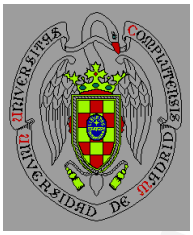

Del bit al qubit*

Alberto Galindo
Departamento de Física Teórica
Universidad Complutense
Madrid, 28040, España

* Lección inaugural del Curso Académico 2001-2002.

A.G.T.

Excmo. y Magnífico Sr. Rector.
Dignísimas Autoridades. Señores Claustrales.
Distinguidos Profesores. Estimados Alumnos.
Señoras. Señores.

0 Introducción

Fue una agradable sorpresa la invitación a impartir esta lección inaugural. En tres décadas largas de desempeño de mi labor como catedrático en esta Universidad, es la segunda vez que la Facultad de Físicas accede a este estrado para cumplir con tan honrosa misión. Por eso, y dado que estoy ya cercano a la jubilación forzosa, acepté a la primera, aun sabiendo el compromiso que conlleva el no defraudar a los compañeros de Facultad a los que represento por el privilegio de mi antigüedad.

He elegido como lección un tema de física. Es tan rara la oportunidad de contar con un auditorio como éste, que no podía permitir dejar pasar una ocasión que tardará en repetirse.

Voy a centrarme en un campo de gran actualidad, en el que confluyen los extraños cuantos de Planck y la información. Los quanta, cuyo centenario celebramos el pasado 14 de diciembre, no sólo han trastocado la visión del mundo físico, sino que su desarrollo tecnológico ha afectado profundamente a la sociedad (microelectrónica, comunicaciones, medicina, farmacia, transportes, computación, gestión administrativa, etc.). La información, que domina incuestionable y crecientemente nuestra vida cotidiana (libros, prensa escrita, radio, televisión, internet),[1] es un cuerpo científico desde los trabajos seminales de Shannon de 1948, y es por su naturaleza un objeto de la física.

De la confluencia de los cuantos y de la información, alentada tanto por los avances tecnológicos en la manipulación de sistemas físicos de unos pocos átomos, fotones, etc., como por la profundización en el desarrollo conceptual de la teoría de la información clásica, ha surgido en la pasada década un vigoroso campo, llamado teoría cuántica de la información, llamado a alterar substancialmente los sistemas de almacenamiento, transmisión y procesado de la información. El objetivo número uno es la fabricación de un ordenador cuántico a escala razonable. Es posible que exija más años de lo que nos gustaría. En esta empresa van a converger con seguridad físicos, matemáticos, ingenieros, químicos, expertos en computación, etc., atraídos por las enormes expectativas que despierta. Y de este empeño se van a beneficiar, y mucho, 1/ la propia física fundamental, por la mejor comprensión del mundo cuántico que facilita la teoría cuántica de la información, y que nos acercará más a su misterioso y extraño comportamiento, y 2/ la tecnología misma de vanguardia, como la metrología de precisión y la nanotecnología [26].

1 Un siglo de "cuantidad"

> *You have nothing to do but mention the quantum theory, and people will take your voice for the voice of science, and believe anything.* GEORGE BERNARD SHAW

Max (Karl Ernst Ludwig) Planck se vió abocado a discretizar los cambios de energía entre átomos y radiación para conseguir explicar los datos experimentales sobre el es-

[1] Parafraseando a John Maynard Keynes, podemos decir, sin mucha exageración, que en la actualidad todos, desde el ciudadano que usa un teléfono móvil o escribe con un ordenador, hasta el científico que calcula una explosión supernova, somos prácticamente esclavos de algún lógico difunto [159].

pectro del cuerpo negro. Fue, diría más tarde, "como un acto de desesperación"(*als einen Akt der Verzweiflung*).[2] El 14 de Diciembre del año 1900 presentó ante la Sociedad Alemana de Física su famoso trabajo[3] donde introducía en la física la constante universal h.

Pocos años después, en su *annus mirabilis* de 1905, Albert Einstein explicaría el efecto fotoeléctrico postulando[4] que la energía de la luz monocromática de frecuencia ν está concentrada en forma de gránulos indivisibles de valor $h\nu$. Estos quanta o paquetes de energía recibirían veinte años después el nombre de fotones.[5]

Roto el viejo tabú de que *Natura non facit saltus* y liberado el duende de la discretización, nuestra visión de la realidad ya nunca sería como antaño. Los cuantos asomaron por doquier (fotones, fonones, fluxones, excitones, rotones, magnones, plasmones, spinones, holones, orbitones,[6] etc.), y todas las partículas del universo pasaron a ser excitaciones elementales de unos pocos campos, uno por especie, lo que explicaba su total indistinguibilidad dentro de cada una de éstas.

Nueve genios sentaron en el primer cuarto del siglo XX las bases de la nueva física:[7] Planck (1900), Einstein (1905) y Niels (Henrik David) Bohr (1913), seguidos de Louis (Victor Pierre Raymond, 7º Duque) de Broglie (1923), Werner Karl Heisenberg (1924), Wolfgang Pauli (1925), Erwin Schrödinger (1926), Max Born (1926), y Paul (Adrien Maurice) Dirac (1928).

1.1 Éxitos de la física cuántica

El impacto de esta naturaleza discontinua ha sido tremendo. Ciertas magnitudes clásicamente continuas (energía, momento angular, ...) presentan valores discretizados. Sistemas simples como los átomos, moléculas y núcleos exhiben espectros de energías (colecciones de energías posibles) con partes discretas. Son como sus "notas" o "vibraciones" características, y se llaman niveles energéticos. Estos espectros de un sistema físico lo identifican generalmente, y gracias a eso hemos podido conocer, por ejemplo, la composición química de las estrellas, y la expansión del Universo. La pequeñez del quantum de acción h de Planck relativa a los valores típicos de la acción clásica impide discernir la cuantización de la energía y de otras magnitudes en la vida ordinaria.

La microfísica actual, desde la escala subnuclear hasta la molecular, sería inconcebible sin el auxilio de los principios cuánticos. La física de la materia condensada, en la que se apoya básicamente gran parte de la tecnología que nos rodea, cambió dramáticamente con la mecánica cuántica (MQ). Los fenómenos más espectaculares de

[2] Noventa años más tarde el universo proclamaría también, a los cuatro vientos, la validez de la fórmula espectral de Planck, al mostrarnos un espectro perfectamente planckiano, mejor que los obtenidos en laboratorio, para el fondo cósmico de microondas, esa radiación fósil liberada por el universo primitivo cuando éste, tras neutralizarse, se hizo transparente a la luz.

[3] Título del trabajo: *Zur Theorie der Gesetzes der Energieverteilung im Normalspektrum* (Sobre la teoría de la ley de distribución de energía del espectro normal), Verhandlungen der Deutschen Physikalischen Gesellschaft **2**, 237-245 (1900).

[4] Título del trabajo: *Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt* (Sobre un punto de vista heurístico concerniente a la producción y transformación de la luz), Annalen der Physik **17**, 132-148 (1905).

[5] El químico G.N. Lewis publicó en 1926 un artículo, *The conservation of photons*, en el que propone un mecanismo de enlace químico basado en unas partículas que llamó "fotones". El nombre cuajó, aunque, evidentemente, no el significado por él propuesto.

[6] La existencia de orbitones ha sido puesta en evidencia recientemente [183].

[7] Los nueve serían galardonados con el premio Nobel de Física: Planck (1918), Einstein (1921), Bohr (1922), De Broglie (1929), Heisenberg (1932), Pauli (1945), Schrödinger (1933), Max Born (1954), y Dirac (1933).

la materia, como la superconductividad y superfluidez, son consecuencia de cuasicondensaciones cuánticas Bose-Einstein. La miniaturización creciente (nanotecnología, sistemas mesoscópicos) ha hecho posible experimentar el efecto de la dimensionalidad, revelando notables diferencias entre los comportamientos de los sistemas 0D (motas o puntos cuánticos), 1D (hilos o alambres cuánticos), 2D (gases bidimensionales) y 3D (sistemas ordinarios).[8] Hasta en la evolución del Universo es necesario invocar la MQ para describir los procesos elementales que ocurrieron hasta la liberación de la luz y mucho más tarde en la producción de energía en las estrellas, y para adentrarnos en la época de Planck, los primeros 10^{-43} s tras la Gran Explosión.

Basta hojear el número de marzo 1999 de Reviews of Modern Physics, celebrando el centenario de la American Physical Society, y que empieza con un artículo de Hans Albrecht Bethe sobre *Quantum Mechanics*, para ver la MQ en todos los rincones de la física, incluida por supuesto la Física Biológica.

1.1.1 Precisión de la MQ

El acuerdo entre teoría basada en MQ y experimento ha alcanzado las más altas cotas conocidas en la física. Un par de ejemplos bastan: 1/ En el problema típico de 3 cuerpos dado por el átomo bielectrónico de He, el cálculo teórico, una vez incluídas las correcciones pertinentes tanto de masa, como relativistas y radiativas o de electrodinámica cuántica (EDQ), las energías de ionización de algunos estados excitados (como el $1s2s\,^1S_0$) concuerdan con los valores experimentales con precisión de 1 parte en 10^9. 2/ Lo mismo ocurre con el momento magnético anómalo del electrón, expresado a través de su anomalía $a_e := \frac{1}{2}(g_e - 2)$, cuya predicción teórica mediante la EDQ ajusta el valor observado en precisión similar a la anterior [85, 219].

1.2 La sorprendente física de los quanta

Si cierto es que la relatividad de Einstein demolió creencias tan arraigadas como la existencia del tiempo con carácter absoluto, o la simultaneidad, desde el punto de vista epistémico ha sido seguramente más perturbadora la teoría de los quanta de Planck que ha dado origen a la actual física cuántica. Con ella se ha derrumbado el determinismo laplaciano, las leyes del azar se han enseñoreado de la predicción científica, lo continuo y lo discreto han dejado de ser antagónicos para convivir en armoniosa dualidad, y media realidad se oculta para dejar ver a la otra mitad.

