celulares, como la llamada *Regla 110*, desarrollada por Stephen Wolfram, que se supone de evolución impredecible. También está el aprovechamiento de la propia teoría cuántica para generar

[6]Se trata de comprobar que no hay ninguna información a obtener que relacione el texto original y el encriptado, lo que lleva a que la entropía de la clave debe ser igual o mayor que la del texto plano original. Véase, por ejemplo, la referencia (Galindo Tixaire 2007)

números aleatorios (QRNG, o *quantum random number generators*). Actualmente hay compañías, como la suiza *ID Quantique*, que implementa chips que se aprovechan de las fluctuaciones de fotones en cavidades láser para generar aleatoriedad, y ya forman parte de la arquitectura de algún teléfono móvil. Desde luego, aunque pasen todos los controles de los certificados actuales de seguridad, eso no quiere decir, a mi juicio, que se haya alcanzado la supremacía cuántica, siempre que haya algún algoritmo clásico que también los pase. Lo que es importante es que parece que sí se ha descubierto recientemente un diseño experimental cuántico que puede certificar la calificación de un número como aleatorio puro, al menos de forma tan tajante como se puede afirmar la causalidad relativista. El descubrimiento se ha realizado en el Instituto Nacional de Estándares y Tecnología norteamericano (NIST)[7], bajo la dirección del físico Krister Shalm y el matemático Peter Bierhorst (Bierhorst et al. 2018). Este es un campo que avanza con celeridad, y mientras redacto este trabajo parece que se ha implementado, bajo la dirección de la física chinoamericana Hui Cao, de la universidad de Yale, el QRNG más rápido hasta la fecha (Kim et al. 2021).

Sin embargo, la idea de la criptografía simétrica para el intercambio de información, incluso con las mejoras introducidas en los llamados *cifrados por bloques*, no es práctica, y se utiliza especialmente en comunicaciones de alto rango, como entre organismos de seguridad nacionales, o el ejército. El intercambio previo de claves supone un contacto directo entre Alice y Bob, o, cuanto menos, una comunicación que también podría ser interceptada. Y esto para cada comunicación. Por este motivo, desde los últimos años sesenta ya se estaba desarrollando en la inteligencia británica un nuevo método de criptografía, llamada *asimétrica*, por la que se podía usar una clave secreta sin contacto. Aunque los primeros en desarrollarlo fueron James Ellis, Malcolm Williamson y Clifford Cocks, el primer método de este tipo que vio la luz fue el de los estadounidenses Whitfield Diffie y Martin Hellman en 1976, aunque parece ser que fueron también ayudados por su compañero de Standford Ralph Merkle (Diffie y Hellman 1976). Vio la luz la llamada *criptografía de clave pública* (PKC), apta para dos usuarios que, sin contacto previo, quieran intercambiar información de forma secreta. La idea es sencilla, Alice tiene un secreto que mete en un cofre y lo cierra con un cerrojo cuya llave solo ella posee, lo manda públicamente a Bob, que añade un cerrojo propio, cerrando doblemente el cofre con una llave propia y reenviándolo de nuevo a Alice, que abre su cerrojo y retorna el cofre a Bob, que ya podrá abrirlo sin problemas. La confianza de este sistema, lógicamente, radica en que la apertura de los

[7]El NIST ya tenía publicados diferentes tests para comprobar la aleatoriedad de una cadena de bits, aunque hay que tener en cuenta que estas condiciones siempre eran condiciones necesarias de aleatoriedad, no suficientes, es decir, no podían garantizar la seguridad. Algunas de las condiciones que debían pasar tienen que ver con los *postulados de Golomb* (Golomb 1967).

cerrojos públicos, sin sus llaves privadas, sea difícil para cualquier interceptador del cofre.

Más concretamente, el cifrado asimétrico más popular, el llamado RSA por las iniciales de sus publicadores en el MIT, Ronald Rivest, Adi Shamir y Leonard Adleman (aunque de nuevo parece que tres años antes el británico Clifford Cocks había descubierto algo muy parecido), basa su supuesta seguridad en las propiedades de la aritmética modular (Rivest, Shamir, y Adleman 1978). Para que Bob pueda recibir un mensaje de Alice, debe hacer públicos dos números, su *clave pública*: (N, A). Para ello genera dos números primos grandes, p y q, y calcula el producto $N = p \cdot q$. Además, calcula el llamado *indicador de Euler*, $\phi(N) = (p-1) \cdot (q-1)$, y elige un número entero positivo, A, entre 1 y $\phi(N)$, que no tenga divisores comunes con $\phi(N)$, es decir, $mcd(A, \phi(N)) = 1$, y calcula el inverso de A módulo $\phi(N)$, es decir, el número A^{-1} que cumpla que $A^{-1} \cdot A - 1$ sea múltiplo de $(p-1) \cdot (q-1)$. Esta será su *clave privada*. Así, cuando Alice quiera mandarle un mensaje, m, a Bob, este solo tiene que hacerle llegar su clave pública, y Alice lo cifrará calculando la potencia $c = m^A$ módulo N. Una vez que lo envíe a Bob, este solo tendrá que hacer uso del *pequeño teorema de Fermat* para saber que $m = c^{A^{-1}}$ módulo N, abriendo el cofre con su clave privada[8]. Este sistema permite también la firma digital, sin más que mandar un anexo a los mensajes cifrado con el mismo método.

Lo esencial de la descripción de este algoritmo es quedarse con que, para un espía, calcular la clave secreta a partir de las públicas es de una dificultad comparable a la de la factorización de números enteros grandes, un problema que se cree que no está en **P**. El sistema se considera seguro por el ingente tiempo de cálculo que requeriría descifrar un solo mensaje. No significa, claro está, que no se pueda, y Martin Gardner nos demostró, en 1977, que en estos temas no hay que ser fanfarrón. En su columna de juegos matemáticos de *Scientific American*, explicando el nuevo método de encriptación (de hecho fue la primera vez que fue divulgado), lanzó el reto de descifrar un mensaje codificado en RSA-129, es decir, de 129 dígitos decimales (426 bits). Lo tituló nada menos que "A new kind of cipher that would take millions of years to break", afirmando que, según Rivest, los ordenadores de la época tardarían unos 40 cuatrillones de años en descifrarlo (Gardner 1977). En diecisiete años se apagó la magia: en abril de 1994, después del primer experimento de trabajo computacional cooperativo, coordinado también desde el MIT, en el que intervinieron 600 voluntarios y unos 1600 ordenadores durante más de seis meses, se logró descifrar. En 2005 se anunció la desencriptación de un RSA-640, es decir, la facto-

[8]La descripción contada aquí es la versión simple, llamada también *textbook* RSA (de libro de texto). En la práctica se usa una versión más sofisticada, complementada con el llamado *relleno óptimo para cifrado asimétrico* (RSA-OAEP).

rización de un número de 640 bits (193 cifras decimales)[9]. Los factores primos eran de 320 bits cada uno, lo que requirió más de cuatro meses de cálculo cooperativo entre 80 ordenadores de unos 2 GHz de velocidad. Se recomienda desde entonces que los factores primos usados en este protocolo sean de 1024 a 2048 bits, es decir, del orden de las trescientas o seiscientas cifras decimales, dependiendo de la importancia de la encriptación y, en cualquier caso, tiempos de desencriptado tan grandes siguen siendo inviables para los piratas informáticos (también llamados *hackers*).

Sin embargo, tanto este sistema de encriptado como otros tantos más o menos relacionados, basados en definitiva en la dificultad **NP** de calcular la inversa de una función, fueron puestos de verdad en jaque a partir del algoritmo de Shor descrito en la sección anterior, ya que desde entonces se sabe que la factorización está en **BQP**, lo que indica que el desarrollo de ordenadores cuánticos de forma escalable equivaldría a la capacidad para que cualquier hacker rompa este cifrado en tiempos razonables. Las leyes cuánticas se iban no obstante a aliar de nuevo con los criptoanalistas para ayudar a crear una red a este saltar por el trapecio, se iban a desarrollar los protocolos basados en la distribución cuántica de claves (QKD, *quantum key distribution*), que ayudarían a que Alice y Bob compartieran un secreto de antemano sin haberse visto e imposible de interceptar sin dejar huella.

De nuevo fue el ubicuo Charles Bennett, de IBM, junto con Gilles Brassard, de la Universidad de Montreal, los que publicaron, en 1984, el primer protocolo de distribución cuántica de claves (Bennett y Brassard 1984). Al parecer, se basaron en ideas previas de su amigo Stephen Wiesner, que había descubierto esta idea en 1969[10]. El primer protocolo de criptografía cuántica se denominó BB84 debido a estos dos autores, y más adelante, en los noventa, se desarrolló alguno más, uno del propio Bennett, el B92, y otro de Artur Ekert, el E91, muy citado, basado en las desigualdades de Bell (Bennett 1992; Ekert 1991). En general, la idea es la seguridad ante fisgones que da el principio de incertidumbre de Heisenberg. La medida de magnitudes cuánticas es irreversible, perturba el sistema y no es posible reconstruirlo. Esta es la principal diferencia con el espionaje clásico. El espía clásico puede pasar inadvertido. El espionaje del espía cuántico se asemeja más a alguien que rompe un jarrón chino en una visita a casa ajena: el *Loctite* se va a notar siempre. Eve lo tiene difícil para que su mirada no se note. Alice manda a Bob una sucesión de fotones con polarizaciones aleatorias, y Bob los mide con un medidor colocado en direcciones también aleatorias dentro de una base. Alice y Bob comparten información, por un canal

[9]Desde el RSA-576 el apellido numérico del protocolo se refiere a la cantidad de cifras binarias, no decimales.

