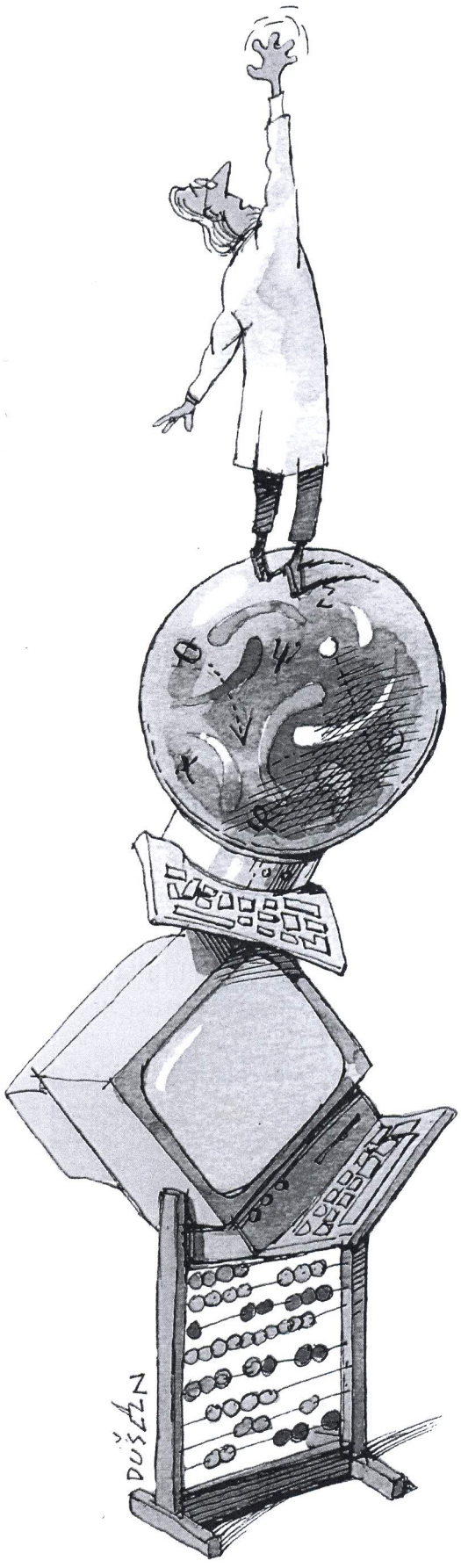


LOS LIMITES DE LA Computac

Scott Aaronson

Las computadoras cuánticas podrían ser velocísimas en tareas muy concretas. En la mayoría de los problemas apenas descollarían sobre los ordenadores de hoy

Un error frecuente —recuérdese, por ejemplo, *The Economist* de 15 de febrero de 2007— consiste en afirmar que, en teoría, las computadoras cuánticas podrían resolver rápidamente una colección de problemas de singular dificultad, los llamados problemas NP-completos, algo que hasta el momento no se puede hacer ni aun con los ordenadores más potentes. Se presumía que las computadoras cuánticas podrían lograr tal hazaña porque permitirían el procesamiento simultáneo de todas las posibles soluciones.

Si en verdad fuese posible construir semejante computadora mágica, capaz de resolver un problema NP-completo en un abrir y cerrar de ojos, el mundo se convertiría en un lugar muy diferente. Podríamos, por ejemplo, ordenarle a nuestra mágica computadora que buscase posibles regularidades en las fluctuaciones de los mercados de valores, en las series de datos meteorológicos o en la actividad cerebral. A diferencia de los ordenadores actuales, cuya programación exige una perfecta comprensión de los problemas, la elucidación de tales regularidades sería enteramente rutinaria; no exigiría un conocimiento detallado de la sustancia del problema.

La computadora mágica podría, asimismo, automatizar la creatividad matemática. Podríamos pedirle a nuestra computadora que examinase todas las posibles demostraciones o refutaciones de un problema sin resolver que contuvieran hasta, sea por caso, mil millones de símbolos. (Si una demostración se extendiese más, ¿quién iba a leerla?)

Si las computadoras cuánticas prometieran estas fuerzas matemáticas cuasidivinas, su aparición sería, a buen seguro, coetánea de los viajes por el hiperespacio y los escudos antigravitatorios. Pero si bien es cierto que no debemos aceptar las habituales hipérboles, a mi entender no es menos erróneo desdeñar la computación cuántica como pura ciencia ficción. Lo que se ha de hacer es averiguar dónde se encuentran sus límites.

En los 26 años que han transcurrido desde que Richard Feynman propuso la idea de computación cuántica, las ciencias del cómputo han realizado enormes progresos en la averiguación de los tipos de problemas donde la computación cuántica sería eficaz. De acuerdo con nuestros conocimientos actuales, sí *proporcionarían* aceleraciones impresionantes en unos cuantos problemas concretos: por ejemplo, para descifrar los códigos criptográficos hoy ampliamente utilizados en las transacciones monetarias por Internet. En el caso de otros problemas, sin embargo, como los de jugar al ajedrez, las reservas de plaza en las líneas aéreas o la demostración automática de teoremas, las computadoras

ILUSTRACIONES DE DUŠAN PETRIČIĆ

ión cuántica

cuánticas sufrirían de muchas de las limitaciones algorítmicas que hoy padecen los ordenadores clásicos.

Estas limitaciones son completamente independientes de las dificultades prácticas que entraña la construcción de computadoras cuánticas, como la decoherencia (interacción indeseada entre la computadora cuántica y su entorno, que introduce errores). En particular, las limitaciones matemáticas de lo programable en un ordenador persistirían aunque se pudiera construir una computadora cuántica que no sufriese en absoluto los efectos de la decoherencia.

Difícil, más difícil todavía, dificilísimo

¿Cómo es posible que una hipotética computadora cuántica pueda proporcionar grandes aceleraciones en determinados problemas, así el descifrado de códigos, y no pueda hacerlo, en cambio, en otros? ¿Acaso un ordenador rápido no es siempre rápido? Pues no, y la explicación nos lleva directamente al meollo intelectual de la ciencia de la computación. En esta ciencia, lo más importante de un problema es la rapidez con que aumenta el tiempo requerido para resolverlo conforme crece su tamaño. El tiempo se mide por el número de pasos elementales necesarios para que el algoritmo llegue a una solución.