Las características básicas de la física cuántica son [190]:

1. La indefinición objetiva.
2. El azar y probabilidad objetivos.
3. El enredo.

Desde un punto de vista más físico, hay que añadir [89]:

4. La dualidad onda-partícula.

[8] Ya en 1959 Feynman invitaba a los físicos a explorar tecnológicamente el mundo de lo pequeño, en una conferencia con el provocador título *There's plenty of room at the bottom*. Desde la posibilidad de escribir la Enciclopedia Británica en la cabeza de un alfiler, o meter toda la información escrita existente, que estimaba en unos 10^{15} bits (equivalente a varias decenas de millones de libros), en un cubo de materia del tamaño de una mota de polvo de 100 μm, hasta la fabricación de máquinas capaces de circular por el riego sanguíneo para reparar, por ejemplo, válvulas en el corazón. Decía con su gracia característica: *A friend of mine . . . says that, although it is a very wild idea, it would be interesting in surgery if you could swallow the surgeon. You put the mechanical surgeon inside the blood vessel and it goes into the heart and "looks" around. . . . It finds out which valve is the faulty one and takes a little knife and slices it out. Other small machines might be permanently incorporated in the body to assist some inadequately-functioning organ.*

5. El principio de indeterminación.

1.2.1 La indefinición

Significa que en un estado cuántico α, aunque esté máximamente conocido, hay siempre eventualidades E (proposiciones sí/no) indefinidas, que no son ni ciertas ni falsas. Cuando se somete a consulta al sistema en estado α para ver si una eventualidad E (por ejemplo, estar en una región dada) es verdadera o no, el resultado es objetivamente azaroso, con unas probabilidades que dependen sólo del estado α y de la eventualidad E, y no del ánimo o conocimientos del experimentador. Decimos que la eventualidad E es potencial en α (no tiene un valor definido) y que la acción de una de estas consultas (medida de E) actualiza su potencialidad.

Un estado cuántico es, por así decirlo, una red de potencialidades; consta no sólo de aquellas eventualidades que tiene bien definidas (hablamos entonces de propiedades del estado), sino también de las probabilidades de hallar cierto o falso al actualizar las otras eventualidades, las indefinidas.

1.2.2 El azar cuántico

En el mundo cuántico manda la ventura, y para describir sus fenómenos recurrimos a las probabilidades. Pero no es un mundo azaroso alocado, sino sometido a una reglas muy precisas. La probabilidad $P(\beta,\alpha)$ de que en un estado α del sistema hallemos como ciertas unas eventualidades que, de estar bien definidas, harían que el sistema estuviese en un estado β, viene dada por $|(\beta,\alpha)|^2$, donde la amplitud de probabilidad (β,α) es un número complejo.

El lenguaje de la nueva física es el lenguaje de las amplitudes de probabilidad, con las que, como acabamos de decir, se predice la probabilidad de que algo ocurra en el mundo físico; las certezas se han evaporado, y por mucho que afinemos en el conocimiento del estado inicial de un sistema físico subsisten elementos de ignorancia irreductibles.

Pero estas probabilidades cuánticas obedecen a unas reglas de juego muy peculiares e inequívocas: cuando algo puede ocurrir de varias maneras indistinguibles, la probabilidad de que ocurra no es la suma de las probabilidades individuales (como ocurre al tirar un dado), sino el cuadrado de la suma de sus "raíces cuadradas", de sus amplitudes de probabilidad. Y como las raíces cuadradas pueden ser positivas y negativas (mejor dicho, tienen fase), puede muy bien ocurrir que se cancelen y que la probabilidad total sea nula (interferencia destructiva). ¿Alguien esperaría que al arrojar a la vez dos dados no trucados nunca pudieran sumar 3, cuando lo común sería que esa suma se diera una vez cada 18, en promedio? Pues eso podría ocurrir con dados cuánticos.

Cuando las potencialidades no se actualizan, esto es, cuando las alternativas son indistinguibles, las amplitudes se suman antes de calcular la probabilidad: por ejemplo,

$$(\beta,\alpha)=\textstyle\sum_\gamma(\beta,\gamma)(\gamma,\alpha),\quad P(\beta,\alpha)=\left|\sum_\gamma(\beta,\gamma)(\gamma,\alpha)\right|^2.$$

donde γ es un estado cualquiera con propiedades definidas para un conjunto completo de eventualidades compatibles (es decir, simultáneamente medibles) no actualizadas. Pero si estas se observan, la probabilidad pasa a valer

$$\bar{P}(\beta,\alpha)=\textstyle\sum_\gamma|(\beta,\gamma)|^2|(\gamma,\alpha)|^2=\sum_\gamma P(\beta,\gamma)P(\gamma,\alpha).$$

Decimos entonces que al medir se rompe la coherencia de las diferentes alternativas.

Estas reglas explican una de las peculiaridades de los quanta, su disposición a interferir. No es lo mismo el cuadrado de la suma que la suma de cuadrados:

$$|(\beta,\alpha)|^2 = \left|\sum_\gamma (\beta,\gamma)(\gamma,\alpha)\right|^2 \neq \sum_\gamma |(\beta,\gamma)(\gamma,\alpha)|^2.$$

En la primera igualdad se producen interferencias cuánticas, pues las alternativas γ no se materializan. La segunda igualdad corresponde al caso de que se actualicen estas eventualidades.

1.2.3 El enredo

El enredo, entrelazamiento o enmarañamiento es quizá la más peregrina y enigmática distinción de los quanta [92]. Introducido el enredo (*Verschränkung*) por Schrödinger en 1935 para denotar superposición lineal de estados factorizables de varias partículas, se refería a él diciendo que "no era *un* sino *el* rasgo característico de la MQ". Einstein no soportaba sus consecuencias de aparente acción instantánea a distancia. De "acción fantasmal a distancia" hablaba Einstein en una carta a Born. De "vudú" cuántico lo ha calificado Charles H. Bennett.

El enredo se da, por ejemplo, en un sistema bipartito 1+2 que tiene un estado global mejor definido que cualquiera de sus partes 1 y 2. Los estados enredados presentan correlaciones sutiles sin equivalente clásico.

El enredo no existe clásicamente; pero en la MQ, en que los estados son una red de potencialidades como he dicho, es posible tener un estado en que unas eventualidades E_1, E_2 de las partes 1 y 2 estén individualmente indefinidas, pero correlacionadas entre sí de forma tal que al actualizarse en sendas medidas, siempre sean las dos falsas, o las dos correctas.

Un estado enredado por antonomasia es el estado singlete de dos partículas de spin $\frac{1}{2}$: $2^{-1/2}(\uparrow\downarrow - \downarrow\uparrow)$. Las dos partículas tienen sus polarizaciones anticorrelacionadas: si el spin de una apunta en una dirección, el de la otra lo hace en la opuesta. Ninguna de ellas tiene un estado definido; la información del estado reside en correlaciones no locales esparcidas por todo, sin que ninguna medida local sobre una de las partes pueda revelarla por sí sola. Si la partícula 1 vuela hacia Zaragoza y la 2 hacia Sevilla, lugares en que nuestros colegas físicos miden sus estados de polarización en dirección vertical, los resultados, aunque aleatorios para cada uno, están en perfecta correlación mutua $\uparrow \Longleftrightarrow \downarrow, \downarrow \Longleftrightarrow \uparrow$. Y esto se cumple, por muy separados que estén entre sí los físicos que comparten el par.[9]

El enredo está doquiera: desde los estados atómicos (estados hiperfinos del H, por ejemplo), hasta la materia condensada (pares de Cooper, por ejemplo). Pero no es fácil producir estados enredados en un sistema de modo que los subsistemas que lo componen estén lo bastante separados espacialmente como para poder actuar individualmente sobre ellos.

El papel del enredo como recurso informático en la actual teoría cuántica de la información y en sus desarrollos experimentales es, como veremos, central, comparable al de la energía o al de la entropía. Se ha llegado a decir que es como *iron to the classical world's bronze age* [164]. Esta manera moderna de mirar al enredo como un recurso, una especie de moneda de cambio como pueda ser la energía, independiente de

[9] Estas correlaciones máximas se han observado en pares enredados de fotones separados a distancias de 10.9 km (entre las localidades suizas de Bellevue y Bernex). Los fotones se produjeron en Ginebra y llegaron por fibra óptica de la Swiss Telecom a esos pueblos próximos a Ginebra (a 4.5 y a 7.3 km de Ginebra, respectivamente). Este experimento muestra que, con extremo cuidado en el manejo experimental, las correlaciones no disminuyen con la distancia.

su soporte, culminará el día en que dispongamos de un lenguaje científico de alto nivel en el que el enredo sea ingrediente básico en el razonamiento. Todavía no sabemos bien cómo cuantificar el enredo, ni conocemos las leyes que rigen su transferencia, su creación o su desaparición [163]. Como muestra del potencial impacto del enredo en otras áreas, diremos que el problema central de la teoría de la computación, a saber, la inclusión propia $\mathsf{P} \subsetneq \mathsf{NP}$, quedaría resuelto en sentido afirmativo si el contenido de enredo de algunos estados cuánticos superase un cierto umbral [162].[10]

1.2.3.1 ¿Transmisión superlumínica? ¿Cabe utilizar el enredo compartido para enviar información de Zaragoza a Sevilla a velocidad superlumínica? Sí, si los físicos de Zaragoza supieran codificar un mensaje significativo con los bits de polarización que obtienen. Pero no es así, pues las leyes cuánticas garantizan que cada muestra de bits obtenida en Zaragoza es absolutamente aleatoria. Si se selecciona un subconjunto de la misma para codificar información, por ejemplo una secuencia de tres 1's seguidos si queremos transmitir el número primo 3, en Sevilla medirán en esos lugares tres 0's. Pero habrá que decirles (teléfono, correo electrónico, etc.) a qué lugares deben fijarse si queremos que identifiquen la información del 3. Y que sepamos, nadie sabe hacer superlumínico este último paso de la comunicación.

Si la clonación general de estados cuánticos fuera posible,[11] el enredo podría ser usado para la transmisión superlumínica de información: pues en Zaragoza podrían medir la polarización de sus miembros de los sistemas enredados siguiendo un mensaje binario ($0 \longleftrightarrow \pm_z, 1 \longleftrightarrow \pm_x$), lo que instantáneamente haría que los comiembros en Sevilla se polarizasen en las direcciones opuestas; su clonación haría posible a los colegas sevillanos determinar con fidelidad estas polarizaciones, y por tanto, leer el mensaje.

1.2.3.2 Consecuencias del enredo El enmarañamiento es responsable de algunas de las predicciones más sorprendentes de la MQ. El siguiente ejemplo (adaptado de uno similar de John Preskill [172]) ilustra lo extraño que es el mundo cuántico.