[10]Sin demasiado éxito entre la comunidad científica. Más adelante se retiraría, por elección propia, a trabajar como obrero de la construcción en Jerusalén (Aaronson 2013a, p. 127)

clásico, sobre los modos de polarización en los que han medido los fotones, desechando los casos en los que no han empleado los mismos modos. Además, comparten también por el canal clásico la mitad de los resultados de sus medidas, para asegurarse las coincidencias, y que no han sido interceptados en el camino, desechando también estos resultados. Así, les queda una secuencia de bits común, lo que corresponderá a su clave privada. En el protocolo de Ekert, la violación de las desigualdades de Bell es la garantía que tienen Alice y Bob de que sus fotones siguen entrelazados, de que no han sido interceptados. Las propiedades cuánticas de entrelazamiento y no clonación proporcionan seguridad al encriptado. La presencia de la espía Eve queda prohibida por las leyes de la mecánica cuántica, ya que, de medir esta un estado, como mucho tendría que hacer una copia exacta y mandársela a Bob para que no se notara, lo que quedaría prohibido por la no clonación. Son, según Brassard, las leyes de la naturaleza, y no una empresa de seguridad, las que están proporcionando privacidad al sistema criptográfico, con lo que se puede asegurar su total confianza. El único problema, de nuevo, es la fragilidad de los qubits, susceptibles de corrupción, no solo por espías malintencionados, sino por el propio entorno.

3.5. Muchos mundos y viajes en el tiempo

La computación cuántica también revivió la interpretación heterodoxa de los muchos mundos, o los universos paralelos, de Hugh Everett (Everett 1957)[11]. Se trataba de nuevo de evitar el colapso de la función de onda. Ese postulado, llamado *de proyección*, de la mecánica cuántica no convencía a muchos físicos. La explicación de esta interpretación se visualiza muy convenientemente con el archiconocido ejemplo del gato de Schrödinger. Recordemos que el gato, encerrado en una caja, podría estar en un estado cuántico de vivo y muerto a la vez hasta que no la abriéramos y comprobáramos si una sustancia altamente radiactiva había hecho su efecto. Las objeciones a esta aparente paradoja tenían que ver con el advenimiento del acto de medición, que se hacía supuestamente sobre un sistema aislado, y habría a la larga que incluir en el sistema gato más variables, como el dispositivo radiactivo mismo, que también tendría que tener sus estados, o cualquier otra interacción ambiental. Esto daba lugar a una regresión infinita que solo se paraba incluyendo al propio observador en el formalismo, es decir, al final tenía que acabar inevitablemente en la consciencia de un observador humano. Así pensaba Eugene Wigner o el propio von Neumann, y derivó en especulaciones como las de Penrose, mezclando la reducción del

[11] Aunque a menudo el lenguaje es el mismo, no hay que confundir el multiverso cuántico con el derivado de la cosmología, según el cual en la inflación cósmica se crearon muchos universos sin conexión causal con el nuestro. Los muchos universos de Everett en cuántica se supone que se crean constantemente en las alternativas a cada medición, y se admiten interferencias entre ellos. Hay trabajos teóricos, no obstante, que hacen confluir las dos versiones.

paquete de ondas, o colapso cuántico, con el advenimiento de la misma conciencia[12]. De ahí sobrevinieron multitud de malentendidos esotéricos en torno a la mecánica cuántica, y, desde el punto de vista filosófico, se la asociaba con el subjetivismo.

Las reinterpretaciones de la mecánica cuántica surgidas en los ochenta, ya se ha comentado, dieron lugar a la negación del colapso de la función de onda cuántica, a la no aceptación del postulado de von Neumann. Este solo quedó como una regla mnemotécnica, para operar, sin asociarle ningún tipo de realidad física. Se relacionó, a partir de entonces, la pérdida de los estados cuánticos superpuestos, con los grados de libertad de los sistemas físicos, es decir, con la interacción con el entorno, con la entropía ambiental, en lo que se empezó a llamar «interpretación de la información cuántica». De esta manera, no hay tal paradoja en estados macroscópicos, como un gato. La caja no puede estar aislada del entorno, entre otras cosas porque el gato se supone que debe recibir oxígeno. Fue el desarrollo de la ya comentada decoherencia. Aún así, algunos físicos siguen pensando que la verdadera explicación es la de que, en cada observación, los resultados alternativos al dado, no se pierden en la interacción con el ambiente, sino que se dan en efecto en otros mundos. Es el caso de David Deutsch. El universo es un sistema libre de decoherencia, pues es un sistema cerrado por definición. Cada bifurcación de la función de onda, cada superposición, puede dar lugar a un valor medido distinto en cada universo. En un universo habrá un "yo" midiendo un gato vivo y en otro un "yo" midiendo un gato muerto. Esta interpretación es también llamada actualmente la de las «historias decoherentes consistentes».

Deutsch entiende que la computabilidad cuántica proporciona un espaldarazo definitivo a la interpretación de muchos mundos[13]. Su argumento principal, desarrollado en el texto *The Fabric of Reality*, se basa en la falta de verdaderas explicaciones que, según él, tendrían algoritmos como el de Shor para ser entendidos con las interpretaciones existentes. Para él, los cálculos cuánticos solo tienen sentido si se admite una cooperación entre muchos universos. Para factorizar un número de 250 dígitos, por ejemplo, supone que están interfiriendo nada menos que 10^{500} universos, de lo contrario uno se puede preguntar exactamente dónde se están haciendo esos cálculos (Deutsch 1997, p. 217):

[12]Sin mucho éxito esta vez, de nuevo, como en el tema de la complejidad, la estrategia consiste en asociar suposiciones indemostrables, o hechos difícilmente falsables. En este caso tres: el mecanismo de la decoherencia, el funcionamiento cerebral y la inexistente teoría de la gravitación cuántica (Penrose 1996; Hameroff y Penrose 2014).

[13]Aunque maneja una interpretación sutilmente diferente de la de Everett: para el los distintos universos no se crean en cada medición, sino que ya estaban ahí, lo único que cambia es su historia.

"When Shor's algorithm has factorized a number, using 10^{500} or so times the computational resources that can be seen to be present, where was the number factorized? There are only about 10^{80} atoms in the entire visible universe, an utterly minuscule number compared with 10^{500}. So if the visible universe were the extent of physical reality, physical reality would not even remotely contain the resources required to factorize such a large number. Who did factorize it, then? How, and where, was the computation performed?".

Ni qué decir tiene que la postura de Deutsch sigue siendo muy minoritaria en la comunidad científica. Entre los físicos le achacan especialmente consistir en una explicación metafísica, e, igual que Everett, está condenado a un camino solitario[14]. Entre los teóricos de la computación le achacan que, a la postre, su asunción parece sugerir que en efecto la factorización no está en **BPP** sobre ninguna base convincente. No se ha descartado todavía la posibilidad de que exista un algoritmo de factorización clásico rápido. Además, una objeción en la que coinciden ambos grupos es en el llamado problema de *elección de base*. ¿Cómo se elige la división entre un universo paralelo y otro? En principio en un espacio vectorial hay infinitas bases en las que se pueden bifurcar los estados. Por otra parte, la base de la computación cuántica la proporciona la interferencia, en la que los múltiples universos tienen que cooperar, un mecanismo que no queda muy claro en esta teoría. Todos los críticos acaban haciendo alusión a la *navaja de Occam*, y a la imposible *falsabilidad* popperiana de la teoría[15]. La interpretación de muchos mundos sin embargo daría una explicación, al modo del principio antrópico, de por qué nuestro universo está ordenado de forma tan patente, y por qué se dan en la física y la biología coincidencias tan notables. Es difícil explicar que a partir de un caos como el del Big Bang se hayan logrado distribuciones de materia y energía tan uniformes en el universo, y la baja probabilidad de que aparecieran organismos vivientes en él. Todo esto sería así porque vivimos en uno de los pocos universos en donde se han dado estas casualidades, y lo constatamos precisamente porque vivimos en él. A la larga se trataría de evitar una interpretación epistemológica poco convincente, como es la de la ortodoxia cuántica, con postulados de alguna manera *ad hoc*, con otra de tipo ontológico, a mi juicio menos convincente todavía.

Para cerrar esta sección, cabe destacar la idea de la resolución de problemas computacionales a través de viajes en el tiempo. A esto se han dedicado también algunos físicos

[14] Aunque en un principio apoyado por su mentor, John Archibald Wheeler, Everett no convenció, dejó la física teórica para dedicarse a la industria de defensa, y murió joven, víctima del tabaco y el alcohol. Su hijo, un conocido músico de rock, *Mr. E*, dirigió un documental sobre su padre, *Parallel Worlds, Parallel Lives* `https://youtu.be/ZnnA3sgMXCI`.