Si efectuamos una multiplicación por el método que aprendimos en la escuela elemental, el cálculo del producto de dos números de n cifras requiere una cantidad de tiempo que crece con n^2, el cuadrado del número de dígitos (el tiempo empleado es un "polinomio en n). Pero la descomposición de un número en sus factores primos, utilizando incluso los métodos más avanzados conocidos, exige un tiempo que aumenta en función exponencial del número de dígitos (más en concreto, como 2 elevado a la raíz cúbica del número n). La descomposición en factores constituye un problema intrínsecamente más difícil que la multiplicación, y cuando se llega a millares de dígitos, tal diferencia adquiere una importancia mucho mayor que la diferencia entre un Commodore 64 y un superordenador.

El tipo de problemas que los ordenadores pueden resolver en tiempos de duración razonable, incluso para valores grandes de n, son aquellos para los que existe un algoritmo que requiere un número de pasos que crece como una potencia de n con exponente fijo, como n, o n^2 o $n^{2,5}$. De tales algoritmos se dice que son "eficientes". Los problemas resolubles mediante algoritmos eficientes se dice que pertenecen a la clase de complejidad P, abreviatura de "tiempo polinómico".

He aquí un ejemplo sencillo de problema de clase P: Dado un mapa de carreteras, ¿es alcanzable cada ciudad desde otra ciudad cualquiera? P contiene asimismo problemas cuyas soluciones eficientes no son tan obvias. Sea por caso: Dado un número entero, ¿es primo (como el 13) o es compuesto (como el 12)? Dada una lista de hombres y mujeres que desean casarse unos con otros, ¿será posible asociar a cada persona con una que quiere casarse con ella?

Supongamos, en cambio, que se nos proporcionan las dimensiones de una serie de cajas y que deseamos encajarlas en el maletero del coche. O que se nos entrega un mapa y deseamos colorear cada región de rojo, de azul o de verde, de modo que no haya dos regiones fronterizas del mismo color. O que se dispone de una lista de islas conectadas por puentes y deseamos un recorrido de ida y vuelta que visite cada isla exactamente una vez. Aunque se conocen para estos problemas algoritmos que son algo mejores que el puro tanteo de todas las posibles soluciones, no se conoce ninguno que sea fundamentalmente mejor. Todos los algoritmos conocidos necesitarán de tiempos de ejecución que crecerán exponencialmente con el tamaño del problema.

Resulta que los tres problemas que acabo de mencionar comparten una propiedad muy interesante: en el fondo, todos son "el mismo

CONCEPTOS BASICOS

- Las computadoras cuánticas se valdrían de las extrañas reglas de la mecánica cuántica para procesar información de maneras que resultarían imposibles en un ordenador común.
- Podrían resolver ciertos problemas, como la factorización de números enteros, a velocidades vertiginosas en comparación con lo que puede hacerse, en el mejor de los casos, con ordenadores clásicos. Pero los análisis llevan a pensar que en la mayoría de los problemas las computadoras cuánticas sólo superarían ligeramente a las máquinas ordinarias.
- Raras alteraciones de las leyes físicas podrían consentir la construcción de computadoras que resolviesen amplias categorías de problemas difíciles. Pero alteraciones así no parecen verosímiles. La imposibilidad de resolver estos problemas en el mundo real tal vez debería ser considerada un principio fundamental de la física.

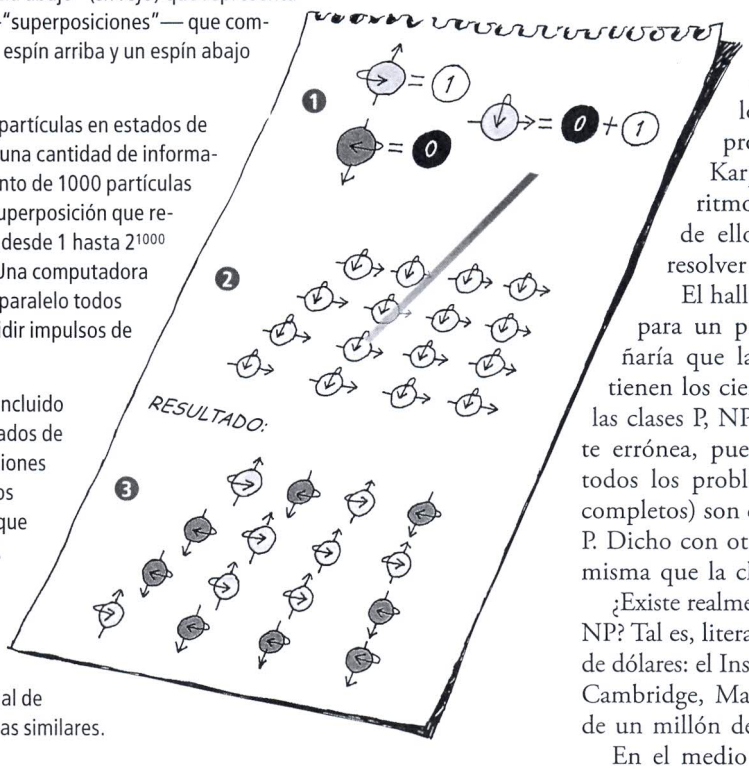
Computación cuántica:

Los físicos están persiguiendo con tenacidad la construcción de computadoras cuánticas, que sacarían provecho de la mecánica cuántica y sus peculiaridades para lograr una eficiencia mayor que la conseguida por los ordenadores en uso.

❶ La característica fundamental de una computadora cuántica es que no utiliza bits, sino qubits. Un qubit puede quedar plasmado en una partícula, un electrón por ejemplo, con "espín hacia arriba" (*en azul*) que representa un 1 o "espín hacia abajo" (*en rojo*) que representa un 0, y estados cuánticos —"superposiciones"— que comportan simultáneamente un espín arriba y un espín abajo (*en amarillo*).

❷ Un pequeño número de partículas en estados de superposición puede incluir una cantidad de información enorme: un mero conjunto de 1000 partículas puede encontrarse en una superposición que represente todos los números desde 1 hasta 2^{1000} (aproximadamente, 10^{300}). Una computadora cuántica podría manejar en paralelo todos esos números, haciendo incidir impulsos de láser sobre las partículas.