Supongamos tres cajas A, B, C, una en Zaragoza, otra en Madrid, y otra en Sevilla. Cada caja tiene tres puertas, 1 (frontal), 2 (lateral) y 3 (superior), y su interior aparece de color rojo o verde al abrirla por cualquiera de ellas. Según qué puerta se abra, el color puede cambiar, de acuerdo con estas reglas: si vemos un interior rojo (verde) al abrir una de las puertas, al cerrarla y volverla a abrir de nuevo seguimos viendo el rojo (verde); pero si, tras conocer el color interior al abrir por una puerta, cerramos esta y optamos seguidamente por destapar otra puerta distinta, un 50% de las veces vemos que el interior es rojo, y en el otro 50% restante, verde.

Supongamos que se ha preparado el conjunto de interiores en estas "curiosas" cajas en un estado especial, en el que al abrir las tres por la puerta superior (puerta 3) aparecen sus interiores o todos rojos, o todos verdes, con igual amplitud de probabilidad.

Experimentalmente se comprueba sobre ese estado que si en una caja se abre la puerta 1 y en las otras dos cajas la puerta 2, siempre se ve un número par (0 o 2) de interiores rojos e impar (1 o 3) de verdes.

Luego podemos inferir con certeza el color $c \in \{r, v\} := \{\text{rojo,verde}\}$ que se verá al destapar una puerta arbitraria $k \in \{1, 2, 3\}$ de la caja $X \in \{A, B, C\}$ conociendo los

[10] De paso el que pruebe esto se llevará 1 M$, ofrecido por el Clay Mathematics Institute a quien resuelva alguno de los siete grandes problemas matemáticos de este nuevo siglo.

[11] Como comentaré luego, la linealidad/unitariedad de la MQ prohíbe la clonación cuántica: ¡no existen fotocopiadoras cuánticas!

colores que se ven al abrir las otras dos cajas $Y, Z \in \{A, B, C\}$ por puertas adecuadas: 1/ Si $k = 3$, basta abrir Y, Z por la puerta 3, y su color (común necesariamente) es también el de X. 2/ Si $k = 1$, abramos Y, Z por la puerta 2; si sus colores son iguales, entonces $c = v$, y si son distintos, $c = r$. 3/ Si $k = 2$, abriendo Y por la puerta 2, y Z por la puerta 1, rige la misma conclusión que en el caso 2/. El color del interior al destapar una puerta arbitraria k de una caja X sería, por tanto, determinable con certeza observando solamente sobre el resto Y, Z del sistema, un resto que bien podría estar separado causalmente de X; según dicta el realismo local, dicho color debe ser en consecuencia un elemento de realidad según el criterio de Einstein, Boris Podolsky y Nathan Rosen, una propiedad que posee la caja en cuestión con independencia de que se miren o no los interiores de las otras dos cajas a través de puertas cualesquiera.

Ahora nos entra la curiosidad de saber *a priori* qué veremos si abrimos las tres cajas por la puerta 1. Y vamos a razonar del modo siguiente, que presupone la existencia de esos elementos de realidad que acabamos de mencionar. Al abrir dos de las cajas (digamos la A y la B) por la puerta 1 pueden ocurrir tres casos: los interiores respectivos son ambos verdes, ambos rojos, o uno rojo y el otro verde. a/ Supongamos que ambos son verdes. En virtud del hecho experimental antes citado, los interiores por la puerta 2 de las cajas B y C (A y C) deben ser ambos del mismo color, y por tanto también los de las cajas A y B, lo que a su vez exige que el interior de la caja C por la puerta 1 sea verde. b/ Si los interiores de las cajas A y B por la puerta 1 son rojos, los de las cajas B y C (A y C) por la puerta 2 deben ser de distinto color, y por tanto iguales los de las cajas A y B, con lo que concluimos de nuevo que el interior de la caja C por la puerta 1 deber ser verde. c/ Finalmente, si los interiores de las cajas A y B por la puerta 1 son distintos, digamos rojo en la A y verde en la B, los de las cajas B y C (A y C) por la puerta 2 deben ser de distinto (igual) color, y por tanto distintos los de las cajas A y B, de donde inferimos que el interior de la caja C por la puerta 1 deber ser rojo.

En cualquier caso, pues, podemos afirmar por nuestra argumentación teórica que al abrir las tres cajas por la puerta 1 veremos un número par de interiores rojos.

Comprobémoslo ahora experimentalmente ... ¡Vaya! ¡Pero si sale todo lo contrario! ¡Siempre se ve a través de las tres puertas 1 un número impar de interiores rojos!

¿Dónde falla el argumento? Sólo hay algo que hemos supuesto tácitamente, al aceptar los elementos de realidad: que la observación de los interiores de dos de las cajas no altera el interior de la otra. Y para más respaldo interno a esta hipótesis, podemos pensar en llevar cada una de las tres cajas a una galaxia diferente (la 1 a Andrómeda, la 2 a la Gran Nube de Magallanes, y la 3 la dejamos en nuestra Galaxia), y destapar las tres a la vez, de modo que no haya tiempo a que la información de lo visto en alguna de las cajas llegue a las otras. ¿Cómo va a "influir" el abrir la caja 2 en la Gran Nube de Magallanes sobre el color interior (por cualquiera de sus puertas) de las caja 1 en Andrómeda y 3 aquí? Es absurdo pensarlo, ¿no? Pues sí, será todo lo absurdo que nos parezca, pero de hecho esa *spooky action at a distance*, esa inesperada coordinación no local, forma parte de las leyes de la naturaleza, y se da en el insólito mundo de los quanta. Este experimento de las cajas es evidentemente ideal, pero otros de similar concepción y en principio factibles en el laboratorio podrían mostrar nítidamente que la MQ es incompatible con el realismo local.[12]

Querámoslo o no, la MQ es extraña y antiintuitiva. Decía Bohr: "Quien no se sienta estupefacto ante la MQ es que no la ha entendido bien".

[12] El debate histórico Bohr-Einstein en torno a esta cuestión acaba de cerrarse, a favor del primero: un experimento reciente con pares de iones $^9Be^+$ enredados muestra inequívocamente que el realismo local es insostenible [182].

1.2.4 Dualidad onda-partícula

Isaac Newton mantuvo la naturaleza corpuscular de la luz, pero Christiaan Huygens defendió su naturaleza ondulatoria, que Thomas Young demostraría brillantemente muchos años después. Al comenzar el siglo XX nadie dudaba de que la luz era una onda electromagnética (EM). Pero ciertos fenómenos (como el efecto fotoeléctrico, y el efecto Compton) requerían la vuelta atrás hacia una imagen de la luz como un chorro de partículas, los fotones. ¿Cómo reconciliar estos aspectos corpusculares con los aspectos ondulatorios, evidenciados por todas las experiencias de interferencia y difracción?

No ha sido fácil aprender a convivir con una realidad extraña que se comporta de dos modos opuestos según el entorno [89]. Nuestro lenguaje ha debido acomodarse; no es "científicamente correcto"decir que la luz es una onda, ni tampoco que es una colección de partículas. No es ninguna de esas cosas, sino ambas a la vez. Dependiendo de las circunstancias externas, se realza una faceta y se deprime la complementaria.

Corrientemente el aspecto discretizado de la luz no es discernible, debido al elevado número de fotones que hay en una onda EM ordinaria. Pensemos que, por ejemplo, una humilde vela de 0.1 mW en visible arroja por segundo la friolera de 3×10^{14} fotones de esa parte del espectro; a 100 m de distancia el número de tales fotones que penetran en cada uno de nuestros ojos es 10^5. De una estrella de primera magnitud recibimos una energía visual de unos 2×10^{-8} W/m^2, que corresponde a 10^6 fotones por pupila y segundo.

Si las ondas por antonomasia, las ondas EM, se comportan a veces como partículas (de masa nula), ¿no podrán acaso presentarse en ocasiones las partículas (de masa no nula) como si fueran ondas? Esta es la pregunta que se planteó el joven De Broglie (1923-1925) y para la que, por puras consideraciones de analogía y simetría, se atrevió a proponer una respuesta afirmativa, contra toda evidencia secular. Su idea impresionó a Einstein.

De Broglie postuló que toda partícula material lleva asociada una onda "de materia"que la dirige o guía (onda "piloto") en su movimiento; más adelante (Born 1926) se concluiría que se trataba en realidad de una onda amplitud de probabilidad, cuyo módulo cuadrado en un punto era proporcional a la (densidad de) probabilidad de hallar allí la partícula. Si la partícula, de masa m, tiene energía total $E=\gamma(v)mc^2$ y momento lineal $p=\gamma(v)mv$, la onda asociada tiene frecuencia y longitud de onda dadas por las mismas expresiones que rigen para los fotones:

$$\lambda = h/p, \quad \nu = E/h$$

Se conocen como relaciones de Einstein-De Broglie. La primera proporciona el valor de la longitud de onda de De Broglie.

Los experimentos de Davisson-Germer y de Thomson[13] confirmaron plenamente la existencia de las ondas de materia.

En la vida ordinaria no percibimos esta dualidad: la longitud de onda de los cuerpos macroscópicos es tan pequeña que no hay "ranuras"ni "orificios"que puedan utilizarse para desvelar su aspecto ondulatorio.[14] Sin embargo, ahí está.

[13] Curiosa familia esta de los Thomson, en la que el padre, Joseph John Thomson, recibió el premio Nobel en 1906 por descubrir la "partícula electrón" en 1897, y el hijo, George Paget Thomson, lo recibió en 1937, compartido con Clinton Joseph Davisson, por mostrar la "onda electrón". Sobre esta doble "personalidad" de los sistemas cuánticos bromeaba William Henry Bragg, que compartió el Nobel en 1915 con su hijo William Lawrence Bragg, diciendo: *Physicists use the wave theory on Mondays, Wednesdays, and Fridays, and the particle theory on Tuesdays, Thursdays, and Saturdays.*

[14] Echemos la cuenta. Para una bola de billar de masa $m = 0.5$ kg, por ejemplo, que se mueva sobre el

1.2.4.1 Ondas de materia En un bonito experimento se han detectado las ondas de materia asociadas a fullerenos C_{60} [7]. Se trata de los proyectiles de mayor masa (en un orden de magnitud, pues su masa es de unas 720 u) y complejidad (60 núcleos y 360 electrones, y por tanto con muchos grados de libertad internos excitables) con que se han podido ver interferencias en un experimento del tipo doble rendija (en este caso una red de difracción); hasta la fecha, se habían observado con electrones, neutrones, átomos, dímeros, y cúmulos pequeños de varios átomos de gases nobles ligados por fuerzas de van der Waals. Los fullerenos fueron producidos en un horno de unos 900-1000 K, que tras pasar por dos ranuras de colimación de 10 μm separadas en 1.04 m, incidían sobre una red de difracción de rendijas de 50 nm y período de separación de 100 nm. La imagen de interferencia se observó a 1.25 m de la red, detectando los fullerenos tras su ionización mediante un rayo láser.