[15] En realidad, Deutsch afirma que precisamente los fenómenos cuánticos, como el de la famosa *doble rendija de Young*, son la demostración experimental de su teoría, y más lo sería el desarrollo de la computación cuántica. En el librito de entrevistas *El espíritu en el átomo* habla de un posible experimento crucial, que parece más bien de nuevo pura especulación (Davies y Brown 1989, p. 130).

y teóricos de la computación. No vamos a compendiar aquí las limitaciones que existen en la física relativista para estos viajes, especialmente para aquellos que se realizan al pasado, ni las paradojas y reflexiones a las que conducen, como la famosa *paradoja del abuelo* o la limitación del libre albedrío del viajero en el tiempo. Hay estructuras, dentro de la relatividad general, que admiten bucles temporales, aunque sean hoy en día muy especulativas. Pero el asunto es, por supuesto, qué pasa si podemos mandar bits al pasado. Si las restricciones de la relatividad general parecen condenar los viajes en el tiempo clásicos, no está tan claro si las leyes físicas permiten o no las llamadas "curvas cerradas de género tiempo" (CTC). Un estudio sobre la consistencia causal en esta clase de curvas lo hizo, cómo otro, David Deutsch, en 1991 (Deutsch 1991). Allí demostraba que la estructura probabilística de la mecánica cuántica podría proporcionar vías de comunicación que no afectaran causalmente a la historia y, por tanto, evitaran paradojas como la del abuelo. Trabajos posteriores de Bennett y Lloyd parece que han limitado, sin embargo, este punto de vista (Aaronson 2013a, p. 320).

En cualquier caso, volviendo a la computación, la idea, por supuesto, es dejar lanzado un programa en un ordenador que, con un algoritmo de fuerza bruta, calculara los casos que se dieran en un problema **NP-completo**, y dejarlo correr hasta que alcanzara la solución. Si esa solución nos pudiera ser comunicada desde el futuro, tendríamos, por supuesto, el colapso $\mathbf{NP} = \mathbf{P}$ garantizado, es decir, podríamos resolver cualquier problema **NP** de manera eficiente (Bacon 2004). De hecho, podríamos resolver cualquier problema de la clase **PSPACE**, es decir, aquellos que agotan recursos materiales solamente de forma polinómica respecto al tamaño de la entrada, pero que pueden ser temporalmente exponenciales. Más allá se ha demostrado que no se podría llegar. En 2008, Scott Aaronson y John Watrous demostraron que no se podrían resolver problemas que no estuvieran limitados polinómicamente al tamaño de la memoria del ordenador, con lo que se concluye que en realidad nos daría igual qué clase de computación utilizar o, dicho de otra forma, si existiesen las curvas temporales cerradas, los ordenadores cuánticos no serían más potentes que los clásicos (Aaronson y Watrous 2009).

Capítulo 4

MATERIALIZACIÓN

4.1. Ordenadores cuánticos

El pistoletazo de salida para la construcción material de ordenadores cuánticos lo supuso la llamada *trampa de iones*, ideada en 1995 por Juan Ignacio Cirac, profesor entonces de la Universidad de Castilla-La Mancha, y Peter Zoller, de la Universidad de Innsbruck (Cirac y Zoller 1995). Se trata de aislar unos pocos átomos, despojados de un electrón, y colocarlos en el vacío formando una hilera suspendidos gracias a campos electromagnéticos producidos por electrodos. La fuerza coulombiana de repulsión de cargas iguales que opera entre ellos actúa de enlace, de modo que cualquier presión a uno de ellos se transmite a todos los demás. Cada ión está controlado por una luz láser, que puede actuar individualmente sobre uno de ellos, provocando transiciones electrónicas, o sobre toda la hilera. Así se crean unas ligaduras entre los iones que pueden crear entrelazamiento, y se pueden diseñar puertas lógicas cuánticas que, como hemos visto son los bloques básicos con los que se puede hacer cualquier computación. Concretamente se han implementado puertas **CNOT** con esta clase de dispositivos. El problema es que estos iones atrapados deben estar en el vacío, a temperaturas cercanas al cero absoluto, y los láseres que se encargan de la estructura de los enlaces entre ellos deben tener precisiones enormes. La susceptibilidad a interacciones electromagnéticas ambientales también es grande. Solamente se mantienen controlados del orden de una decena de átomos, cuando se estima que para realizar un cálculo significativamente comparable a un ordenador clásico se deberían controlar de entre 70 y 100 qubits. Normalmente, los estados de superposición de átomos se mantienen, salvo casos excepcionales, a lo sumo durante unos pocos microsegundos, cuando la interacción con el entorno se produce. La tendencia, dado que largas cadenas de iones son imposibles de controlar, es agruparlos por bloques aislados. *IonQ*, una empresa emergente de *Google*, está desarrollando tecnología escalable de iones atrapados (Monroe y Kim 2013).

Otra estrategia para la implementación de un ordenador cuántico ha sido la de los circuitos elaborados con materiales superconductores, en donde los **0** y **1**'s de los qubits son representados por el sentido horario o antihorario de la corriente eléctrica que recorre el circuito. Esta es la línea fundamental de la empresa canadiense *D-Wave*, pionera de la computación cuántica, pero también la implementan la propia *Google*, *IBM* o *Rigetti*. Según los defensores de esta técnica, sería la más susceptible de escalación, y están trabajando con cientos de qubits, aunque la mayoría se utilizan para la corrección de errores, y de nuevo solo quedaría un número del orden de las decenas para elaborar cálculos competitivos (Pudenz, Albash, y Lidar 2014a).

Por último, parece que de la física del estado sólido podría venir otra de las fuentes de implementación de ordenadores cuánticos, gracias a la codificación en qubits de los estados de espín de ciertos materiales. En especial, las redes de diamante, como las que fabrica la empresa británica *Element Six*, podrían simular el comportamiento atómico gracias a la introducción de impurezas de nitrógeno o silicio. Esta técnica está siendo desarrollada por el físico ruso de la Universidad de Harvard Mikhail Lukin (Nguyen et al. 2019), cofundador de la empresa *Quantum Diamond Technologies*, dedicada a la implementación de dispositivos cuánticos para el diagnóstico médico.

Aunque sin ninguna duda se consiguen pequeñas metas importantes, los ingenieros cuánticos siguen luchando contra los problemas que se encuentran en la construcción de ordenadores cuánticos. Hoy en día, por ejemplo, no es difícil conseguir temperaturas cercanas al cero absoluto, pero a medida que se aumenta el número de qubits y de puertas cuánticas, la tasa de errores se dispara, y, como se ha visto, los algoritmos cuánticos ya son en esencia probabilísticos, con lo que la ventaja con la computación clásica se pierde. Se estima que las mejores puertas cuánticas materializadas tienen un error por cada 200 operaciones (0,5 %), cuando la tasa de errores clásica está en uno por cada 10^{17}. Parece que, aparte de todas estas tecnologías estudiadas, hace falta un gran salto, como el del invento del transistor de los cuarenta.

4.2. Retórica cuántica

Es muy difícil hacerse una idea de cuándo podremos tener un ordenador cuántico universal escalable. Recordemos, a modo de analogía, lo que sucede en la rama biosanitaria: las noticias lanzadas por los laboratorios y los centros de investigación confunden a los legos en la materia. No hay una semana, por ejemplo, que no se oiga en algún telediario alguna cura de algún cáncer y, sin embargo, todos sabemos que sigue siendo una enferme-

dad complicada de tratar, al menos farmacológicamente. Evidentemente, se hacen avances significativos en casos especiales, y se están curando muchos más tumores de los que se curaban hace veinte años, pero no se puede decir que haya una cura contra el cáncer, ni siquiera contra un tipo concreto, o al menos no tan definitivamente. En computación cuántica asistimos a un fenómeno publicitario parecido, los plazos se alargan cada vez más, y, sin embargo, se tiene la sensación de que es algo que va a tardar poco en alcanzarse, y a menudo saltan noticias afirmando que alguna empresa, de hecho, ya lo ha logrado.

El algoritmo de Shor se materializó por primera vez en 2001, con siete qubits, correspondientes a los espines de siete núcleos atómicos, logrando la factorización del número 15 (Vandersypen et al. 2001). El equipo fue liderado por Isaac Chuang, de la Universidad de Stanford, en una investigación de la empresa IBM. Las noticias decían que 15 era igual a 3x5 la mayor parte de las veces (otras no). En el desarrollo de esta técnica se usaron los llamados *trucos de precompilación*, para cablear el algoritmo usando información a priori (es decir, los factores del número)[1]. Una técnica sin esta limitación se publicó en 2016 en la revista *Science*, usando cinco átomos atrapados con una alternativa al algoritmo de Shor llamado algoritmo de Kitaev (Kitaev 1995; Monz et al. 2016).

En cuanto a supuestos computadores escalables, existen fundamentalmente dos arquitecturas, la que se basa en el llamado temple cuántico (*quantum annealing*), en donde se diseña un modelo cuyos estados energéticos corresponden con el problema a resolver, usado por la empresa *D-Wave*, y las que intentan el desarrollo de los bloques básicos de la algorítmica, las puertas cuánticas, que desarrollan *IBM*, *Google* o *Rigetti*. La mencionada empresa *D-Wave*, por ejemplo, presentó en 2007 su sistema de computación cuántica *Orion*, que se pudo confundir con el logro de un verdadero ordenador cuántico. En realidad, se trataba de un dispositivo diseñado especialmente para una función, un acelerador de hardware para resolver el llamado *problema de Ising* bidimensional, una red de espines acoplados interaccionando, según las leyes de la mecánica cuántica, dentro de un campo magnético, con un sistema de 16 qubits[2]. *Google* y la *NASA* adquirieron los sistemas de *D-Wave* en 2011, cuando esta empresa comenzó a vender "ordenadores cuánticos", y desde entonces la liberación de sus nuevos productos no ha parado, si bien sigue habiendo un ambiente bastante escéptico en cuanto a sus logros (anuncian miles de qubits), ya que las

[1] Véase, por ejemplo, el blog del físico Francisco R. Villatoro, `https://francis.naukas.com/2016/03/07/cifrado-con-un-ordenador-de-5-cubits/`

[2] En las noticias de la revista *Scientific American* se puede leer, con algo de ironía, el epígrafe : "**First "Commercial" Quantum Computer Solves Sudoku Puzzles**", dado que uno de sus objetivos era la implementación del programa *SudoQ* para la resolución de estos acertijos. Aaronson tiene también una entrada en su blog muy esclarecedora con preguntas y respuestas acerca del "anti-bombo" sobre el sistema *Orion*:`https://www.scottaaronson.com/blog/?p=198`

pruebas de su supremacía se ponen en cuestión, objetando que no logran más velocidad que los ordenadores comunes (Jones 2013; Pudenz, Albash, y Lidar 2014b).