❸ Sin embargo, una vez concluido el cómputo, al medir los estados de las partículas, todas las versiones de los 10^{300} estados paralelos desaparecen, excepto una, que resulta seleccionada al azar. No obstante, una manipulación inteligente de las partículas permitiría resolver muy rápidamente la descomposición factorial de números grandes y problemas similares.



problema", en el sentido de que, de existir un algoritmo eficiente para uno cualquiera de ellos, se dispondría de algoritmos eficientes para los demás. Stephen A. Cook, de la Universidad de Toronto, Richard Karp, de la Universidad de California en Berkeley, y Leonid Levin, ahora en la de Boston, llegaron a esta notable conclusión hace más de 30 años, fechas en las que desarrollaron la teoría de NP-completitud.

NP es abreviatura de "tiempo polinómico no determinista". No se preocupe por el significado de esa expresión. En esencia, el conjunto NP está constituido por la clase de problemas para los cuales, una vez hallada una solución, se puede verificar en tiempo polinómico (algo así como n^2 o similar) que tal solución es correcta, a pesar incluso de que tal solución resulte difícil de hallar. Si se nos da un mapa que contiene miles de islas y puentes, es posible que se necesiten años para hallar un circuito que visite cada isla una sola vez; ahora bien, si nos es presentado un circuito concreto, no es difícil saber si ese circuito constituye una solución. Cuando un problema goza de esta propiedad, se dice que pertenece a NP. La clase NP abarca un enorme número de problemas de interés práctico. Cabe señalar que todos los problemas P son asimismo problemas NP; expresado de otro modo, la clase P está contenida en la clase NP. Pues si es posible resolver un problema rápidamente, la solución obtenida también podrá verificarse con presteza.

Los problemas NP-completos son, en esencia, los problemas de máxima dificultad de la clase NP. Constituyen los problemas que poseen la propiedad enunciada por Cook, Karp y Levin: de hallarse un algoritmo eficiente para uno cualquiera de ellos, podría ser adaptado para resolver los demás problemas NP.

El hallazgo de un algoritmo eficiente para un problema NP-completo entrañaría que la idea que en este momento tienen los científicos de la computación de las clases P, NP y NP-completa es totalmente errónea, pues tal hallazgo supondría que todos los problemas NP (incluidos los NP-completos) son en realidad problemas de clase P. Dicho con otras palabras, la clase P sería la misma que la clase NP, P = NP.

¿Existe realmente tal algoritmo? ¿Es P igual a NP? Tal es, literalmente, la pregunta del millón de dólares: el Instituto Clay de Matemáticas, en Cambridge, Massachusetts, ofrece un premio de un millón de dólares por su elucidación.

En el medio siglo transcurrido desde que se formuló el problema, no se ha descubierto un algoritmo eficiente para un problema NP-completo. En consecuencia, los expertos en computación de hoy están de acuerdo en que P no es igual que NP, $P \neq NP$, aunque todavía nuestro saber no alcance para comprender por qué es así, o para demostrarlo y dar a esa aserción carácter de teorema.

Lo que la computación cuántica puede hacer

Si se concede que $P \neq NP$, queda tan sólo una esperanza para resolver problemas NP-completos en tiempo polinómico, a saber, generalizar lo que entendemos por "computadora". Parece, a primera vista, que la mecánica cuántica podría suministrarnos precisamente el tipo de recursos necesarios. La mecánica cuántica hace posible el almacenamiento y manipulación de una vasta cantidad de información en los estados de un número no muy grande de partículas. Para comprender cómo se puede lograr tal cosa, imagine que tenemos 1000 partículas y que cada partícula, al ser medida, se nos presenta con espín hacia arriba o hacia abajo.

Para nuestros propósitos, es irrelevante lo que signifique que el espín de la partícula apunte en uno u otro sentido; lo único que importa es que la partícula posee una propiedad que, al ser medida, ofrece uno de dos valores.

Si hemos de describir el estado cuántico de esta colección de partículas, deberemos especificar un número para cada posible resultado de su medición. Tales números reciben el nombre de "amplitudes de probabilidad" de los resultados posibles y guardan una relación determinada con la probabilidad de cada uno. Mas, a diferencia de las probabilidades, las amplitudes cuánticas pueden tomar valores positivos o negativos (más aún, sus valores son números complejos). Por ejemplo, es necesaria una amplitud para describir la posibilidad de que el espín de todo el millar de partículas esté orientado hacia arriba, otra amplitud para la posibilidad de que el espín de las 500 primeras partículas apunte hacia arriba, y el de las otras 500, hacia abajo, y así sucesivamente. Existe un total de 2^{1000} posibles resultados, o sea, unos 10^{300} distintos valores; por eso, su expresión requiere números tan grandes: ¡mayores que el número de partículas del universo visible! La terminología técnica para esta situación es que las 1000 partículas se encuentran en una superposición de esos 10^{300} estados.

En otras palabras: podríamos almacenar simultáneamente 10^{300} números en nuestro colectivo de 1000 partículas. Seguidamente, efectuando ciertas operaciones sobre esas partículas y sobre otras auxiliares —mediante secuencias de impulsos de láser o de ondas de radio— podríamos ejecutar un algoritmo que transformase al mismo tiempo la totalidad de los 10^{300} números (cada uno de los cuales representa una posible solución). Si una vez efectuada esta operación nos fuera posible observar con precisión cada uno de los estados cuánticos finales de las partículas, tendríamos una genuina computadora mágica: se habrían comprobado 10^{300} posibles soluciones para un problema; y al final, podríamos discernir rápidamente cuál es la correcta.

Pero existe una dificultad. Según dictan las reglas de la mecánica cuántica, en la medición de las partículas (operación necesaria para observar su estado final) se seleccionará al azar una de las 10^{300} posibilidades, e inmediatamente todas las demás desaparecerán. El resultado no sería mejor que si utilizásemos un ordenador clásico y ensayásemos una hipotética solución elegida al azar: en uno y otro caso, nuestra información se reduciría a esa hipotética solución.