Este experimento revela la interferencia de cada fullereno consigo mismo. Esta interferencia es visible porque no se tiene información de qué camino ha seguido el fullereno. Si éste emitiese luz que nos indicase por qué rendija ha pasado, la imagen de interferencia desaparecería. Para ello es preciso que la longitud de onda λ de la radiación emitida satisfaga $\lambda \ll d$, siendo d la distancia entre rendijas consecutivas. Pero a 900 K, cada fullereno tiene una energía vibracional de unos 7 eV, almacenados en 174 modos vibracionales; cuatro de estos modos emiten radiación infrarroja de 7-19 μm, y durante los 3 ms de tránsito entre la red y la detección emiten de 2 a 3 de esos fotones infrarrojos. Mas su longitud de onda cumple $\lambda \gg d$, y por tanto no permitan identificar la rendija atravesada. Otro tanto pasa con la radiación de cuerpo negro que cada fullereno caliente emite, y que es del orden de 0.1 eV durante su tiempo de vuelo por el trayecto, por lo que cada fotón asociado tiene como mínimo una longitud de onda de $10\,\mu\text{m} \gg d$. La velocidad media de estos fullerenos del experimento fue de 220 m/s, y por tanto su longitud de onda de De Broglie era 2.5 pm, unas 400 veces menor que su diámetro de ~ 1 nm. Es posible que este tipo de experimentos pueda extenderse a sistemas más grandes, como macromoléculas e incluso a virus.[15]

1.2.5 El principio de indeterminación

En la física clásica, conociendo las posiciones y momentos iniciales de cada una de las partículas de un sistema, podíamos en principio predecir con exactitud cuáles iban a ser esas magnitudes un rato más tarde. Ya no; para empezar, un principio de indeterminación, debido a Heisenberg, impide que podamos medir con precisión arbitraria y a la vez una variable de posición y la correspondiente variable del momento. O una u otra; debemos conformarnos con conocer sólo una mitad de las variables que clásicamente estaban a nuestro alcance [89].

Un ciudadano normal alberga pocas dudas sobre la posibilidad de medir a la vez la posición de una moto y su velocidad; por eso encuentra natural que en la notificiación de una multa de tráfico por exceso de rapidez le señalen ambos datos. En un mundo hipotético en que la constante de Planck tuviese un valor parejo al de la acción de una

tapete a 0.4 m/s, la longitud de onda λ de De Broglie vale $h/mv = 3 \times 10^{-33}$ m. No se conocen "orificios"ni "ranuras"de estas dimensiones para poder observar la difracción e interferencia de tales ondas. Incluso para cuerpos tan livianos como una mota de polvo ($m \sim 1\ \mu$g), y velocidades tan pequeñas como las provocadas por agitación térmica debida al fondo cósmico de microondas ($T \sim 3$ K, $v \sim 10^{-7}$ m/s), resulta $\lambda \sim 10^{-18}$ m.

[15] La difracción de helio por una red similar ha permitido medir recientemente [98] la longitud de enlace de las moléculas diatómicas más grandes y menos ligadas, a saber, moléculas $^4He_2$. Su energía de ligadura es de unos 10^{-7} eV, y la longitud de enlace de unos 5 nm.

avioneta en vuelo durante 1 s, por ejemplo, $h \sim 10^6$ J s,[16] el agente de policía tendría que renunciar o al lugar o a la celeridad, pues, como consecuencia del principio de indeterminación de Heisenberg que vamos a discutir, medir la velocidad de la moto con precisión de 10 km/hora exigiría desconocer su localización en aproximadamente 2 km. Y eso porque en tan extraño escenario la mera iluminación transversal del motorista con un solo fotón de ondas de radio de $\lambda \sim 1$ m para verle al pasar con precisión de 1 m podría transferirle momento más que suficiente para desviarle peligrosamente de su trayectoria.

Vivimos, sin embargo, en un Universo en el que el cuanto de acción es pequeño a escala ordinaria, y los efectos del principio de indeterminación se dejan notar sobre "motoristas"mucho más livianos: electrones, protones, núcleos atómicos, moléculas, etc.

Tras un cuidadoso análisis de los procedimientos de medida de magnitudes básicas como posición, momento y energía, Heisenberg enunciaba en 1927 su famoso principio de indeterminación. Este principio de incertidumbre limita las precisiones con que se pueden medir simultáneamente sobre una partícula pares (A, B) de magnitudes conjugadas tales como (x, p_x): $\triangle A \triangle B \geq \frac{1}{2}\hbar$.

La razón de las relaciones de indeterminación reside en la dualidad onda-partícula. Por ejemplo, para ver dónde está una cosa con precisón $\triangle x$, lo normal es iluminarla con luz de longitud de onda $\lambda \lesssim \triangle x$, pero los fotones intercambian energía y momento con ella (efecto Compton), lo que conlleva una imprecisión $\triangle p_x \sim h/\lambda \gtrsim h/\triangle x$.

Quizás la consecuencia más distinguida del principio de indeterminación sea la estabilidad de la materia: clásicamente los electrones atómicos son como pequeñas antenas radiantes que deberían caer sobre el núcleo en tiempos de unos pocos ps, haciendo inestables los átomos. El principio de indeterminación viene a su rescate, posibilitando de este modo la existencia de la tabla periódica y toda la riqueza estructural de la física atómica y molecular: al caer los electrones, se confinarían más; esto obligaría cuánticamente a aumentar su energía cinética, contrarrestando así la caída.[17]

1.3 ¿Entender la MQ? Una cierta insatisfacción colectiva

> *Turning to quantum mechanics, we know immediately that here we get only the ability, apparently, to predict probabilities. Might I say immediately, so that you know where I really intend to go, that we always have had (secret, secret, close the doors!) we always have had a great deal of difficulty in understanding the world view that quantum mechanics represents. At least I do, because I'm an old enough man that I haven't got to the point that this stuff is obvious to me. Okay, I still get nervous with it. And therefore, some of the younger students . . . you know how it always is, every new idea, it takes a generation or two until it becomes obvious that there's no real problem. It has not yet become obvious to me that there's no real problem. I cannot define the real problem, therefore I suspect that there's no real problem, but I'm not sure there's no real problem. So that's why I like to investigate things.*
>
> FEYNMAN

> *Quantum mechanics, that mysterious, confusing discipline, which none of us really understands, but which we know how to use.*
>
> GELL-MANN

Nadie presume de entender la MQ. Todo lo contrario. Los más grandes físicos de este siglo (Bohr y Einstein) y otros también preclaros (John Stewart Bell, Richard Phillips Feynman, Murray Gell-Mann y Steven Weinberg) se han mostrado perplejos y

[16] Esta acción macroscópica es también parecida a la desarrollada por un ciclista en una etapa contra-reloj a lo largo de un par de km.

[17] Este argumento, aunque físicamente correcto, no es consecuencia rigurosa de las relaciones de indeterminación de Heisenberg. Puede sustanciarse mediante una desigualdad de Sobolev algo más refinada [90, 91].

nerviosos ante las sutiles fintas dialécticas que propician los quanta.[18] Ninguno niega su enorme éxito para explicar cuantitativamente los fenómenos conocidos tanto en la física de lo pequeño como en la física de la materia condensada. Y la mayoría de los físicos saben cómo aplicarla correctamente en esas situaciones. Pero cuando se intenta describir el comportamiento de un quantum individual, la extrañeza y el desconcierto se nos apoderan.

Tres cuartos de siglo no han sido suficientes para disipar todos las dudas que plantean los principios cuánticos a gran número de profesionales. Destaca como particularmente acérrimo o rebelde el problema de la medición: mientras la evolución de un sistema cuántico cerrado es unitaria, y por ende lineal, reversible y determinista, al actualizar potencialidades, como en una medición sobre el sistema, el estado de éste sufre generalmente el infame "colapso" [91, 93], o "reducción",[19] no unitario, irreversible y probabilista. ¿Son reconciliables ambos tipos de cambio?

La linealidad de la evolución de un sistema en entornos no reactivos (esto es, insensibles a los cambios del sistema) traslada la indefinición objetiva de los sistemas cuánticos a los aparatos de medida, contra toda evidencia práctica. El gato de Schrödinger es la ilustración pintoresca de este conflicto.[20] Se han ofrecido muchas soluciones a este problema: desde considerar evoluciones no lineales, que se percibirían sólo en sistemas de muchos grados de libertad, con la virtud de llevar en tiempos muy cortos cualquier combinación lineal de estados base del aparato macroscópico de medida (los correspondientes a posiciones definidas de sus agujas) a uno de ellos, hasta reemplazar la ecuación de Schrödinger por otra estocástica, de origen tal vez en la propia estructura del espacio-tiempo que se supondría siempre bien definida (como ajena a las peculiaridades cuánticas). Ninguna de estas propuestas ha fructificado, y algunos experimentos han impuesto límites muy rigurosos a una posible no linealidad en la MQ.

Una alternativa radical es la "interpretación del estado relativo" de Hugh Everett III (1957), o "interpretación de muchos mundos" (modernizada en el formalismo de historias consistentes). En ella el problema que nos preocupa desaparece como por encanto; niega simplemente que se actualicen potencialidades. Hay un sistema cerrado global, el Universo, con un estado que evoluciona lineal y unitariamente. Dado un subsistema 1, y el subsistema resto 2 (del que los observadores formamos parte), al medir en el 1 una magnitud A que puede distintos valores $\{a_1, a_2, \ldots\}$, el Universo (y con él nosotros) se bifurca en una colección de "ramas" o alternativas en las que todos los que allí estamos vemos que esa magnitud A tiene uno solo de esos valores, digamos a_k. No hace falta "reducir" el estado; nuestro estado relativo (neuronal o de consciencia) en esa rama está ya dispuesto a ver sólo ese valor a_k. Pero existen otros observables, para las que la ramificación será distinta y también real. En estas nuevas ramas, el valor de A no estará bien definido, y los observadores en esas ramas tendríamos la incómoda sensación de ver las agujas del aparato que mide A en posiciones indefinidas, en estados "grotescos" como los del gato ni vivo ni muerto. Volvemos, pues, a lo de siempre. No hemos resuelto nada; sí, nos hemos arropado con una miríada de mundos gratuitos (en violación grosera del principio de Occam) donde esconder el problema, pero éste, imperturbable, regresa siempre.