El público general asiste desde hace años a una ceremonia de la confusión a propósito de la consecución de la construcción del primer ordenador cuántico. A menudo los dispositivos no son programables, o mezclan tecnologías clásicas con cuánticas, y no acaban de demostrar su superioridad respecto a las máquinas clásicas, cuyos algoritmos, por otra parte, cada vez son más eficientes. La algorítmica cuántica no es demasiado rica, y la supremacía cuántica no parece estar definitivamente demostrada en ningún supuesto nuevo computador universal. A pesar de ello, la empresa *Google* ya anunció, en 2017 y en 2019, que la había alcanzado, por medio de un computador cuántico de 53 qubits [3]. Fue un ingeniero informático español, Sergio Boixo[4], el que dirigía la división de programación en este caso (Boixo 2018). Uno de los problemas de esta clase de anuncios es que a menudo, seguramente por cuestiones de privacidad empresarial, no van acompañados de una publicación de sus diseños y resultados concretos en revistas de revisión por pares, como exige la ortodoxia metodológica en la ciencia actual. Científicos independientes podrían analizar las metas a las que se ha llegado y aquellas a las que no se ha podido llegar con tal o cual experimento, al margen de cuestiones fundamentalmente publicitarias (la empresa *D-Wave* tiene registradas más de cien patentes relacionadas con su tecnología cuántica). Por supuesto, la empresa *IBM*, uno de sus competidores, no tardó en ponerlo en duda[5], arguyendo que la tarea que resolvía la computadora de *Google*, que supuestamente necesitaría 10000 años en una computadora clásica, ellos en realidad la podían implementar clásicamente en dos días y medio con mayor precisión.

La mayoría de los expertos afirman que la computación cuántica universal escalable no está a la vuelta de la esquina, aunque los periodos de tiempo que auguran que han de pasar para que se dé varían mucho (el más optimista que yo haya leído es el de un ingeniero de *Intel*, que en 2018 dijo que en diez años estaría resuelto). El tema de la supremacía cuántica, como comenta Aaronson en su blog[6], no puede estar tan claro. No se trata de la conquista de la Luna sino más bien, si no de la mencionada lucha contra el cáncer, sí de una lucha contra una epidemia (de la que desgraciadamente en las últimas fechas sabemos mucho). La tecnología cuántica puede conseguir hitos importantes, pero la clásica puede contraatacar, tanto por el diseño técnico de sus estructuras, como por su

[3] En octubre de 2019 la misma Ivanka Trump puso un tweet anunciando que *Google* había conseguido el logro con ayuda de la Administración de Trump, de la que no había recibido un centavo (Dowling 2021, p. 212).

[4] Sergio Boixo también es licenciado en filosofía por la UNED.

[5] Véase `https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/`.

[6] `https://www.scottaaronson.com/blog/?p=4372`

algorítmica lógico-matemática, para resolver cualquier problema.

4.3. Criptografía y dinero cuánticos

Si el desarrollo de los ordenadores cuánticos escalables parece avanzar muy lentamente, en el terreno de la criptografía cuántica se van consiguiendo hitos importantes. El primer experimento relacionado con la criptografía cuántica fue implementado en octubre de 1989 (Bennett y Brassard 1989; Bennett et al. 1992). Fueron los mismos autores del protocolo BB84 los que lo comprobaron con luz polarizada, en un montaje de aproximadamente un metro de longitud entre Alice y Bob. A partir de ahí, este campo es el que ha sido más ampliamente desarrollado en la práctica. En 2006, en *Los Alamos*, se implementó el protocolo BB84 a lo largo de 148.7 km de fibra óptica (Hiskett et al. 2006), y, a través del aire, destacar el experimento entre las islas de *La Palma* y *Tenerife*, en 2007, salvando sus aproximadamente 144 km de distancia (Schmitt-Manderbach 2007)[7]. Como ya se ha comentado, el objetivo ahora son las comunicaciones Tierra-Espacio-Tierra por medio de satélites, y en eso China ha tomado la iniciativa. En 2016 se puso en órbita el satélite cuántico *Mozi*, y actualmente el récord de una conferencia segura y fluida lo tiene la que establecieron, gracias a Jian-Wei Pan y Anton Zeilinger, el presidente de la Academia Austriaca de Ciencias en Viena y el de la Academia China en Pekín. La comunicación segura a 7500 km de distancia perteneció a una misión que costó alrededor de 100 millones de dólares[8].

Ya se pueden comprar artefactos de encriptado cuántico, ya que hay varias empresas dedicadas a ello. Especialmente lo hacen instituciones financieras y gubernamentales. La empresa de Ginebra *Id Quantique SA* proporciona un alcance de decenas de kilómetros por fibra óptica. De hecho, desde 2007 el sistema criptográfico instalado por esta empresa proporciona seguridad a la red de comunicaciones en las elecciones cantorales entre los centros de recuento en Ginebra y los repositorios del gobierno. Esta empresa también es famosa por ofrecer chips de generación cuántica de números aleatorios. Otra destacada es la americana *MagiQ Tecnnologies*, que trabaja principalmente para el Ejército, proporcionando alcances seguros de cientos de kilómetros.

[7]Como chascarrillos acerca de estos experimentos, decir que en los primeros montajes de Bennett y Brassard, este último cuenta que la fuente de alimentación emitía tanto ruido en las emisiones, que casi se podían "oír" los fotones y sus polarizaciones, con lo que Eve debería estar sorda para no interceptar el mensaje simplemente escuchando (Brassard 2005). En cuanto a los experimentos de Canarias, preguntado Anton Zeilinger sobre la elección de su ubicación, este dio cuatro razones: su despejada atmósfera, que el tiempo era mejor que en Viena, que era una oportunidad de salir del alcantarillado vienés y la cuarta fue en forma de pregunta:"**you have never had good Spanish wine?**" (Dowling 2013, p. 249)

[8]Ver `https://en.wikipedia.org/wiki/Quantum_Experiments_at_Space_Scale`

Los organismos bancarios tampoco son ajenos a la revolución de la computación cuántica. En 2004 se realizó en Viena la primera transferencia bancaria cuántica entre el Ayuntamiento y el *Bank Austria* situado a 500 m. En 2017 el *Russian Quantum Center* de Moscú estableció el primer enlace seguro operativo entre dos sedes bancarias del *Sberbank* a través de 25 kilómetros. Por otra parte, la idea germinal del *dinero cuántico* fue de Stephen Wiesner , en su famoso artículo de 1969 que no fue publicado hasta los ochenta (Wiesner 1983), gracias a la revisión de sus ideas en un congreso celebrado en *Puerto Rico* (Bennett et al. 1992). La idea es crear billetes bancarios imposibles de falsificar, grabando los números de serie en estados cuánticos de espín o polarización de fotones dentro de ellos. En realidad serían más bien los correspondientes a cheques, ya que el banco tendría que verificarlos a través de un registro de polarizaciones y números de serie. Cualquier intento de copia destrozaría el estado cuántico grabado y no se podría validar en el banco. El problema sigue siendo la fragilidad, y el dinero cuántico no es algo en lo que se este apostando de momento, dado que deberían estar más desarrolladas las memorias cuánticas (los estados cuánticos, como se viene comentando en este trabajo, pierden su integridad en poco tiempo).

4.4. Disidencia

Actualmente hay un grupo de científicos, como Leonid Levin, Oded Goldreich, Gerardus 't Hooft, Gil Kalai y otros, que no creen que la computación cuántica sea posible. Entre los argumentos que esgrimen para su negación los hay, de nuevo, de tipo físico y de tipo matemático-lógico, normalmente relacionados con los campos de estudio de los autores en cuestión, aunque sustancialmente manejan siempre algunas ideas de índole filosófico.

Los argumentos de tipo físico están relacionados con cálculos de tamaño, que dan lugar a límites prácticos en la implementación de los cálculos que se podrían llevar a cabo en esos ordenadores, con el inherentemente ruidoso carácter de las señales que deben manejar, y con la imposibilidad de controlar el aislamiento que se debe dar en los componentes de todo ordenador cuántico. Todas estas consideraciones están, a la postre, relacionadas, pues la susceptibilidad a los errores de las implementaciones materiales de los algoritmos cuánticos hace que se deban crear, como se ha comentado, múltiples redundancias, es decir, conjuntos añadidos de qubits transportando la misma información, para que la pérdida de varios de ellos en el proceso no afecte demasiado al resultado final, y este se pueda dar con un margen adecuado de precisión. Algunos creen que hay una distancia insalvable, con la tecnología actual, entre las decenas de qubits que hoy en día pueden

controlar los laboratorios de las grandes empresas, a los millones de ellos requeridos para que la computación cuántica escalable sea un objetivo factible.