Por fortuna, quedan todavía teclas que tocar para extraer alguna ventaja de nuestras partículas cuánticas. Las amplitudes pueden cancelarse mutuamente cuando las que son positivas se combinan con las negativas, fenómeno conocido como interferencia destructiva. Así pues, un buen algoritmo cuántico aseguraría que las sendas computacionales conducentes a respuestas erróneas se cancelasen de ese modo. Debería también garantizar que las conducentes a soluciones correctas tuvieran todas ellas amplitudes del mismo signo, lo que resultaría en una interferencia constructiva y reforzaría, en consecuencia, la probabilidad de encontrarlas cuando se midiesen las partículas al final del proceso.

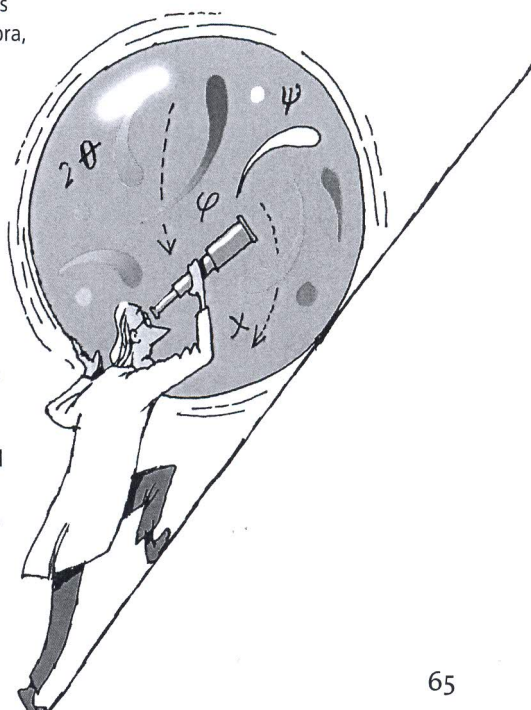
¿Para qué clase de problemas computacionales podemos organizar esta clase de interferencia, utilizando un menor número de pasos que los necesarios para resolver el problema por medios clásicos?

El primer ejemplo de algoritmo cuántico capaz de acelerar de forma impresionante la so-

La buena noticia

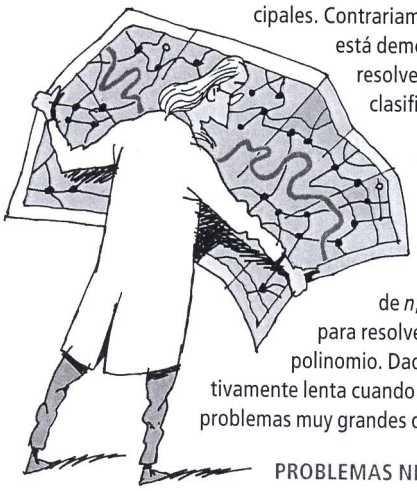
Si una computadora cuántica ideal y de gran tamaño sufriese las mismas limitaciones que afectan a los ordenadores clásicos, ¿deberían los físicos que tratan de construir computadoras cuánticas —labor de dificultad extraordinaria, incluso para las más rudimentarias— recoger sus trastos e irse a casa? Estoy convencido de que no, por cuatro razones.

- Si las computadoras cuánticas llegan a ser realidad algún día, su aplicación básica no consistirá en descifrar códigos, sino en algo, que de puro evidente, apenas se menciona: la simulación de fenómenos cuánticos. Se trata de un problema fundamental en química, en nanotecnia y en otros campos; tan importante, que se han concedido premios Nobel incluso por progresos parciales.
- Conforme los transistores de los microchips se aproximan a dimensiones atómicas, es probable que las ideas procedentes de la computación cuántica adquieran relevancia para la computación clásica.
- Los experimentos de computación cuántica concentran la atención sobre las más desconcertantes peculiaridades de la mecánica cuántica. Abrigo la esperanza de que cuantos menos de estos enigmas tengamos que ocultar bajo la alfombra, más habrán de ser quienes se vean obligados a comprenderlos.
- Se puede considerar que la computación cuántica sería la verificación más estricta a la que nunca haya sido sometida la propia mecánica cuántica. A mi modo de ver, el más apasionante de los posibles resultados de la investigación en computación cuántica consistiría en descubrir una razón fundamental por la que las computadoras cuánticas *no* fueran posibles. Un fracaso de tal magnitud volvería del revés la imagen que nos hemos formado del mundo físico. En cambio, el éxito en construirlas se limitaría meramente a confirmarla.



Capacidades y limitaciones de los ordenadores clásicos

En las ciencias de cómputo, los problemas se categorizan de acuerdo con el número de pasos computacionales que exigiría la resolución de un ejemplo grande del problema utilizando el mejor algoritmo conocido. Los problemas se agrupan, según su dificultad, en amplias clases, no mutuamente excluyentes. Adjuntamos tres de las principales. Contrariamente a lo que se proclama sin fundamento, no está demostrado que las computadoras cuánticas puedan resolver la clase de problemas muy difíciles a los que se clasifica como NP-completos.



PROBLEMAS P: **Problemas que los ordenadores pueden resolver en tiempo polinómico**

Ejemplo: Dado un mapa en el que figuran n ciudades, ¿se podrá ir desde una ciudad hasta cualquier otra? En el caso de un valor grande de n, el número de pasos que necesita el ordenador para resolver el problema aumenta en proporción a n^2, un polinomio. Dado que los polinomios crecen a velocidad relativamente lenta cuando n aumenta, los ordenadores pueden resolver problemas muy grandes de tipo P en unos tiempos razonables.

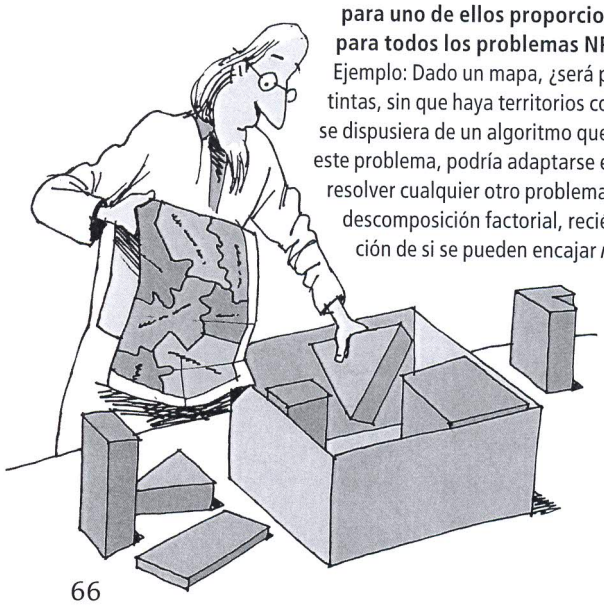
PROBLEMAS NP: **Problemas cuya solución es fácil de comprobar**

Ejemplo: Se sabe que un cierto número de n dígitos es el producto de dos números primos grandes, y deseamos hallar esos dos factores primos. Si se nos proporcionan los factores, podemos comprobar —multiplicándolos— que son la solución. El tiempo consumido en la comprobación es polinómico.