[18] Durante las jornadas "Cajal on consciousness" (Zaragoza, 29/11/99-01/12/99), me decía Gell-Mann que ya por fín comprendía la MQ. Ante mi insistencia, matizaría que la entendía "prácticamente" toda.

[19] La reducción matemática del estado aparece como un *modus ponens* intranscendente en la formulación de la MQ con historias. Pero la unicidad de la actualización es, evidentemente, otro cantar.

[20] *Mesogatos* o gatos mesocópicos de Schrödinger ya se han producido en laboratorio: estados atómicos superposición lineal de estados localizados y separados a distancias de 80 nm, muy superiores a sus tamaños individuales de unos 7 nm, y a las dimensiones atómicas del orden de 0.1 nm.

Siendo pragmático, se puede despachar el asunto[21] de esta guisa. El sistema cuántico interactúa con el aparato de medir, que a su vez lo hace con el ambiente. Los tres, sistema, aparato y entorno, están enredados. Como los grados de libertad de este último, es decir su microestado, no se controlan ni observan por lo general, hay que promediar tomando trazas sobre ellos. En la práctica, el ambiente induce descoherencia entre los "estados de la aguja" del aparato de medida, esto hace perder irremediablemente sus fases relativas, y arrastra con ello al colapso. Sin embargo, sigue abierta la cuestión central de cómo se pasa del "y" al "o", es decir, por qué el resultado de cada acto de medición es uno y no varios. ¿Caerá tal vez fuera de la física?

1.4 ¿Qué será de la MQ en el siglo XXI?

No hay atisbos de necesidad de cambio (pero también a finales del XIX se creía terminado el edificio de la física).[22] La MQ funciona perfectamente, diríamos que demasiado bien para los impacientes que se cansan de paradigmas ya seculares. Sólo la gravitación se resiste a la doma cuántica. La teoría de cuerdas ofrece una solución, lejana de los fenómenos a las escalas de laboratorio, y costosa en dimensiones.[23] Pero a lo mejor es el precio a pagar para una futura revolución de la física en que la propia estructura del ET se haga no conmutativa y supersimétrica, y la MQ, con su constante $\hbar$ de Planck, sea el marco obligado para expresar las nuevas dualidades que generalizan $\alpha_{\rm EM} \leftrightarrow 1/\alpha_{\rm EM}$.

Alguien tan importante como Gerardus 't Hooft defiende que la MQ surge de las fluctuaciones estadísticas en una teoría clásica determinista aplicable en la escala de Planck. Contra esta opinión de 't Hooft, hay otra no menos autorizada. Dice Steven Weinberg: *This theoretical failure to find a plausible alternative to quantum mechanics suggests to me that quantum mechanics is the way it is because any small changes in quantum mechanics would lead to absurdities.*

¿Quién tiene la razón? A lo mejor ninguno. La comparación de la historia de la física del siglo recién acabado con lo que se predecía para ella hace 100 años recomienda el callarse,[24] y esperar alguna que otra sorpresa que alguien contará aquí en el 2101.

Lo que sí es seguro es que, mientras tanto, los físicos experimentadores seguirán realizando brillantes exhibiciones de esas que, por ilustrar de modo simple cuestiones fundamentales de la MQ, automáticamente pasan a los libros de texto, y los físicos teóricos continuarán por un lado descubriendo resultados sorprendentemente simples (teleportación, p.e.) y por otro aplicando las técnicas de cálculo de la MQ a problemas cada vez más complejos, inventando procedimientos computacionales nuevos con la esperanza de que algún día se sepan hacer cálculos precisos y no perturbativos en

[21] *For all practical purposes* (FPAP), como decía Bell en uno de sus últimos trabajos, en el que proponía prohibir el uso del término "medición" en toda discusión seria sobre MQ, y reemplazarlo por el de "experimento".

[22] Lord Kelvin (William Thomson, Baron Kelvin of Largs) llegó a decir que el futuro de la física estaba en medir hasta la sexta cifra decimal. Y Albert Abraham Michelson, en 1894, afirmaba: *The more important fundamental laws and facts of physical science have all been discovered* ....

[23] La gravedad submilimétrica intenta escudriñar ese nuevo mundo a través de presuntas modificaciones de la ley de la gravitación de Newton [6]. Medidas recientes [105] no hallan indicios de cambio de esta a distancias superiores a 0.2 mm. También una aparente violación de la conservación de la energía en el futuro colisionador LHC (*Large Hadron Collider*) del CERN podría señalar la existencia de dimensiones extra por las que se moverían los gravitones, pero no las otras partículas. El fascinante problema de la posible generación y desaparición de las dimensiones tanto espaciales como extra con la evolución del Universo está ya siendo objeto de atención por los físicos [5].

[24] Como dice Woody Allen, "predecir es muy difícil, sobre todo el futuro".

teorías tan ricas y difíciles como la Cromodinámica Cuántica a baja energía [218]. No es descartable en absoluto que nuevas e inesperadas consecuencias de las leyes cuánticas puedan surgir en cualquier momento, resultados que abran perspectivas nuevas. ¡Quién iba a pensar, por ejemplo, que medio siglo después de que se inventara la MQ todavía seguirían descubriéndose aspectos elementales y profundos de la misma, como la imposibilidad de clonación de estados cuánticos!

2 Medio siglo de "bitología"

Según su 7ª acepción en el DRAE, información es "comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada". En esta magnífica definición aparecen de forma más o menos explícita, y en este orden, las tres operaciones a que se somete toda información: transmisión, procesado, y almacenamiento. Y en las tres interviene la física: el vehículo transmisor puede consistir en ondas sonoras, ondas EMs, impulsos electrónicos, etc.; el mensaje recibido se transforma mediante un cerebro, un ábaco, un ordenador, etc., antes de incorporarlo a un archivo y modificar otros datos preexistentes; para uso posterior la información resultante se guarda en una memoria o archivo, ya sea del cerebro, ya sea la de un disco duro, etc., o se escribe en un cuaderno, o en una ficha, o se graba sobre una tableta cuneiforme, etc.[25] Por ello puede afirmarse, con Landauer [131, 132], que la información tiene naturaleza física. Y como objeto físico que es, está sometida, nos guste o no, al dictamen inexorable de las leyes físicas, que por un lado la limitan, y por otro, la potencian; por ejemplo, la información no puede nunca transmitirse a velocidad superior a la de velocidad c de la luz en vacío, pero en cambio goza de las ventajas, como paralelismo masivo, que los principios cuánticos le otorgan.

2.1 El bit

La información está discretizada; viene dada en paquetes irreductibles. La unidad elemental de información clásica es el *bit* (con más precisión *c-bit*, o incluso *cbit*, por bit clásico), un sistema clásico con tan sólo dos estados 0 y 1 (Falso y Verdadero, No y Sí). El nombre de bit (por *binary digit*) se debe a John Wilder Tukey,[26] y su uso como unidad fue introducido por Claude Elwood Shannon en lo que se considera como la Carta Magna de la era de la información: su trabajo, en dos partes, titulado *A mathematical theory of communication* [188].[27]

Cada bit puede ser guardado físicamente; en los ordenadores clásicos, un bit se registra como un estado de carga de un condensador (0 = condensador descargado,

[25] En 1 TB de almacenamiento cabe el contenido de unos 10^6 libros. En los próximos años tendremos discos duros de 400 GB. Hoy se almacenan con tecnología magnetorresistiva gigante (GMR) unos 100 GB por pulgada^2. Con almacenamiento holográfico puede llegarse hasta 6000 GB por pulgada^2, es decir, 1 TB por cm^2.

[26] También se debe a Tukey el nombre de *software*.

[27] Shannon murió el pasado 24 de febrero del 2001. Ha pasado a la historia como pionero de la revolución digital, y sin duda como una de las más grandes figuras del siglo XX. Creador de la codificación, nos enseñó cómo combatir la corrupción mediante la redundancia. Así el corte de un CD con una tijera a lo largo de un radio no afecta para nada la calidad de su audición. Demostró también, contra todo pronóstico, que por un canal ruidoso pueden viajar mensajes con fidelidad tan alta como se desee sin necesidad de bajar sin límite el ritmo de transmisión, bastando que este se mantenga siempre menor que una característica del canal llamada su capacidad. Hasta casi medio siglo después no se han conocido códigos explícitos cercanos a ese ritmo límite de Shannon. La repercusión científica, económica, cultural y social de la obra de Shannon crece con el tiempo, y el mundo actual sería inconcebible sin ella [52].

o diferencia de potencial nula entre sus placas; 1 = condensador cargado, o tensión no nula). Se trata de (islotes continuos de) estados macroscópicamente diferenciados, y separados por una buena barrera de energía para evitar tránsitos indeseables entre ambos; esto es, han de ser lo bastante robustos o estables. Su lectura (con el debido cuidado) no les afecta, y pueden ser clonados o replicados sin problemas.

Cualquier texto ordinario es codificable en una cadena de bits: por ejemplo, nos bastará con asignar a cada símbolo su código ASCII,[28] pasando luego este número a su forma binaria, y completándolo a continuación mediante un bit de paridad a la derecha. Ejemplo: `el siglo de los quanta` se puede codificar como

```
11001010 11011000 01000001 11100111 11010010 11001111
11011000 11011110 01000001 11001001 11001010 01000001
11011000 11011110 11100111 01000001 11100010 11101011
11000011 11011101 11101000 11000011
```

2.2 Los teoremas centrales de Shannon

Aunque ya R.V.L. Hartley en 1928 intentara asignar una medida cuantitativa a la información, la teoría clásica de esta se debe a Shannon, quien en los dos trabajos fundamentales ya mencionados del año 1948, tras la segunda guerra mundial, sentó definitivamente sus bases. Con su *teorema de codificación en ausencia de ruido* mostró cuán *compresible* puede ser un mensaje, o equivalentemente, qué redundancia tiene, y con su *teorema de codificación en un canal ruidoso* halló cuánta redundancia debe incorporarse como mínimo a un mensaje para que a pesar del ruido del canal de transmisión sea *comprensible* a su llegada al otro extremo.