En efecto, el problema de la decoherencia, o interacción con el entorno, de los estados cuánticos en superposición, es un problema que se agrava de forma exponencial, dado que la probabilidad de la intersección de un conjunto de sucesos independientes es el producto de sus respectivas probabilidades, y por cada qubit que añadimos al sistema el estado del mismo es mucho más difícil de controlar. Para evitar esto, la herramienta más inmediata que se está aplicando es la mencionada corrección de errores por redundancia. Sin embargo, actualmente se estima que la razón de redundancias que debería de haber por cada qubit es $1 : 10^4$, con lo que, si quisiéramos tener un ordenador cuántico con mil qubits operativos, deberíamos en realidad tener la capacidad de construir una máquina con cien millones de qubits (Cirac 2019, m. 34). Ateniéndonos a lo lento que está avanzando el desarrollo de máquinas con unas decenas de qubits, el augurio no puede ser muy esperanzador.

Gerardus 't Hooft, por ejemplo, pronosticó en el año 2000 que un ordenador cuántico no podría factorizar enteros de más de unos miles de cifras decimales. El problema de la decoherencia para él es un problema irresoluble. Su argumento se basaba en la impredecibilidad de la teoría cuántica en las escalas llamadas de Planck, en donde se define un volumen mínimo esencialmente indeterminado en donde, según él, se produce disipación de información. Las interacciones no deseadas con el sistema son inevitables. Estimaba que un ordenador que ocupara el espacio de un cubo de alrededor de diez metros de arista no sería capaz de factorizar numeros mayores de unas cuatro mil cifras. Paul Davies se alinea con este grupo de objeciones, afirmando que los estados exponenciales no son físicos, debido al llamado *principio holográfico*, desarrollado por el mismo 't Hooft y Leonard Susskind[9], que establece un límite superior al conjunto de bits que pueden ser almacenados en una región finita del espacio-tiempo (Davies 2007, p. 81). Leonid Levin, por su parte, afirma que son las minúsculas amplitudes que entran en juego en los procesos de computación cuántica las que tampoco son físicas. El mismo Set Lloyd, aunque confíe en el desarrollo tecnológico de la computación cuántica, puso límites físicos a la computación (Lloyd 2000).

Desde la perspectiva matemática e informática, también piensan algunos que la reducción del ruido no es tan solo una cuestión de ingeniería. Así piensa el matemático Gil Kalai, que ha trabajado en la interacción de los errores provocados por las fluctuaciones

[9]Basándose en los estudios sobre la termodinámica de la información en torno a los agujeros negros llevado a cabo por los desaparecidos Jacob Bekenstein y Richard Hawking en los setenta, según el cual toda la entropía de un agujero negro sin rotación ni carga yace en su superficie.

de los procesos asociados al cómputo cuántico. Las correlaciones de estos errores hacen que haya probabilidades no nulas de que afecten a muchos qubits a la vez, con lo que ni siquiera la redundancia los pondría a salvo. Con técnicas relacionadas con el análisis de Fourier, este autor afirma que existe un umbral de ruido que no se puede reducir. De este modo objeta que la decoherencia siempre será mayor que el umbral de tolerancia a fallos y que los errores no son independientes, dos de las objeciones más importantes que apunta Aaronson en su texto.

Otra línea alternativa, como la del físico Stephen Wolfram, es defender, de una u otra forma, la verdad de la tesis extendida de Church-Turing. Así se retoma la idea del universo computable de Edward Fredkin y Konrad Zuse, llevándola a las últimas consecuencias. En este caso, al defender una algorítmica clásica (aunque su sistema, según él, va más allá de los autómatas celulares), de alguna manera están soterrando la supremacía cuántica. Estos físicos, ya se ha comentado, piensan que el universo, aunque no sea aprehendido por la matemática, sí puede serlo digitalmente. Wolfram defiende que, a partir de sencillos programas de ordenador, se puede generar una gran complejidad[10]. Si bien no hace un análisis dentro de la teoría de la complejidad computacional, su llamadoo *principio de equivalencia computacional* afirma que todos los sistemas naturales son sistemas de cómputo, desde el funcionamiento del cerebro humano hasta la meteorología. De hecho, propuso una de las llamadas *teorías del todo* a partir de variantes de los autómatas celulares clásicos, aplicando la teoría de grafos, con lo que tácitamente se admite que la computación cuántica no añadiría cualitativamente nada más a la cuántica, negando su supremacía. Famosa es su aludida *Regla 110*, una versión de una máquina de Turing universal.

Detrás de esto parece que de nuevo está el debate kantiano entre el mundo y su cognición y, de esta manera, se vuelve al principio de este trabajo, con las ideas germinales de Feynman y el mismo debate de la teoría cuántica. Los físicos posteriores a la primera generación de cuánticos en su mayoría habían aceptado la interpretación de Copenhague y su antirrealismo. Pero si uno afirma, como hacía Feynman, que para simular la naturaleza no nos valdrían dispositivos clásicos, porque la propia naturaleza *es* cuántica, está aceptando como verdad el concepto de supremacía cuántica y negando la tesis extendida de Church-Turing. Si, a partir de ese principio anunciado por Feynman, del que han bebido muchos de los científicos que hemos estudiado aquí, se cree que la computación cuántica va a ser imposible, se tendrá que aceptar que nuestro acceso a la naturaleza va a estar inevitablemente mutilado. Desde posiciones antirrealistas contemporáneas, como la

[10]Nada nuevo, le dicen, la *teoría del caos* ya demostró esto décadas antes.

del científico computacional Oded Goldreich, por ejemplo, se invierten las implicaciones anteriores y se acaba dudando de que la computación cuántica sea un objetivo alcanzable algún día.

Aún así, creemos que la investigación en el desarrollo de la computación cuántica, como tantas otras que a menudo parecen alejadas de las necesidades reales de la sociedad, no va a caer en saco roto. La cantidad de resultados, más técnicos que teóricos, a los que se está llegando, siempre contribuye a un fondo de conocimiento que puede algún día dar a luz algún descubrimiento más importante. Quizás haya que dar eso, un gran salto, como el que supuso el transistor, pero el camino no deja de ser fructífero por ello. Acabo el capítulo con unas palabras de un físico cuántico francés, el premio Nobel Serge Haroche, otro de los escépticos sobre la computación cuántica, en este mismo sentido (Haroche y Raimond 1996, p. 52):

"The newly discovered strategies for partially controlling the effects of decoherence, which would have been deemed impossible until very recently, greatly advance our understanding of dissipation in mesoscopic systems. Testing quantum decoherence in conceptually simple experiments is also an important and challenging task. Rather than teaching us how to build a large quantum computer, such experiments are more likely to teach us about the processes that would ultimately make the undertaking fail. It is important to advertise this fascinating subfield of quantum optics for what, it really promises, which is a deeper insight into the most counterintuitive theory yet discovered by physicists..".

CONCLUSIONES

En este trabajo se ha hecho un recorrido por las ideas y los hitos más importantes que se han dado en los últimos cuarenta años, desde la caracterización en los ochenta de la máquina de Turing cuántica universal, en torno a la computación cuántica. El origen de nuestras reflexiones ha estado en el desarrollo material de la computación y en los límites a los que se enfrentaba esta cuando se acercaba al dominio de la física cuántica. Los primeros autores, como Feynman o Benioff, se dedicaron a adaptar los principios de Turing a estas leyes, y, por otra parte, la teoría de la complejidad matemática requirió una revisión de la llamada tesis de Church-Turing, para adaptarla a la eficiencia polinómica de la nueva teoría de la complejidad computacional en desarrollo. De este modo, esta tesis extendida, que venía a afirmar que los ordenadores cuánticos no eran más potentes que los clásicos, era puesta en cuestión. A partir de los trabajos de los primeros científicos dedicados a las nuevas ciencias de la computación, como Edward Fredkin, Charles Bennett o David Deutsch, se desvelaron los retos a los que se podría enfrentar la tesis de Church-Turing dentro del nuevo paradigma, en el que confluían la matemática, en la teoría de la complejidad computacional, y la física de la teoría cuántica. Naturaleza y computación, física y matemática, deberían ajustarse al paradigma cuántico, recuperando algunas de las ideas clásicas de teóricos de la información de la primera mitad del siglo XX, como Claude Shannon o Alfréd Rényi.

Hemos dado también algunas pinceladas de lo que supone la algorítmica cuántica como motivación para el desarrollo material de esta nueva rama de la ciencia. Pocos algoritmos, pero prometedores, abarcando dos grandes retos de la ciencia de nuestros días. Nos hemos parado a explicar un poco más en detalle el algoritmo de Grover, de 1996, por lo que tiene de relación con la solución de los problemas de gran complejidad por el método de fuerza bruta, también llamado de *caja negra*. Hoy en día es un debate abierto si la prueba de un teorema matemático, por ejemplo, puede aceptarse a partir de un ingente cálculo de todos los casos implicados, como las llamadas *demostraciones de conocimiento cero*, o debe hacerse solo mediante una formalización deductiva rigurosa. El algoritmo de Grover, diseñado en principio para búsquedas en bases de datos desestructuradas, vendría a supo-

ner una ventaja computacional importante para cualquier clase de problema que busque la solución correcta entre muchas otras soluciones incorrectas por el método de la caja negra. Aunque este algoritmo, como hemos visto, no otorga a la computación cuántica una ventaja exponencial respecto de la clásica, sí es cierto que el ahorro de tiempo para resolver este tipo de problemas, de existir los ordenadores cuánticos escalables, sería notable. Por otra parte, hemos visto la amenaza que supone, para la seguridad informática de una sociedad cada vez más digitalizada el otro gran algoritmo cuántico, el de Shor, de 1994, y la carga teórica que tiene en cuanto a la defensa de la consecución de la supremacía cuántica, o, dicho de otro modo, de la demostración de la falsedad de la tesis de Church-Turing extendida.