Todo problema P es también un problema NP, por lo que la clase NP integra en sí a la clase P. Se conjetura que el problema de la factorización queda fuera de la clase P, porque no se conoce ningún algoritmo mediante el cual un ordenador común pueda resolverlo en un número polinómico de pasos. Antes bien, el número de pasos aumenta exponencialmente al aumentar n.

PROBLEMAS NP-COMPLETOS: **Una solución eficiente para uno de ellos proporcionaría una solución eficiente para todos los problemas NP**

Ejemplo: Dado un mapa, ¿será posible colorearlo con sólo tres tintas, sin que haya territorios contiguos del mismo color? Si se dispusiera de un algoritmo que resolviera eficientemente este problema, podría adaptarse el algoritmo de marras para resolver cualquier otro problema NP (como el problema de descomposición factorial, recién mencionado, o la averiguación de si se pueden encajar n cajas de diversos tamaños en un cajón de dimensiones conocidas). En este sentido, los problemas NP-completos constituyen los problemas NP de máxima dificultad. No se conoce ningún algoritmo capaz de resolver eficientemente un problema NP.



lución de un problema práctico fue descubierto por Peter Shor en 1994. Shor demostró que una computadora cuántica podría factorizar un número de n dígitos en una secuencia de pasos cuya longitud creciese solamente como n^2, es decir, en tiempo polinómico. Según hemos mencionado, en el mejor de los algoritmos conocidos para computadoras clásicas el número de pasos crece exponencialmente.

Cajas negras

Así pues, al menos para la descomposición en factores, aplicando métodos cuánticos se puede lograr una aceleración exponencial sobre los algoritmos clásicos conocidos. Pero ni está demostrado, ni parece que el problema de la descomposición en factores sea NP-completo, pese a que muchos crean que lo es. Shor, para construir su algoritmo, se valió de ciertas propiedades matemáticas de los números compuestos y de sus divisores; resultaban particularmente idóneas para producir el tipo de interferencia constructiva o destructiva del que puede sacar partido un ordenador cuántico. Los problemas NP-completos no parecen compartir estas propiedades especiales. Hasta la fecha, sólo se han hallado unos pocos algoritmos cuánticos que, al parecer, podrían permitir aceleraciones que rebajasen en ciertos problemas los tiempos, llevándolos de exponenciales a potenciales.

La cuestión, pues, sigue abierta. ¿Existe un algoritmo cuántico eficiente, capaz de resolver problemas NP-completos? Aunque se ha puesto en ello gran empeño, no se ha descubierto ningún algoritmo de ese tipo, si bien —no puede sorprender— tampoco se ha demostrado que no exista. Después de todo, ni siquiera podemos demostrar que no existe un algoritmo clásico de tiempo polinómico capaz de resolver problemas NP-completos.

Lo que sí podemos afirmar es que un algoritmo cuántico capaz de resolver eficientemente problemas NP-completos tendría que sacar partido, como el algoritmo de Shor, de la estructura del problema, pero debería hacerlo por métodos que caerían mucho más allá de las técnicas disponibles. No es posible lograr una aceleración exponencial tratando los problemas como si fuesen "cajas negras" que careciesen de estructura, consistentes en un número exponencial de soluciones que habría que verificar en paralelo. Sí se podría conseguir, no obstante, una cierta aceleración con este enfoque de caja negra; los expertos en computación han determinado exactamente cuánta y cuáles son sus limitaciones. El algoritmo que produce la aceleración es el segundo en importancia de los principales algoritmos cuánticos.

Como ilustración de la metodología de "cajas negras" supongamos que se busca la solución de un problema difícil y que la única operación que se sabe realizar consiste en ir probando presuntas soluciones y ver si funcionan. Supongamos que existan S posibles soluciones y que el número S crece exponencialmente al aumentar el tamaño n del problema. No es imposible que se tenga suerte y se atine con la solución a la primera, pero en el caso más desfavorable habría que efectuar S ensayos. Por término medio, el número de tanteos necesarios sería de $S/2$.

Supongamos ahora que fuese posible preguntar por todas las posibles soluciones que se hallan en superposición cuántica. En 1996, Lov Grover, de los Laboratorios Bell, desarrolló un algoritmo para hallar la solución correcta en un tal supuesto con sólo unos $\sqrt{S}$ pasos. Una aceleración que rebaja desde $S/2$ hasta $\sqrt{S}$ constituye un avance de interés en ciertos problemas, pues si hay un millón de posibles soluciones, el número de pasos necesarios rondaría en torno a 1000, en lugar de 500.000. Pero la raíz cuadrada no transforma el tiempo exponencial en tiempo polinómico: produce, sencillamente, una exponencial más pequeña. Y el algoritmo de Grover es lo más que se puede lograr con este tipo de búsqueda de caja negra: en 1994 se había demostrado ya que cualquier algoritmo de caja negra necesita cuando menos $\sqrt{S}$ pasos.

A lo largo de los últimos diez años, se ha venido demostrando que aceleraciones de similar modestia señalan los límites para muchos otros problemas, amén de la búsqueda de una lista: el recuento de votos en unas elecciones, la determinación de la ruta más corta en un mapa o los juegos de estrategia, como el ajedrez o el Go. Un problema que planteaba especial dificultad era el llamado problema de la colisión, que consiste en hallar dos elementos idénticos —que "colisionan"— en una lista extensa. De existir un algoritmo rápido para resolver este problema, muchos de los bloques constructivos básicos del comercio electrónico perderían su utilidad en un mundo provisto de computadoras cuánticas.