Un sistema de comunicaciones consta genéricamente de estos elementos: 1/ una fuente de información (por ejemplo, una persona hablando), que emite mensajes M; 2/ un codificador de fuente que transforma M en una palabra $m(M)$ de un cierto alfabeto (por ejemplo, cadenas de bits); 3/ un codificador de canal que asocia inyectivamente a cada $m = m(M)$ una palabra código $w = w(m(M))$, generalmente binaria; 4/ un canal de comunicación que recibe a la entrada la palabra w para su transmisión, pero que por ser en general ruidoso introduce errores, y da a su salida una palabra $w' \neq w(m(M))$; 5/ un descodificador de canal que intenta corregir w' cambiándola por la palabra código $w(m(M'))$ más parecida, y produce a su salida una palabra $m' = m(M')$; y 6/ un descodificador de fuente que envía M' a la estación de destino.

2.2.1 Primer teorema de Shannon

Vamos a suponer ahora que el canal de transmisión es perfecto, sin ruido, y para evitar pasos intermedios, que los mensajes de la fuente de información van directamente al canal de transmisión, que los lleva a su destino con toda fidelidad. Pero esto puede ser un proceso costoso, cuya ejecución en tiempo conviene optimizar. Lo cierto es que no todos los mensajes imaginables requieren transmisión frecuente. Es poco usual que alguien quiera mandar a otro un mensaje como `ñkfqÑihn?.#jhubxgdh`, y cuando, por contra, un mensaje se repite a menudo, digamos `Universidad Complutense de Madrid`, podemos acudir al uso de acrónimos como `UCM` para simplificarlos. Estas elementales consideraciones nos indican la prescripción a seguir para ahorrar en el uso del canal: representemos o codifiquemos, de mutuo acuerdo previo entre el que manda el mensaje y su destinatario, los mensajes muy frecuentes por otros más cortos, aunque

[28] *American Standard Code for Information Interchange.*

esto exija alargar la representación de los mensajes poco frecuentes. Estos mensajes código (generalmente números) son los que se envían por el canal. Recordemos, por ejemplo, el código Morse, en el que a la letra que más aparece en inglés, la "e", se le asigna el ".", mientras que la "z", la menos frecuente, se representa por "–..".[29]

El primer teorema de Shannon formalizará estas ideas.

Sea un alfabeto finito $A := \{a_1, \ldots, a_{|A|}\}$, provisto de una distribución de probabilidad $p_A : a_i \mapsto p_A(a_i)$ sobre A, con $\sum_{1\le i\le |A|} p_A(a_i) = 1$. Escribiremos a veces $A := \{a_i, p_A(a_i)\}_{i=1}^{|A|}$. Consideremos los mensajes, palabras o cadenas $x_1x_2\ldots x_n \in A^n$ de caracteres de A, provenientes de una fuente sin memoria o de memoria cero, es decir, formados de modo que en cada lugar de la cadena aparece cada símbolo a con probabilidad $p_A(a)$, estadísticamente independiente de los símbolos en los otros sitios de la cadena.[30]

2.2.1.1 Compresión El primer teorema citado de Shannon asegura que, si $n \gg 1$, la información[31] suministrada por un mensaje genérico de n letras coincide esencialmente con la transmitida por otro mensaje binario, de longitud $nH(A)$, donde $H(A)$ es la entropía de Shannon[32] (incertidumbre, ignorancia o falta de información sobre A antes de recibir una de sus letras, o equivalentemente, la información media aportada por un símbolo de A tras su recepción)

$$H(A) = -\sum_{1\le i\le |A|} p_A(a_i)\log_2 p_A(a_i).$$

En otras palabras, cada letra es comprimible a $H(A)$ bits. Además, este resultado es óptimo.[33]

Sigue de lo dicho que la entropía $H(A)$ de Shannon puede interpretarse como la información esencial, incompresible, de cada letra del alfabeto A; o lo que es lo mismo, como nuestra ignorancia a priori por letra antes de recibir ningún mensaje, de modo que para que al receptor le quede totalmente especificado un mensaje de n letras hay que mandarle por un canal sin ruido $nH(A)$ bits ($n \gg 1$), o equivalentemente, $nH(A)/\log_2|A|$ letras. Por eso se define la redundancia de la fuente A como $R(A) := 1 - H(A)/\log_2|A|$.[34]

[29] Estamos pensando en textos normales en inglés. Notable excepción es la novela GADSBY, A STORY OF OVER 50,000 WORDS WITHOUT USING THE LETTER "E", de Ernest Vincent Wright, en la que no aparece la "e" en ninguna de sus páginas (título, nombre del autor, e introducción excluidos).

[30] Los lenguajes naturales no son así; por ejemplo, en español nunca se da (espero) el digrama QÑ. Pero son, en buena aproximación, límites de fuentes markovianas ergódicas a los que pueden generalizarse los teoremas de Shannon. Se estima que la entropía $H_{\text{inglés}}$ del inglés (con 26 letras y un símbolo de espacio en blanco) es del orden de 1; más concretamente, $0.6 \le H_{\text{inglés}} \le 1.3$, a comparar con la entropía $\log_2 27 = 4.76$ que tendría si fuera una fuente sin memoria y de signos equiprobables.

[31] En la teoría de la información no interesa el contenido semántico de un mensaje, sino su composición sintáctica, la colección de símbolos o letras que lo integran.

[32] La palabra entropía había sido ya introducida en la termodinámica por Rudolf Julius Emanuel Clausius en 1864. Feynman cuenta [81] que Shannon adoptó el nombre de entropía aconsejado por von Neumann, pues esto le daría ... *a great edge in debates because nobody really knows what entropy is anyway.*

[33] La idea básica de la demostración es simple: consiste en fijarse preferentemente en los mensajes *típicos* o más probables. Hay $2^{nH(A)}$ de ellos asintóticamente ($n \to \infty$), en un total de $|A|^n$ mensajes. Los mensajes atípicos son asintóticamente ignorables en probabilidad. Todos los mensajes típicos tienen probabilidades similares $\sim 2^{-nH(A)}$ ($n \to \infty$). Basta con transmitir por el canal de comunicación (supuesto perfecto, sin ruido) el número binario de longitud $nH(A)$ asignado, de común acuerdo entre remitente y destinatario, a cada mensaje típico, para que a su recepción pueda ser identificado el mensaje enviado.

Que esta compresión es óptima se comprende teniendo en cuenta que todas las secuencias típicas son igualmente probables en el límite, y por tanto es imposible enumerarlas con menos bits de modo inyectivo.

[34] Cuando se trata de un idioma, ya hemos dicho en otra nota que este resultado es aplicable aproximada-

2.2.1.2 Codificación Codificar consiste en inyectar mediante una aplicación π un alfabeto fuente F en palabras de un alfabeto código C. La codificación π tiene una extensión π^* al conjunto F^* de palabras de F por concatenación de las imágenes de sus letras (palabras código): $\pi^* : f_1 f_2 \dots f_n \mapsto \pi(f_1)\pi(f_2)\dots\pi(f_n)$. Interesan las codificaciones con descodificación única, esto es, aquellas π tales que π^* es inyectiva. Son las únicas que consideraremos.

Existen métodos muy prácticos de codificación clásica con eficacia cercana al valor óptimo, como el sistema Huffman de codificación instantánea, de múltiples aplicaciones (facsímil, televisión de alta definición, etc.). La esencia de este método consiste, como era de esperar, en representar con series cortas de bits aquellas letras que con más frecuencia aparecen. El siguiente ejemplo servirá de ilustración. Supongamos un alfabeto de cuatro símbolos, digamos A, B, C, D, son probabilidades $0.6, 0.2, 0.1, 0.1$, respectivamente. La codificación binaria ingenua $A \mapsto 00$,$B \mapsto 01$, $C \mapsto 10$, $D \mapsto 11$, en pares de bits tiene una longitud media de 2, que difiere bastante de la entropía $H = 1.57$ bits de este alfabeto. Mucho mejor es su codificación Huffman $A \mapsto 0$,$B \mapsto 10$, $C \mapsto 110$, $D \mapsto 111$, cuya longitud media es 1.6. Nótese además que esta codificación es libre de prefijos o instantánea: ningún código es prefijo de otro y por tanto la descodificación puede realizarse sobre la marcha, sin esperar a recibir toda la ristra binaria, ya que se reconoce inmediatamente el bit último de cada palabra código.[35]

2.2.2 Segundo teorema de Shannon

Si el canal de transmisión es ruidoso (caso común), la fidelidad informativa se pierde, pues una porción de bits pueden alterarse en el camino. Para recuperar la información inicial se echa mano de la codificación, en la que códigos correctores de error se encargan de que los errores inevitables en la transmisión puedan limpiarse al final y quede el mensaje generalmente impoluto y fiel. Pero al contrario que antes, en que la codificación era utilizada para comprimir, ahora las palabras código van a tener muchos bits redundantes; es el precio a pagar para combatir el ruido, pues la transmisión de información se ralentizará inevitablemente. En el lenguaje normal también usamos más letras de las necesarias; pero este exceso es precisamente el que nos permite la identificación instantánea de palabras con alguna errata, o ligeramente incompletas. El segundo y magnífico teorema de Shannon prueba que podemos acercarnos a la fidelidad transmisiva completa tanto como queramos a través de cualquier canal, por ruidoso que sea, siempre que nos conformemos con un ritmo de transmisión que no exceda la llamada capacidad del canal (supuesta no nula).

Supongamos un canal sin memoria y discreto, que acepta palabras de un alfabeto X de la estación de origen (de una fuente sin memoria), y a su salida emite palabras del alfabeto Y de la estación de destino. Sea $(p_{Y|X}(y_j|x_i))$ la matriz estocástica del canal dada por las probabilidades de que el símbolo $x_i \in X$ a la entrada aparezca a la salida como $y_j \in Y$. La distribución de probabilidad de Y viene dada por la distribución marginal $p_Y(y_j) = \sum_i p_{Y,X}(y_j, x_i) := \sum_i p_{Y|X}(y_j|x_i)\,p_X(x_i)$. Una medida de la habilidad

mente (teorema de Shannon-McMillan); así, para el inglés, si $H_{\text{inglés}} \approx 1.2$, un texto en inglés comprensible de n símbolos es codificable mediante $1.2n$ bits, y por tanto mediante $(H_{\text{inglés}}/\log_2 27)n = 0.25n$ símbolos. La redundancia teórica del inglés es, por tanto, $\approx 3/4$. Esto no significa que podamos quitar al azar un 75% de los símbolos manteniendo la comprensibilidad del mensaje. Depende mucho de cómo se simplifique el texto. La redundancia práctica se estima en un 25-50%.