Por otra parte, hemos visto también las limitaciones de la computación cuántica, tanto físicas como lógico-matemáticas. En el terreno de la física, se ha analizado el llamado paralelismo masivo cuántico que, en principio, da a entender que la computación cuántica va a proporcionar una ganancia de tipo exponencial en la resolución de cualquier problema. Esto no es así por razones físicas, ya que la medida en mecánica cuántica solo permite obtener el resultado de una de las ramas de la función de onda, que supuestamente están haciendo cálculos en paralelo, desperdiciando todas las demás. Pero tampoco la ganancia de un algoritmo cuántico que busque soluciones por fuerza bruta es, como se ha visto, de orden exponencial. Como demostraron Bennett y, posteriormente, con el algoritmo de Grover, la importante ganancia que se consigue, sin tener en cuenta la estructura del problema, es tan solo cuadrática.

Se ha hecho un somero repaso por la materialización de esta clase de computación, y las distintas técnicas que se están utilizando para llevarlas a cabo. Asimismo, se ha indicado la dificultad que conlleva, por efecto de la confusa propaganda empresarial, darse cuenta hoy en día de exactamente en qué punto está el desarrollo de una computadora cuántica universal escalable, y si esto va a ser posible algún día. La carrera está liderada por empresas como *Google*, *IBM*, *IonQ*, *Alibaba*, *Microsoft*, *Intel* y algunas otras. La narrativa asociada con la consecución experimental de ciertos logros por parte de estas grandes empresas, algunas de ellas cotizando en los mercados financieros, no ayuda al esclarecimiento del punto exacto en donde se encuentran las investigaciones. Pareciera que se ha tomado en serio la tradición de la retórica en ciencia moderna en torno a los descubrimientos científicos, empezando por la publicidad de las investigaciones ópticas de Isaac Newton, que constituyeron uno de los primeros ejemplos de narrativa convincente versus hechos técnicos detallados incapaces de convencer a las audiencias (Sismondo 2010, p. 149).

Hemos hablado de las dificultades que algunos científicos ven en el desarrollo de esta clase de tecnología, y de conceptos como el de supremacía cuántica. La descripción cuántica de la naturaleza es inherentemente exponencial. Por tanto, cualquier enfoque epistemológico que aspire a una simulación fiel de la misma debe tener en cuenta la teoría de la información y de la complejidad computacional. Desde el punto de vista filosófico, algunos se basan en el nuevo estatus ontológico de la información. Según esto, la propia naturaleza pondría límites a la posibilidad de una computación sin barreras. Desde el punto de vista del universo como un gran ordenador, la información ocupa un puesto predominante sobre la materia, y es esta su fuente. El famoso "**It from bit**" de Wheeler reflejaría este enfoque, frente a la dependencia clásica inversa. Los límites descubiertos en la teoría de la información serían también límites al desarrollo de esta nueva tecnología cuántica.

La confianza que está depositada en el desarrollo de esta tecnología, se basa, sin embargo, en encontrar una salida a un cruce de caminos, el ya conocido como *trilema de Aaronson*, proveniente del trabajo doctoral de este científico computacional, en donde al menos una de las siguientes proposiciones debería ser cierta: 1) La tesis extendida de Church-Turing es falsa, 2) la mecánica cuántica es falsa o 3) existe un algoritmo de factorización clásico que se ejecuta en tiempo polinomial. Como todos los indicios parecen indicar que las dos últimas proposiciones son falsas, los científicos creen que en efecto no existe una máquina de Turing universal clásica capaz de simular eficientemente cualquier problema físico, con lo que la única salida para ello sería el desarrollo de la computación cuántica, o el abandono de este propósito.

Así, se ha visto que bajo el desarrollo de esta tecnología, que siempre puede parecer algo prosaico, subyacen ideas filosóficas, tanto epistemológicas como ontológicas, que no hay que pasar por alto, y se remontan a los inicios de la teoría cuántica. Para terminar este escrito, permítaseme hacer algunas reflexiones generales al respecto. Las posibilidades de este nuevo tipo de computación, como hemos visto, reabrieron el debate de los fundamentos de la física cuántica, y de alguna forma dieron voz a algunos de los físicos que, con ideas realistas, habrían sido relegados al ostracismo en las anteriores décadas. Desde los años treinta del siglo XX, cuando se acabó de formalizar la teoría cuántica, con su dogma interpretativo, hasta los años ochenta en donde resurgió el interés por los fundamentos, gracias a las posibles nuevas aplicaciones de la teoría, los físicos que ponían en duda la excesiva carga postulacional del marco teórico de la cuántica, fueron condenados a un forzoso exilio intelectual. Y no digamos los que tenían claras tendencias realistas,

como Bohm, o el mismo Einstein. La idea subyacente a las reflexiones que prendieron el interés por esta clase de computación, que siguen manteniendo muchos de los teóricos de la computación cuántica, es la de establecer un isomorfismo entre naturaleza y computación, y esta fue la motivación principal del inicio de la disciplina. Si la naturaleza es cuántica, una simulación fidedigna de ella solo se podía llevar a cabo desde un dispositivo cuántico. En las últimas décadas , como consecuencia de la llegada de la computación cuántica al panorama de la física teórica actual, se ha retomado la posibilidad de replantearse perspectivas epistemológicas que ya se daban por bien asentadas.

Así, en un reciente artículo de los científicos de Oxford David Deutsch y Artur Ekert, pioneros de la computación cuántica, se afirma que la marginación de las ideas realistas en la génesis de la teoría cuántica fue consecuencia de una "mala filosofía", heredera del empirismo, el positivismo, el positivismo lógico, el instrumentalismo y el relativismo (Deutsch y Ekert 2016). Para Deutsch, de hecho, la cosa tampoco mejoró después, con Wittgenstein y la postmodernidad (Deutsch 2011, p. 394). Según ellos, el mismo Schrödinger habría sugerido, cinco años antes que Everett, que sus superposiciones ondulatorias en efecto sucedían todas a la vez realmente en algún lugar, ideas que no desarrolló supuestamente por la fuerza de la ortodoxia imperante. No diría yo tanto. Precisamente, por lo que se caracterizaban las generaciones de físicos, realistas o no, que alumbraron, no lo olvidemos, las dos grandes teorías físicas del siglo XX, fue por sus inquietudes filosóficas. Es difícil encontrar, en la historia de la ciencia, una figura con tanta agudeza filosófica como la que tenía Niels Bohr. En este sentido, quizás pueda ocurrir como en el ajedrez, que a menudo es mejor tener un plan, aunque sea malo, que no tener ninguno.

Y esto es precisamente lo que pasó con las generaciones de físicos posteriores. Se apartaron de los intereses filosóficos de sus maestros. Más aún, no es infrecuente encontrar alguno que directamente desprecia la filosofía, desde el mismo Feynman hasta Steven Weinberg. Yo mismo noté ese desprecio en mi formación en física - algo heterodoxa, precisamente venía de estudiar un año de filosofía en el otro "bando" -, coincidente con la época de los malentendidos del caso Sokal. En este sentido, Deutsch y Ekert no andan desencaminados, y me acercaría algo a su postura. Ellos creen que llevamos ya unas décadas volviendo a perspectivas realistas, con el propósito de "encauzar" a la filosofía de la ciencia. En realidad, yo creo que, simplemente, se está volviendo, tímidamente, a la reflexión pausada que reclamaba John Bell para sus días de fiesta. Y todo gracias al desarrollo de la computación cuántica, y a la lucha que se está dando contra sus posibles amenazas en relación con las sociedades digitalizadas de nuestro tiempo. Si una limitación teórica profunda cercenase finalmente su materialización, quizás se abriera de nuevo el melón de

los fundamentos de la teoría cuántica, y tuviéramos que replantearnos su reinterpretación o, por qué no, su sustitución.

Cierro este escrito con unas palabras de Scott Aaronson, que precisamente proviene de la informática teórica, un soplo de aire fresco en la vieja física, y no ha sido contaminado de prejuicios para estancarse en las visiones ortodoxas de la mecánica cuántica, esperando que haya gustado este escrito, y no haya errado mucho el tiro (Aaronson 2005a):

"For almost a century, quantum mechanics was like a Kabbalistic secret that God revealed to Bohr, Bohr revealed to the physicists, and the physicists revealed (clearly) to no one. So long as the lasers and transistors worked, the rest of us shrugged at all the talk of complementarity and wave-particle duality, taking for granted that we'd never understand, or need to understand, what such things actually meant. But today-largely because of quantum computing-the Schrödinger's cat is out of the bag, and all of us are being forced to confront the exponential Beast that lurks inside our current picture of the world. And as you'd expect, not everyone is happy about that, just as the physicists themselves weren't all happy when they first had to confront it in the 1920's.".