El examen de una lista en busca de un elemento determinado viene a ser como dar con una aguja en un pajar, mientras que la búsqueda de una colisión es como buscar dos pajitas que sean idénticas, problema con un tipo de estructura del que una computadora cuántica podría sacar partido. Sin embargo, ya demostré en 2002 que, con el modelo de cajas negras, cualquier algoritmo cuántico requiere un tiempo exponencial para resolver el problema de la colisión.

Hay que reconocer que estas limitaciones de las cajas negras no descartan que haya aún por descubrir algoritmos cuánticos eficientes para problemas NP-completos, si no más arduos. Mas, si tales algoritmos existiesen, tendrían

El autor

Scott Aaronson es profesor de ingeniería eléctrica y ciencia de la computación en el Instituto de Tecnología de Massachusetts. En su momento abandonó los estudios de bachillerato; sin embargo, acabó licenciándose en la Universidad Cornell y doctorándose en ciencia de la computación por la Universidad de California en Berkeley, bajo la dirección de Umesh Vazirani.

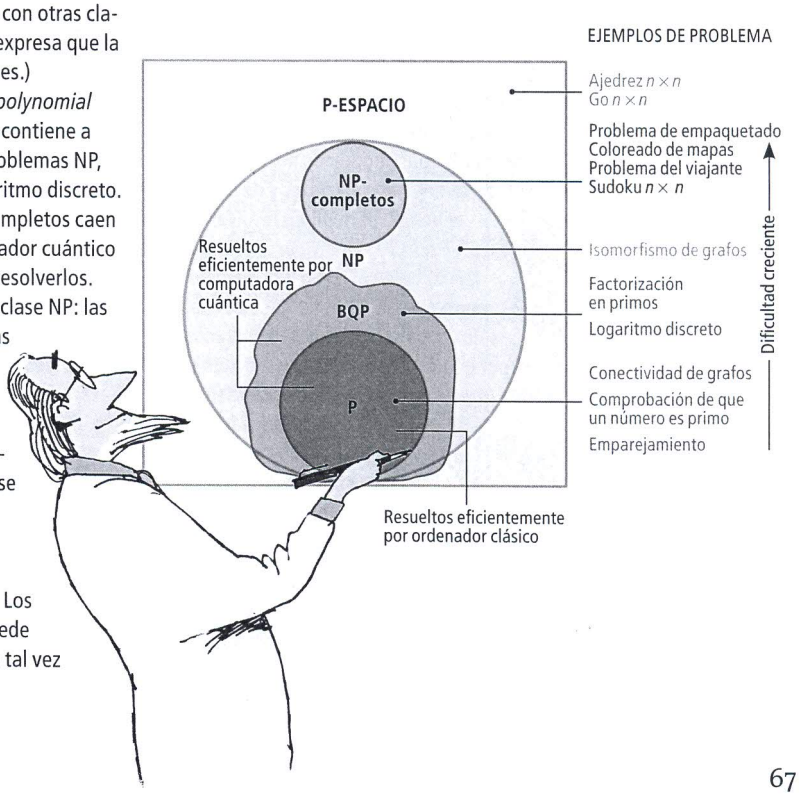
Las computadoras cuánticas encuentran su lugar

El mapa de la derecha representa de qué forma se relacionaría la clase de problemas que los ordenadores cuánticos podrían resolver (BQP) con otras clases de problemas computacionales. (El contorno irregular expresa que la clase BQP no parece encajar pulcramente con las otras clases.)

La clase BQP (la sigla denota *bounded-error, quantum, polynomial time*, es decir, error acotado, cuántico, tiempo polinómico) contiene a todos los problemas de tipo P y también a unos cuantos problemas NP, como el de la factorización o el llamado problema del logaritmo discreto. Se cree que la mayoría de los demás problemas NP y NP-completos caen fuera de la clase BQP, lo que significa que incluso un ordenador cuántico necesitaría más que un número polinómico de pasos para resolverlos.

Por otra parte, los problemas BQP podrían desbordar la clase NP: las computadoras cuánticas podrían resolver ciertos problemas en menos tiempo incluso del que invertiría un ordenador común en comprobar la solución. (Recordemos que un ordenador común puede comprobar eficientemente la solución de un problema NP, pero sólo puede resolver eficientemente los problemas P.) Hasta la fecha, sin embargo, no se conocen ejemplos convincentes de problemas de este tipo.

Los expertos en computación sí saben que la clase BQP no puede extenderse más allá de la clase conocida como P-ESPACIO, que también contiene todos los problemas NP. Los problemas P-ESPACIO son los que un ordenador común puede resolver con una cantidad polinómica de memoria, aunque tal vez exijan un número exponencial de pasos.



ZONAS DE PENSAMIENTO

A diferencia del mundo real, en el cual creemos que los límites computacionales son los mismos dondequiera que se mire, la galaxia de *A Fire Upon the Deep* ("Un fuego sobre el abismo"), novela de ciencia ficción de Vernor Vinge publicada en 1992, está dividida en tres "zonas de pensamiento" concéntricas que poseen límites computacionales y técnicos inherentemente distintos.

En las Profundidades sin pensamiento, las más cercanas al núcleo galáctico, fallan hasta los automatismos sencillos. Los cocientes de inteligencia son ínfimos.

La Zona lenta contiene a la Tierra y tiene las limitaciones que sabemos.

En el Allende, factorías nanotécnicas cuasisentientes construyen maravillas tales como tejidos antigravitatorios y la hipercomputación permite viajar más velozmente que la luz.

La Trascendencia está poblada por peligrosos seres ultrainteligentes y divinales, que poseen técnicas y procesos de pensamiento insondables para los seres de menor rango.

que aprovechar la estructura del problema de formas muy dispares de todo cuanto hayamos visto, de igual modo que deberían hacerlo los algoritmos eficientes de corte clásico. La magia cuántica, por sí sola, no bastaría. Partiendo de esta idea, son muchos ahora los científicos de la computación que conjeturan no sólo que $P \neq NP$, sino también que las computadoras cuánticas no podrían resolver problemas NP-completos en tiempo polinómico.

Teorías mágicas

Por lo que sabemos, los ordenadores cuánticos constituirían la estación término de la computación, la categoría más general de computadoras compatibles con las leyes de la física. Pero no hay todavía una teoría definitiva de la física, por lo que no se puede descartar que algún día una teoría futura descubra un procedimiento físico que resuelva eficientemente problemas NP-completos. Como cabe esperar, no faltan quienes hacen cábalas acerca de clases de computadoras todavía más potentes, algunas de las cuales harían que los ordenadores cuánticos pareciesen tan vulgares como una máquina expendedora. Sin embargo, habrían de basarse en hipotéticos cambios de las leyes de la física.