[35] Se demuestra que para toda fuente F existe alguna codificación Huffman con la que, al codificar grandes bloques, se puede acercar uno por arriba, tanto como se desee, a la barrera $H(F)$ por símbolo. Esta barrera es infranqueable con códigos de descodificación única.

del canal para transmitir información viene dada por su *capacidad* $C := \sup_{p_X} I(X : Y) = \max_{p_X} I(X : Y)$, donde $I(X : Y) := H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X, Y)$ es la *información mutua* de X e Y o información que de X (Y) se tiene por el hecho de conocerse Y (X). En esta expresión aparece la entropía condicional $H(X|Y) := \sum_j p_Y(y_j) \sum_i p(y_j|x_i) \log_2 p(y_j|x_i), \quad p_{Y,X}(y_j, x_i) =: p(x_i) p(y_j|x_i)$, que mide la incertidumbre sobre X conocida Y, y la entropía conjunta $H(X, Y)$ de X, Y $H(X, Y) := -\sum_{j,i} p_{Y,X}(y_j, x_i) \log_2 p_{Y,X}(y_j, x_i)$, o incertidumbre sobre el par X, Y. La convexidad de la función log hace que $I(X : Y) \geq 0$ (conocer Y no puede nunca rebajar la información sobre X). Es claro que $I(X : Y) = I(Y : X)$.

La capacidad C viene a ser el número de bits de salida correctamente transmitidos por cada símbolo de entrada. Su cálculo es por lo general muy difícil.

Muchos canales son simétricos binarios: cada bit transmitido tiene la misma probabilidad p de sufrir inversión, es decir, de ser erróneo a la llegada. Son los canales que consideraremos aquí. Para ellos es elemental el cálculo de la información mutua máxima, con el resultado $C = 1 - H(p) =: C(p)$, donde $H(p) := -p \log_2 p - (1 - p) \log_2 (1 - p)$. Obsérvese que $C(\frac{1}{2}) = 0$; tal canal, de capacidad nula, es inservible como conducto de transmisión, pues transforma cualquier secuencia binaria en otra totalmente aleatoria. Supondremos siempre en lo que sigue que $C(p) < \frac{1}{2}$.

Un procedimiento general de uso de un canal de transmisión ruidoso puede ser este: Una fuente emite palabras m de un cierto alfabeto, que un codificador inyecta en un subconjunto $\mathcal{C}_n \subset \mathbb{Z}_2^n$. Los elementos de este conjunto se llaman palabras código. En la transmisión de una palabra código $w \in \mathcal{C}_n$ puede producirse un error $e \in \{0, 1\}^n$ de modo que la palabra recibida sea $w' = w + e$ (suma mod 2). El subconjunto de palabras $\mathcal{C}_n \subset \{0, 1\}^n$ se dice que es un *código clásico corrector de errores* (CCCE) $e \in \mathcal{E}_n \subset \{0, 1\}^n$ si $(w + \mathcal{E}_n) \cap (w' + \mathcal{E}_n) = \emptyset$ para cualesquiera $w \neq w' \in \mathcal{C}_n$. Es decir, a pesar de la distorsión que en una palabra código $w \in \mathcal{C}_n$ producen los errores, no hay solapamiento de los diferentes conjuntos $w + \mathcal{E}_n$, y la descodificación es posible sin ambigüedades mediante simple asignación de la palabra código que representa la clase $w + \mathcal{E}_n$ en que se encuentra la palabra recibida.

Este es por tanto el procedimiento: 1/ Previamente se acuerda entre la persona emisora y la receptora qué mensaje específico corresponde a cada palabra código, y cómo, a la recepción con errores de ésta, se va a decidir qué palabra código se le asigna; 2/ se envía ésta en lugar del mensaje; 3/ éste se recupera al otro extremo del canal tras asignar a la palabra recibida (que posiblemente presenta errores) una palabra código de acuerdo con el esquema de decisión adoptado en 1/; y 4/ el destinatario recibe el mensaje correspondiente a esta palabra código, mensaje que debería coincidir con el original si el esquema de decisión es acertado.

En el uso práctico de un código $\mathcal{C}_n$ pueden producirse equivocaciones en la recuperación de los mensajes, provocados por errores fuera de $\mathcal{E}_n$, esto es, del ámbito de seguridad del código. Pero mientras la frecuencia de fracasos sea muy baja será tolerable el riesgo. Es claro que convendrá para ello distanciar mucho entre sí (en sentido Hamming, es decir, en el número de bits en los que difieren) las distintas palabras código, pues así disminuirá la posibilidad de que los errores produzcan colisiones de dos palabras código distintas. Pero esto conllevará una disminución del número de palabras código, a no ser que aumentemos n, con la consiguiente ralentización en la transmisión de información esencial. Enseguida volveremos a este asunto.

Se llama *ritmo* del código $\mathcal{C}_n$ a $R := \log_2 |\mathcal{C}_n| / n$. Mide el número de bits informativos por bit transmitido. Es fácil argumentar que para que el código sea fiable su ritmo

no ha de superar la capacidad del canal: $R \leq C(p)$.[36]

El segundo teorema de Shannon cierra la cuestión en el límite asintótico, afirmando, para canales simétricos binarios, que si R es cualquier ritmo de transmisión del código que no sobrepase la capacidad del canal ($0 < R < C$), dado un $\varepsilon > 0$ arbitrariamente pequeño existen códigos $\{\mathcal{C}_n \subset Z_2^n\}_1^\infty$ con $\lceil 2^{nR} \rceil$ elementos (palabras código) y sistemas de descodificación asociados, y un entero $n(\varepsilon)$, tales que la *fidelidad* $F(\mathcal{C}_n)$ o probabilidad de que cualquier mensaje descodificado coincida con su original es $\geq 1-\varepsilon$ (esto es, la probabilidad máxima de error en la identificación de la palabra código a su recepción es $\leq \varepsilon$) para todo $n \geq n(\varepsilon)$. Más aún, se puede conseguir que las probabilidades de error tiendan a 0 exponencialmente en n (Shannon, 1957).

El teorema es óptimo: no puede sobrepasarse la capacidad C si se quiere una transmisión fiel. Se sabe en efecto que para toda sucesión de códigos $\{\mathcal{C}_n\}_1^\infty$ con $|\mathcal{C}_n| = \lceil 2^{nR} \rceil$, cuyo ritmo supera la capacidad del canal ($R > C$) la probabilidad media de error tiende asintóticamente a 1.

La demostración de este teorema de Shannon es sumamente original, pues se apoya en códigos escogidos al azar, y esquemas de decisión basados en el principio de máxima verosimilitud, o equivalentemente para estos canales simétricos binarios, mínima distancia Hamming; por desgracia, no es constructiva, sino existencial, dejando abierto el problema práctico de hallar códigos que se acerquen al máximo de eficiencia y sean de fácil descodificación.

2.3 Corrección clásica de errores

Los errores en el almacenamiento y procesado de la información son inevitables. Una forma de corregirlos clásicamente es echando mano de la *redundancia* (códigos de repetición): se sustituye cada bit por una ristra de $n \geq 3$ bits iguales a él,

$$0 \mapsto \underbrace{00\ldots00}_{n\ 0's}, \quad 1 \mapsto \underbrace{11\ldots11}_{n\ 1's},$$

y si por la causa que sea se produce un error de modo que uno de los bits en una de esas ristras se invierte (por ejemplo $00000 \mapsto 01000$), basta con invocar el voto de la mayoría para corregir el error.[37]

Es claro que si se repasan sistemática y frecuentemente las n-plas de bits, de modo que sea muy poco probable que los errores afecten a dos o más bits, la aplicación de este sencillo método las limpiará de sus errores y las restablecerá a su estado debido. Ahora bien, el precio a pagar quizás resulte demasiado elevado, pues con códigos de longitud n suficientemente grande como para asegurar un pequeño error en la detección, el ritmo de transmisión, que en este caso es de $1/n$ bits fuente por bit canal, puede ser prohibitivamente pequeño.

Antes hablamos de códigos $\mathcal{C} \subset \{0,1\}^n$ correctores de errores ubicados en $\mathcal{E} \subset \{0,1\}^n$. Más generalmente, podemos considerar alfabetos q-arios (cuyos símbolos su-

[36] En efecto, al transmitir una palabra código $w \in \mathcal{C}_n$, se producirá una media de np bits invertidos, y por ello un error e que muy probablemente será alguna de las $2^{nH(p)}$ secuencias típicas. Para que la descodificación sea fidedigna, las esferas de error con centros en las palabras código no habrán de solapar, y por tanto $2^{nH(p)}|\mathcal{C}_n| \leq 2^n$, de donde $R \leq C(p)$. Este resultado sugiere que la capacidad C es cota superior a todos los ritmos de transmisión fiel.

[37] Sea p la probabilidad de que un bit cualquiera se estropee. En general, pueden invertirse varios de los bits de la n-pla. Si $p < 1/2$, la probabilidad de error en la decisión, es decir, de que la decisión mayoritaria falle, puede hacerse tan pequeña como se desee tomando n suficientemente grande. El caso $p > 1/2$ se resolvería haciendo lo contrario del voto de la mayoría, y si $p = 1/2$, no hay nada a hacer, pues las ristras pasan a ser aleatorias.

pondremos que son los elementos del cuerpo finito $\mathbb{F}_q$ de $q = p^f$ elementos, con p primo). Dadas dos palabras $x, y \in \{0, 1, \ldots, q-1\}^n$, sea $d_{\mathrm{H}}(x, y) := |\{i | 1 \leq i \leq n, x_i \neq y_i\}|$ su distancia Hamming (número de lugares en que x, y difieren). Sea la distancia mínima $d := d_{\mathrm{H}}(\mathcal{C}) := \inf_{x \neq y \in \mathcal{C}} d_{\mathrm{H}}(x, y)$ del código. Entonces el código $\mathcal{C}$ permite corregir errores que afecten como máximo hasta $t := \lfloor \frac{1}{2}(d-1) \rfloor$ posiciones o símbolos inclusive: basta sustituir cada palabra recibida por la palabra código más cercana en la métrica de Hamming.[38] Convienen por tanto los códigos con d alta, pero esto se consigue a expensas de disminuir $|\mathcal{C}|$. Si M es el número de palabras código, hablaremos del código $(n, M, d)_q$. Su *ritmo* se define como $R := n^{-1} \log_q M$. El máximo valor $A_q(n, d)$ de M, es decir, del número de palabras código para valores dados de q, n, d, no se conoce en general,[39] pero se dispone de alguna cota superior (de Singleton, y de Hamming o de empaquetamiento de esferas) e inferior (de Gilbert-Varshamov) [145, 181, 211].[40]

2.3.1 Códigos lineales

Cuando $\mathcal{C}$ es un subespacio lineal de $\mathbb{F}_q^n$, el código dícese *lineal*; son los códigos lineales por tanto de la forma $(n, q^k, d)_q$, donde k es la dimensión del subespacio lineal $\mathcal{C}$, d coincide con la longitud mínima de una palabra código no nula, y tienen la gran ventaja práctica de simplificar la búsqueda de la palabra código más cercana a cada palabra recibida. Acostumbran a representarse por $[n, k, d]_q$, o simplemente por $[n, k]_q$ cuando d es irrelevante. Su ritmo es k/n.