Referencias

Aaronson, S., y J. Watrous. 2009. "Closed timelike curves make quantum and classical computing equivalent." *Proceedings of the Royal Society A* 465:631–647.

Aaronson, Scott. 2005a. "Are quantum states exponentially long vectors?" *Proceedings of the Oberwolfach Meeting on Complexity Theory*.

———. 2005b, Marzo. "NP-complete problems and physical reality." *SIGACT News*. `https://arxiv.org/abs/quant-ph/0502072`.

———. 2008. "Los límites de la computación cuántica." En *Computación cuántica*, editado por Investigación y ciencia, 18–25. Barcelona: Prensa científica S. A.

———. 2013a. *Quantum computing since Democritus*. Cambridge, UK: Cambridge University Press.

———. 2013b. "Why Philosophers Should Care about Computational Complexity." En *Computability. Turing, Gödel, Church, and Beyond*, editado por B. Jack Copeland, Carl J. Posy, y Oron Shagrir, 261–327. Cambridge, MA: MIT Press. `https://arxiv.org/abs/1108.1791`.

Agrawal, M., N. Kayal, y N. Saxena. 2004. "PRIMES is in P." *Annals of Mathematics* 160 (2): 781–793. `http://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf`.

Aspect, A., P. Grangier, y G. Roger. 1982. "Experimental Realization of the Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: a New Violation of Bell's Inequalities." *Phys. Rev. Lett.* 49:91–94.

Bacon, Dave. 2004. "Quantum Computational Complexity in the Presence of Closed Timelike Curves." *Phys.Rev.A* 70:032309.

Ballentine, Leslie E. 1998. *Quantum Mechanics. A Modern Development*. Singapore: World Scientific Publishing Co.

Barenco, A., C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. H. Margolus, P. W. Shor,

T. Sleator, J. A. Smolin, y H. Weinfurter. 1995. "Elementary gates for quantum computation." *Physical Review A* 52 (5): 3457–3467.

Bell, J. S. 1964. "ON THE EINSTEIN PODOLSKY ROSEN PARADOX." *Physics* 1 (3): 195–200.

Benioff, Paul. 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.

———. 1982. "Quantum Mechanical Models of Turing Machines That Dissipate No Energy." *Physical Review Letters* 48 (23): 1581–1585.

Bennett, C., E. Bernstein, G. Brassard, y U. Vazirani. 1997. "Strengths and weaknesses of quantum computing." *SIAM J. Comput.* 26 (5): 1510–1523. `https://arxiv.org/abs/quant-ph/9701001`.

Bennett, C. H. 1973. "Logical Reversibility of Computation." *IBM Journal of Research and Development* 17 (6): 525–532.

———. 1982. "The thermodynamics of computation-a review." *International Journal of Theoretical Physics* 21:905–940.

———. 1992. "Quantum cryptography using any two nonorthogonal states." *Phys. Rev. Lett.* 68:3121–3124.

Bennett, C. H., F. Bessette, G. Brassard, L. Salvail, y J. Smolin. 1992. "Experimental quantum cryptography." *Journal of Cryptology* 5 (1): 3–28.

Bennett, C. H., y G. Brassard. 1989. "The experimental prototype is working!" *Sigact News* 20 (4): 78–82.

Bennett, Charles H., y G. Brassard. 1984, Diciembre. "Quantum cryptography: Public key distribution and coin tossing." *Proceedings of the International Conference on Computers, Systems and Signal Processing.* Bagalore, India, 175–179.

Bennett, Charles H., Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, y William K. Wootters. 1993. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels." *Phys. Rev. Lett.* 70:1895.

Bennett, Charles H., y Peter W. Shor. 1998, October. "Quantum Information Theory." *IEEE Transactions on Information Theory*, Volume 44(6).

Bennett, Charles H., y Stephen J. Wiesner. 1992. "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states." *Phys. Rev. Lett.* 69:2881.

Bernstein, E., y U. Vazirani. 1993. "Quantum Complexity theory." *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing.* 11–20.

Bernstein, Ethan, y Umesh Vazirani. 1997. "Quantum Complexity Theory." *SIAM J. Comput.* 26 (5): 1411–1473.

Bierhorst, Peter, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, Martin J. Stevens, y Lynden K. Shalm. 2018. "Experimentally generated randomness certified by the impossibility of superluminal signals." *Nature* 556:223–226.

Blum, L., M. Blum, y M. Shub. 1996. "A Simple Unpredictable Pseudo-Random Number Generator." *SIAM Journal on Computing* 15:364–383.

Bohm, D., y Y. Aharonov. 1957. "Discussion of Experimental Proof for the Paradox of Einstein, Rosen, and Podolsky." *Physical Review* 108 (4): 1070–1076.

Boixo, Sergio et al. 2018. "Characterizing quantum supremacy in near-term devices." *Nature* 14:595–600.

Boschi, D., S. Branca, F. De Martini, L. Hardy, y S. Popescu. 1998. "Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels." *Phys. Rev. Lett.*, vol. 80.

Bouwmeester, Dik, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, y Anton Zeilinger. 1997. "Experimental quantum teleportation." *Nature* 390:575–579.

Brassard, G. 2005. "Brief history of quantum cryptography: a personal perspective." *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.* 19–23.

Buzek, V., y M. Hillery. 1996. "Quantum copying: beyond the no-cloning theorem." *Phys. Rev. A*, vol. 54.

Caves, Carlton M., Christopher A. Fuchs, y Rüdiger Schack. 2002. "Quantum probabilities as Bayesian probabilities." *Phys. Rev. A* 65 (Ene): 022305.

Cirac, J. I., y P. Zoller. 1995. "Quantum Computations with Cold Trapped Ions." *Phys. Rev. Lett.* 74:4091.

Cirac, J. I., P. Zoller, H. J. Kimble, y H. Mabuchi. 1997. "Quantum State Transfer and Entanglement Distribution among Distant Modes in a Quantum Network." *Phys. Rev. Lett.* 78:3221–3224.

Cirac, Juan Ignacio. 2019, Septiembre. "Ordenadores cuánticos: Cómo, cuándo y para qué." *Conferencias de ciencias de la vida.* Calle Vitruvio, 5. 28006. Madrid: Fundación Ramón Areces. `https://bit.ly/3q09PP9`.

Clauser, J. F., y A. Shimony. 1978. "Bell's Theorem: Experimental Tests and Implications." *Rep. Progr. Phys.*, vol. 41.

Davies, P. C. W. 2007. "The Implications of a Cosmological Information Bound for Complexity, Quantum Information and the Nature of Physical Law." En *Randomness and Complexity, From Leibniz to Chaitin*, editado por Cristian S Calude, 69–87. Singapore: World Scientific Publishing Co.

Davies, P. C. W., y J. R. Brown. 1989. *El espíritu en el átomo*. Madrid: Alianza.

Deutsch, David. 1985. "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer." *Proc. R. Soc. Lond. A* 400:97–117.

———. 1989. "Quantum computational networks." *Proc. R. Soc. Lond. A* 425:73–90.

———. 1991. "Quantum mechanics near closed timeline lines." *Phys. Rev. D* 44:3197–3217.

———. 1997. *The Fabric of Reality*. London: Penguin Books.

———. 2011. *The Beginning of Infinity*. London (eBook): Penguin Books.

Deutsch, David, y Artur Ekert. 2016. "Más allá del horizonte cuántico." *Investigación y ciencia* Temas 86:12–17.

Dieks, D. 1982. "Communication by EPR devices." *Physics Letters* 92A, no. 6.

Diffie, W., y M.E. Hellman. 1976. "New Directions in Cryptography." *IEEE Transactions on Information Theory* 22:644–654.

Dowling, Jonathan P. 2013. *Schrödinger's killer app : race to buid the world's first quantum computer*. Boca Ratón, Florida: CRC Press.

———. 2021. *Schrödinger's web : race to buid the quantum internet*. Boca Ratón, Florida: CRC Press.

Einstein, A., B. Podolsky, y N. Rosen. 1935. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete." *Physical Review* 47:777–779.

Ekert, A. K. 1991. "Quantum cryptography based on Bell's theorem." *Phys. Rev. Lett.* 67 (6): 661–663.

Everett, Hugh. 1957. ""Relative State" Formulation of Quantum Mechanics." *Reviews of Modern Physics* 29 (3): 454–462.

Feynman, Richard P. 1960. "There´s Plenty of Room at the Bottom." *Caltech Engineering and Science* 23 (5): 22–36. `http://calteches.library.caltech.edu/47/2/1960Bottom.pdf`.

———. 1965. *The Character of Physical Law*. Cambridge: MIT Press.

———. 1982. "Simulating Physics with Computers." *International Journal of Theoretical Physics* 21:467–488.

———. 1986. "Quantum Mechanical Computers." *Foundations of Physics* 16, no. 6.

———. 1996. *Feynman lectures on computation.* Editado por Tony Hey y Robin W. Allen. New York: Westview Press.

Forman, Paul. 1971. "Weimar Culture, Causality, and Quantum Theory, 1918-1927: Adaptation by German Physicists and Mathematicians to a Hostile Intellectual Environment." *Historical Studies in the Physical Sciences* 3:1–115.

Fredkin, Edward, y Tommaso Toffoli. 1982. "Conservative logic." *International Journal of Theoretical Physics* 21:219–253.

Galindo, A., y M. A. Martín-Delgado. 2002. "Information and computation: Classical and quantum aspects." *Rev. Mod. Phys.* 74:347–423.