Una de las características fundamentales de la mecánica cuántica es la linealidad, una propiedad matemática. Daniel S. Abrams y Seth Lloyd demostraron en 1998, mientras estaban en el Instituto de Tecnología de Massachusetts, que si las ecuaciones de la mecánica cuántica contasen con un pequeño término no lineal, los ordenadores cuánticos podrían resolver eficientemente problemas NP-completos. Antes de que empecemos a soñar, debe entenderse que, de existir semejante término no lineal, podría infringirse también el principio de indeterminación de Heisenberg y resultaría posible enviar señales a mayor velocidad que la de la luz. Como señalaban los propios Abrams y Lloyd, la mejor interpretación de estos resultados quizá sea decir que contribuyen a explicar por qué la mecánica cuántica es lineal.

Otro tipo de máquina conjetural que lograría una capacidad computacional fabulosa sería la que condensase un número infinito de pasos en un tiempo finito. Por desgracia, el tiempo, al menos según enseña la física actual, degenera en un mar de fluctuaciones cuánticas (en una espuma, en vez de extenderse por una línea lisa, continua y uniforme) a la escala de 10^{-43} segundos (el "tiempo de Planck"), lo que tornaría imposible ese tipo de máquina.

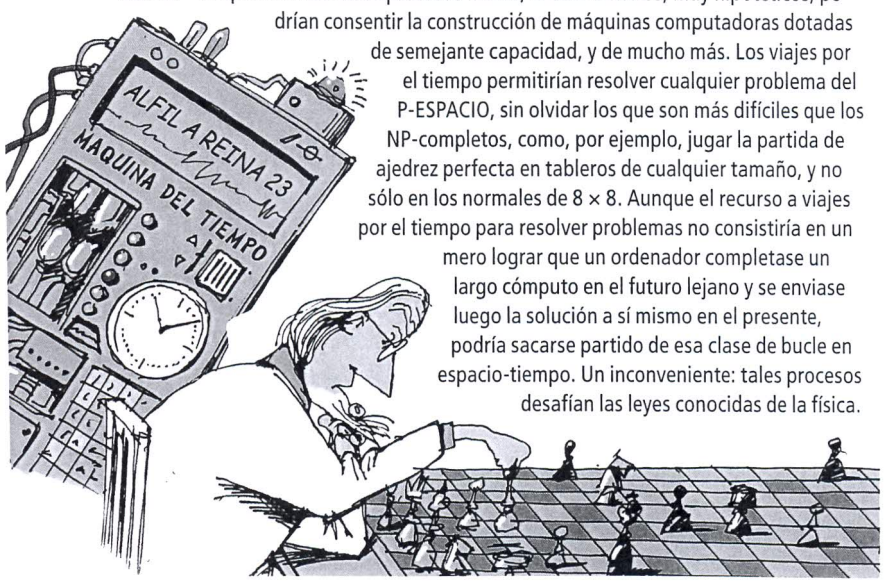
Aunque no resulte posible subdividir el tiempo tanto cuanto se quiera, tal vez otra vía para resolver eficientemente los problemas NP-completos consista en viajar por el tiempo. Quienes estudian el problema no hablan de máquinas del tiempo, sino de curvas de tipo tiempo cerradas (CTC). En esencia, una CTC consiste en una ruta a través del espacio y el tiempo a lo largo de la cual podría viajar materia o energía para reunirse consigo misma en el pasado, generando un bucle cerrado. La teoría física actual no es concluyente sobre la posibilidad de las CTC, pero eso no debería impedir que nos preguntásemos cuáles serían —de existir— sus consecuencias para las ciencias del cómputo.

Parece evidente de qué forma se podría utilizar una CTC para acelerar un cálculo: prográmese nuestro ordenador para que dedique todo el tiempo que haga falta a resolver el problema y seguidamente envíese la solución de vuelta hasta un instante anterior al arranque del ordenador. Es una pena que tan sencilla idea no funcione. Olvida la famosa paradoja del abuelo: remontarse en el tiempo para matar al propio abuelo (así que no naceríamos, con lo que no podríamos retroceder en el tiempo; nuestro abuelo, al fin y al cabo, vivió y tuvo hijos, y después nacimos nosotros, pero entonces...). En nuestro supuesto: ¿qué ocurriría si apagásemos la computadora en cuanto recibiéramos su respuesta remitida desde el futuro?

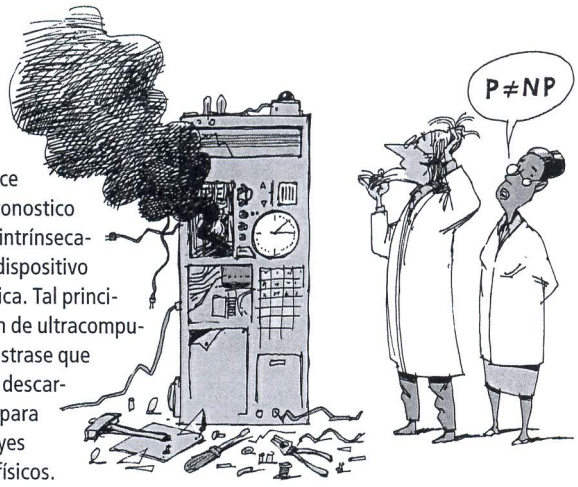
En 1991, el físico David Deutsch, de la Universidad de Oxford, definió un modelo de computación con curvas de tipo tiempo cerradas que elude esta dificultad. En el modelo de Deutsch, la naturaleza garantizaría que conforme se desarrollasen los acontecimientos a lo largo de la línea del tiempo que compone la CTC no llegaran nunca a aparecer parado-

¿Ultracomputadoras llegadas de una física exótica?