Galindo Tixaire, Alberto. 2007. "El arte de disfrazar la información: de la C a la Q." *Rev.R.Acad.Cienc.Exact.Fís.Nat.* 101 (2): 307–320.

García Alcaine, Guillermo. 1998. "Teleportación: realidad y ficción." *Revista Española de Física* 12 (1): 6.

Gardner, M. 1977. "Mathematical Games. A new kind of cipher that would take millions of years to break." *Scientific American*, vol. Agosto.

Gisin, Nicolas. 2002. "Sundays in a Quantum Engineer's Life." En *Quantum [Un]speakables: From Bell to Quantum Information*, editado por Reinhold Bertlmann y Anton Zeilinger, 199–208. New York: Springer.

Goldreich, O. 2004. "On quantum computing." `http://www.wisdom.weizmann.ac.il/~oded/on-qc.html`.

Golomb, S.W. 1982(1967). *Shift Register Sequences. Revised 2nd edn.* Laguna Hills, CA: Aegean Park Press.

Grover, L. K. 1996. "A fast quantum mechanical algorithm for database search." *Proceedings of the 28th Anual ACM Symposium on the Theory of Computing.* Philadelphia, Pennsilvania, USA: ACM Press, 212–219.

Hameroff, Stuart R., y Roger Penrose. 2014. "Consciousness in the universe: A review of the 'Orch OR' theory." *Physics of Life Reviews* 11:39–78.

Haroche, Serge, y Jean-Michel Raimond. 1996. "Quantum Computing: Dream or Nightmare?" *Physics Today* 49 (8): 51.

Hiskett, P.A., D. Rosenberg, C.G. Peterson, R.J. Hughes, S. Nam, A.E. Lita, A.J. Miller, y J.E. Nordholt. 2006. "Long-distance quantum key distribution in optical fibre." *New J. Phys.* 8 (193): 1–7.

Holevo, A. S. 1973. "Bounds for the quantity of information transmitted by a quantum communication channel." *Problems of Information Transmission* 9:177–183. Traducción inglesa.

Jammer, Max. 1974. *The Philosophy of Quantum Mechanics: The Interpretations of Quantum Mechanics in Historical Perspective.* New York: Wiley-Interscience.

Jones, Nicola. 2013. "Computing: The quantum company." *Nature* 498:286–288.

Jozsa, R. 1998(1997). "Quantum algorithms and the Fourier transform." *Proceedings of the Royal Society A* 454 (1969): 323–337.

Kalai, G. 2016. "The quantum computer puzzle." *Notices of the AMS* 63 (5): 508–516.

Karp, R. M., y R. J. Lipton. 1982. "Turing machines that take advice." *Enseign. Math.* 28:191–201.

Kim, KyungDuk, Stefan Bittner, Yongquan Zeng, Stefano Guazzotti, Ortwin Hess, Qi Jie Wang, y Hui Cao. 2021. "Massively parallel ultrafast random bit generation with a chip-scale laser." *Science* 371:948–952.

Kitaev, A.Yu. 1995. "Quantum measurements and the Abelian stabilizer problem." *eprint arXiv*, vol. quant-ph/9511026.

Landauer, R. 1961. "Irreversibility and heat generation in the computing process." *IBM Journal of Research and Development* 5 (3): 183–191.

———. 1991. "Information is physical." *Physics Today* 44 (5): 23–29.

Levin, L. A. 2003. "Polynomial time and extravagant models, in The tale of one-way functions." *Problems of Information Transmission* 39 (1): 92–103.

Lloyd, Seth. 1996. "Universal Quantum Simulators." *Science* 273 (5278): 1073–1078.

———. 1999. "Quantum search without entanglement." *Phys. Rev. A* 61 (Dic): 010301.

———. 2000. "Ultimate physical limits to computation." *Nature* 406:1047–1054.

———. 2007. *Programming the universe.* London,UK: Vintage Books.

Mermin, David. 1990(1989). "What's wrong with this pilow. Physics Today, April, 1989." En *Boojums all the way through: communicating science in a prosaic age*, 198–205. New York: Cambridge University Press.

Meyer, David A. 1999. "Quantum strategies." *Phys. Rev. Lett.* 82:1052–1055.

Monroe, C., y J. Kim. 2013. "Scaling the Ion Trap Quantum Processor." *Science* 339 (6124): 1164–1169.

Monz, Thomas, Daniel Nigg, Esteban A. Martinez, Matthias F. Brandl, Philipp Schindler, Richard Rines, Shannon X. Wang, Isaac L. Chuang, y Rainer Blatt1. 2016. "Realization of a scalable Shor algorithm." *Science* 351:1068–1070.

Nguyen, C. T., D. D. Sukachev, M. K. Bhaskar, B. Machielse, D. S. Levonian, E. N. Knall, P. Stroganov, R. Riedinger, H. Park, M. Loncar, y M. D. Lukin. 2019. "Quantum network nodes based on diamond qubits with an efficient nanophotonic interface." *Phys. Rev. Lett.* 123:183602.

Nielsen, Michael A., y Isaac L. Chuang. 2010. *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press.

Ortega y Gasset, José. 1965(1947). "La idea de principio en Leibniz y la evolución de la teoría deductiva." En *OBRAS COMPLETAS. Tomo VIII*, editado por Revista de Occidente, 61–358. Madrid: Ediciones Castilla.

Penrose, Roger. 1991(1989). *La nueva mente del emperador*. Madrid: Mondadori.

———. 1996. "On Gravity's role in Quantum State Reduction." *General Relativity and Gravitation* 28:581–600.

Pomerance, Carl. 1996. "A Tale of Two Sieves." *Notices of the AMS* 43 (12): 1473–1485.

Popper, Karl. 1982(1956). "Quantum Theory and the Schism in Physics." En *Postscript to The Logic of Scientific Discovery*, editado por III W. W. Bartley. Totowa, New Jersey: Rowman and Littlefield.

Preskill, John. 2013. "Rapporteur talk by J. Preskill: Quantum Entanglement and Quantum Computing." En *The Theory of the Quantum World. Proceedings of the 25th Solvay Conference on Physics*, editado por David Gross, Marc Henneaux, y Alexander Sevrin, 63–80. Singapore: World Scientific. `https://arxiv.org/abs/1203.5813`.

Pudenz, Kristen L., Tameem Albash, y Daniel A. Lidar. 2014a. "Error corrected quantum annealing with hundreds of qubits." *Nature Comm.* 5:3243.

———. 2014b. "Quantum or not, controversial computer yields no speedup." *Science* 344:1330–1331.

Rivest, R., A. Shamir, y L. Adleman. 1978. "A method for obtaining digital signatures and public-key cryptosystems." *Communications ACM* 21 (2): 120–126.

Schmitt-Manderbach, Tobias et al. 2007. "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km." *Phys. Rev. Lett.* 98 (Jan): 010504.

Shannon, C. E. 1948. "A mathematical theory of communication." *Bell Systems Technical Journal* 27:379–423,623–656.

Shi, Yaoyun. 2003. "Both Toffoli and controlled-NOT need little help to do universal quantum computing." *Quantum Information and Computation* 3 (1): 1073–1078.

Shor, P. W. 1994. "Algorithms for quantum computation: discrete logarithms and factoring." *Proceedings of the 35th Anual Symposium on Foundations of Computer Science*. Los Alamitos, CA, USA: IEEE Press.

Simon, D. 1994. "On the power of quantum computation." *Proceedings of the 35th Anual Symposium on Foundations of Computer Science*. Los Alamitos, CA, USA: IEEE Press, 116–123.

Sismondo, Sergio. 2010. *An introduction to Science and Technology Studies*. West Sussex, UK: Wiley-Blackwell.

Smolin, Lee. 2019. *Einstein's unfinished revolution*. New York (eBook): Penguin Press.

Solovay, R., y V. Strassen. 1977. "A Fast Monte-Carlo Test for Primality." *SIAM J. Comput.* 6 (1): 84–85.

't Hooft, G. 1999. "Quantum gravity as a dissipative deterministic system." *Classical and Quantum Gravity* 16:3263–3279.

Vandersypen, Lieven M. K., Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood, y Isaac L. Chuang. 2001. "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance." *Nature* 414:883–887.

Vernam, G. S. 1926. "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications." *IEEE* 45:109–115.

von Neumann, John. 1991(1932). *Fundamentos matemáticos de la mecánica cuántica*. Madrid: CSIC.

Wiesner, S. 1983. "Conjugate coding." *SIGACT News* 15 (1): 78–88.

Wootters, W. K., y W. H. Zurek. 1982. "A single quantum cannot be cloned." *Nature*, vol. 299.

Yao, A. Chi-Chih. 1993, Noviembre. "Quantum circuit complexity." *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*. Palo Alto, CA, USA: IEEE Press.

Zeilinger, Anton et al. 2012. "Quantum teleportation over 143 kilometres using active feed-forward." *Nature* 489:269–273.

Zurek, Wojciech Hubert. 2003. "Decoherence, einselection, and the quantum origins of the classical." *Reviews of Modern Physics* 75:715–775.

Este documento ha sido firmado digitalmente por Carlos Ruiz Jiménez, con DNI 51394302, jurando que este trabajo, *Sobre la computación cuántica*, es de su autoría y no ha sido plagiado.

Firmado por RUIZ JIMENEZ CARLOS - 51394302C el día
09/11/2021 con un certificado emitido por AC FNMT Usuarios