Parece inverosímil que las computadoras cuánticas puedan resolver rápidamente problemas NP-completos. Pero otros procesos físicos, extraordinarios, muy hipotéticos, podrían consentir la construcción de máquinas computadoras dotadas de semejante capacidad, y de mucho más. Los viajes por el tiempo permitirían resolver cualquier problema del P-ESPACIO, sin olvidar los que son más difíciles que los NP-completos, como, por ejemplo, jugar la partida de ajedrez perfecta en tableros de cualquier tamaño, y no sólo en los normales de 8 × 8. Aunque el recurso a viajes por el tiempo para resolver problemas no consistiría en un mero lograr que un ordenador completase un largo cómputo en el futuro lejano y se enviase luego la solución a sí mismo en el presente, podría sacarse partido de esa clase de bucle en espacio-tiempo. Un inconveniente: tales procesos desafían las leyes conocidas de la física.



¿Un nuevo principio físico?



Dado que para construir una computadora capaz de resolver problemas NP-completos parece necesario apelar a propiedades físicas inverosímiles (como los viajes por el tiempo), yo pronostico que los científicos adoptarán algún día un nuevo principio: "Los problemas NP-completos son intrínsecamente difíciles". Es decir, la resolución eficiente de estos problemas es imposible en cualquier dispositivo que pueda construirse en el mundo real, cualesquiera resulten ser finalmente las leyes de la física. Tal principio entraña la imposibilidad de los viajes por el tiempo, pues tales viajes permitirían la creación de ultracomputadoras capaces de resolver eficientemente problemas NP-completos. Más todavía, si se demostrase que una teoría propuesta permitiría la construcción de tales computadoras, dicha teoría podría ser descartada *a priori*. La aplicación del principio sería similar a recurrir a los principios termodinámicos para concluir que las máquinas de movimiento perpetuo son imposibles (están prohibidas por las leyes de la termodinámica) y para deducir características hasta entonces desconocidas de procesos físicos.

jas. Esta circunstancia podría utilizarse para programar un ordenador que trazase un bucle temporal por una CTC con el fin de resolver problemas difíciles.

Con una CTC podríamos resolver eficientemente no sólo problemas NP, sino incluso problemas pertenecientes a una clase más amplia, la clase P-ESPACIO. El P-ESPACIO está constituido por la clase de problemas que podrían resolverse en un ordenador corriente utilizando una cantidad de memoria con crecimiento polinómico, aunque exigieran un tiempo de ejecución con crecimiento exponencial. En efecto, una CTC haría que el tiempo y el espacio fuesen intercambiables en cuanto recursos computacionales. (No hubo necesidad de mencionar hasta ahora la limitación polinómica de la memoria porque para los problemas P y NP no tiene importancia si el ordenador dispone de más memoria que la polinómica.)

Recientemente, John Watrous, de la Universidad de Waterloo en Ontario, y yo hemos demostrado que aunque en una CTC se emplease un ordenador cuántico, por uno clásico, tampoco se podría computar eficientemente ningún problema situado extramuros del P-ESPACIO. Con otras palabras: aunque existieran las curvas de tipo tiempo cerradas, las computadoras cuánticas no se mostrarían más potentes que las clásicas.

Criptonita computacional

Se ignora si futuras teorías llegarán a consentir alguna de estas máquinas tan extraordinarias. Pero, sin negar nuestra ignorancia, podemos ver esta ignorancia desde una perspectiva diferente. En lugar de partir de teorías físicas para preguntarnos cuáles serían sus consecuencias para la computación, podríamos empezar suponiendo que los problemas NP-completos son intrínsecamente difíciles y estudiar después las consecuencias que tal hipótesis tendría para la física. Por ejemplo, si las CTC permitiesen la resolución eficiente de problemas NP-completos y parejamente se admitiera que los problemas NP-completos son intratables, la consecuencia sería que las CTC no pueden existir.

Habrá quienes consideren que tal metodología es superlativamente dogmática. En mi sentir, no difiere de aceptar la validez del segundo principio de la termodinámica o la imposibilidad de la comunicación a velocidad mayor que la de la luz, dos limitaciones que inicialmente tuvieron carácter técnico y que adquirieron con el tiempo el rango de principios físicos. Cierto: cabe la posibilidad de que la segunda ley sea falsada experimentalmente en el futuro. Pero mientras no ocurra, resulta inmensamente más útil suponer que es correcta y aplicar esa hipótesis al estudio de toda clase de cuestiones, desde los motores hasta los agujeros negros. Yo pronostico que la dificultad de los problemas NP-completos recibirá algún día igual consideración: la de un principio fundamental que describe una parte esencial de la naturaleza. No hay forma de saber qué luz teorética arrojará en el futuro la aplicación de un principio fundamental de esta clase, ni las consecuencias prácticas que podría comportar.

En el ínterin, sabemos que no se han de esperar resultados mágicos de las computadoras cuánticas. Habrá quien se sienta decepcionado ante sus aparentes limitaciones. Podemos, sin embargo, darles a estas limitaciones un giro más optimista. Si bien ciertos sistemas criptográficos podrán ser descerrojados en un mundo dotado de computadoras cuánticas, es probable que otros códigos siguiesen siendo seguros. Aumenta así nuestra confianza en que la computación cuántica será posible, pues cuanto más fantástica nos parezca una técnica, mayor deberá ser nuestro escepticismo.

Por último, tales limitaciones aseguran que los científicos de la computación seguirán teniendo tela cortada con la que confeccionar nuevos algoritmos cuánticos. Lo mismo que Aquiles sin su talón o que Supermán sin la criptonita, una computadora carente de limitaciones no tardaría en resultar muy aburrida.

Bibliografía complementaria

QUANTUM COMPUTATION AND QUANTUM INFORMATION. Michael A. Nielsen e Isaac L. Chuang. Cambridge University Press, 2000.

NP-COMPLETE PROBLEMS AND PHYSICAL REALITY. Scott Aaronson en *ACM SIGACT News*, Sección de Teoría de Complejidad, vol. 36. n.º 1. págs. 30-52; marzo de 2005.

QUANTUM COMPUTER SCIENCE: AN INTRODUCTION. N. David Mermin. Cambridge University Press, 2007.

SHOR, I'LL DO IT. (Una explicación del algoritmo de Shor para el no especialista). Scott Aaronson. Disponible en www.scottaaronson.com/blog/?p=208

QUANTUM COMPUTING SINCE DEMOCRITUS. Notas para el curso PHYS771, University of Waterloo, Otoño de 2006. Disponible en www.scottaaronson.com/democritus/