Dado un código $\mathcal{C}$ de tipo $[n, k]_q$, una matriz G, $k \times n$, de filas dadas por las componentes de una base de $\mathcal{C}$, se llama *matriz generadora* de $\mathcal{C}$. Definiendo en $\mathbb{F}_q^n$ el producto escalar en la forma canónica, podemos introducir el código *dual* $\mathcal{C}^\perp$ del código $\mathcal{C}$. Una matriz H, $(n-k) \times n$, generadora de $\mathcal{C}^\perp$ se conoce como *matriz (de comprobación de) paridad* de $\mathcal{C}$; nótese que $\mathcal{C} = \{u \in \mathbb{F}_q^n : Hu^{\mathrm{t}} = 0\}$, lo que justifica parte del nombre dado a H, pues permite "comprobar" fácilmente si un vector u de $\mathbb{F}_q^n$ pertenece o no al subespacio $\mathcal{C}$ viendo si sus componentes satisfacen o no cada una de las $(n-k)$ relaciones lineales impuestas por H.

Tras permutación adecuada de los símbolos en cada palabra código (lo que proporciona un código equivalente a $\mathcal{C}$), siempre puede escogerse G de forma estándar, con $G_{ij} = \delta_{ij}, i, j \leq k$, esto es, $G = (I_k | A)$, donde A es una matriz cuadrada de dimensión $n-k$. Es fácil ver que si $G = (I_k | A)$ está en forma estándar, entonces $H = (-A^{\mathrm{t}} | I_{n-k})$ es una matriz paridad de $\mathcal{C}$, también en forma estándar como matriz paridad (aunque no como matriz generadora del código dual $\mathcal{C}^\perp$). Se dice entonces que el código es sistemático; sus k primeros símbolos se llaman símbolos o dígitos de información o mensaje, y los restantes se llaman símbolos o dígitos de comprobación o paridad.

Es clara la cota de Singleton: $k + d \leq n + 1$. Los códigos que la saturan se llaman códigos *separables en distancia máxima* o códigos MDS. Es mucho más complicado hallar cotas inferiores para d, y sólo se sabe hacer para algunas clases de códigos.

La codificación aplica biyectiva y linealmente las palabras de $\mathbb{F}_q^k$ sobre las palabras de $\mathbb{F}_q^n$ a través de un código $(n, q^k, d)_q$, y se realiza de este modo. Sea $\{e_1, \ldots, e_k\} \subset \mathbb{F}_q^n$ una base de $\mathcal{C}$. Dada una palabra fuente $f = (f_1, \ldots, f_k) \in \mathbb{F}_q^k$, se le asigna la palabra código $w(f) := \sum_i f_i e_i$. En términos de la matriz generadora G, $f \mapsto w(f) := fG$.

[38] Por ejemplo, para el código de repetición $\mathcal{C} = \{0 \ldots 0, 1 \ldots 1, \ldots, (q-1) \ldots (q-1)\}$, con q palabras código de longitud n, se tiene $d = n$, y por tanto corrige exactamente $\lfloor (n-1)/2 \rfloor$ errores.

[39] Se sabe, por ejemplo, que $A_q(n, 1) = q^n, A_q(n, n) = q, A_2(3, 2) = 4, A_2(5, 3) = 4, A_2(5, 5) = 2$; se ignora, sin embargo, el valor exacto en muchos otros casos.

[40] La determinación de $A_q(n, d)$ se conoce como problema fundamental de la teoría de codificación.

Llamemos π a esta biyección. En la transmisión, $w(f)$ puede corromperse, pasando a ser $u := w(f) + e$, donde $e \in \mathcal{E}$ es un posible vector error. Evidentemente, $e \in u + \mathcal{C}$.

Para descodificar se aplica el criterio de mínima distancia (Hamming), reemplazando u por $\pi^{-1}(u - u_0)$, donde u_0 es un elemento de $u + \mathcal{C}$ que minimiza la distancia al origen (tal u_0, no necesariamente único, se conoce como *líder* del conjunto trasladado $u + \mathcal{C}$). La linealidad del código permite aligerar estos trámites. Primero se construye una colección completa $\{z_0 = 0, z_1, \ldots, z_{q^{n-k}-1}\}$ de líderes en correspondencia con las distintas clases de $\mathbb{F}_q^k / \mathcal{C}$, y se calculan sus llamados *síndromes* $\{s_0 = 0, s_1, \ldots, s_{q^{n-k}-1}\}$, definidos como $s_j := z_j H^{\mathrm{t}}$. Cuando recibamos una palabra u, calcularemos su síndrome $s(u) := uH^{\mathrm{t}}$, que forzosamente debe coincidir con uno, y uno sólo, de los s_j, digamos $s(u) = s_{i_0}$. Basta entonces descodificar como $\pi^{-1}(u - z_{i_0})$ [145, 181, 211].

La descodificación anterior recupera el mensaje fielmente si y sólo si el error cometido por el canal es uno de los líderes escogidos.

2.3.1.1 Ejemplos de códigos lineales 1. El código de repetición $\mathcal{C} = \{0 \ldots 0, 1 \ldots 1, \ldots, (q-1) \ldots (q-1)\}$ es del tipo $[n, 1, n]_q$, y aunque para él la distancia mínima es óptima, el ritmo es pésimo.

2. Los códigos de Hamming $\mathrm{H}_q(r)$ son quizás los más famosos de todos [145, 181, 211].[41] Son códigos del tipo $[n = 1 + q + \ldots + q^{r-1}, k = n - r, d = 3]_q$, y son *perfectos*, en el sentido de que el conjunto de las esferas de radio $\lfloor (d-1)/2 \rfloor$, centradas en las palabras código, cubren $\mathbb{F}_q^n$. Para estos códigos el ritmo $R = 1 - r/n$ tiende a 1 para $n \to \infty$, pero sólo corrigen un error.

3. Los códigos de Golay (Golay 1949) G_{24} y G_{23} son binarios, del tipo $[24, 12, 8]_2$, y $[23, 12, 7]_2$, respectivamente [145, 181, 211]. Son posiblemente los códigos más importantes, por la riqueza de su estructura combinatoria y algebraica. El código G_{24} es *autodual*, en el sentido de que su subespacio $\mathcal{C}$ coincide con su ortogonal: $\mathcal{C} = \mathcal{C}^{\perp}$. De tipo $(24, 4096, 8)_2$, ritmo $R = 1/2$, y capaz de corregir hasta 3 errores y de detectar hasta 4 de ellos, fue utilizado por la NASA para la transmisión en 1979-82 desde los Voyagers de las imágenes en color de Júpiter y Saturno.

La descodificación de G_{24} no es complicada aprovechando su autodualidad.

El código G_{23} es perfecto y se obtiene del G_{24} "pinchándolo" en (es decir, eliminando) su última coordenada (lo que equivale a decir que G_{24} se obtiene de G_{23} añadiéndole un bit de paridad, pues la suma de los elementos de cualquier fila de G es par).

Los códigos de Golay G_{12} y G_{11} son ternarios, del tipo $[12, 6, 6]_3$, y $[11, 6, 5]_3$, respectivamente. Como antes, G_{12} es autodual, y G_{11} es perfecto y obtenible del G_{12} suprimiendo la última coordenada (G_{12} se obtiene de G_{11} añadiéndole un bit de paridad).[42]

Los códigos G_{24} y G_{12} tienen peculiares propiedades combinatorias; sus grupos de automorfismos son M_{24} y $2.\mathrm{M}_{12}$, donde M_{24} y M_{12} son los famosos grupos esporádicos de Mathieu. Este último grupo es el subgrupo de S_{12} generado por las permutaciones especiales o barajaduras de 12 naipes numerados del 0 al 11: $0, 1, 2, \ldots, 11 \mapsto 11, 10, 9, \ldots, 0$ y $0, 1, 2, \ldots, 11 \mapsto 0, 2, 4, 6, 8, 10, 11, 9, 7, 5, 3, 1$. También es el grupo de movimientos de la forma $\tau_i \tau_j^{-1}$ de un icosaedro "Rubick", donde τ_i indica el giro de ángulo $2\pi/5$ alrededor del vértice i-ésimo del icosaedro [62]. Precisamente, el descubrimiento de los códigos de Golay impulsó el estudio de los grupos esporádicos que

[41] Fueron descubiertos por Marcel Golay en 1949 y por Richard Hamming en 1950.

[42] Los códigos Hamming, y los Golay G_{23}, G_{11}, son, salvo equivalencia, los únicos códigos (lineales) perfectos no triviales.

desembocaría en la clasificación completa de los grupos simples finitos con el hallazgo por Griess en 1983 del grupo "monstruo" o "gigante amistoso", finito y simple, un enorme subgrupo de $\mathrm{SO}(47\times 59\times 71)$ con unos 10^{54} elementos.

4. Los códigos binarios de Reed-Muller $\mathrm{RM}(r,m)$, con $0\le r\le m$, son del tipo $[n=2^m, k=\sum_{k\le r}\binom{m}{k}, d=2^{m-r}]_2$ [145, 181]. Su ritmo, para r fijo, tiende a 0 al crecer m. Figuran entre los códigos más antiguos conocidos. El subespacio $\mathcal{C}\subset\mathbb{F}_2^n$ del código se define como el conjunto de valores de los polinomios booleanos de grado $\le r$ en m variables. Su descodificación es sencilla.

El código $\mathrm{RM}(1,5)$, de tipo $(32,64,16)_2$, capaz de corregir hasta 7 errores, y de ritmo $R=3/16$, se usó en 1969-72 para transmitir desde los Mariners 6, 7 y 9 las fotos en blanco y negro de Marte. Estas fotos se parcelaban en 700×832 elementos, y a cada uno se le asignaba un nivel de gris entre 0 y 63 (6 bits de mensaje), que se completaban con otros 26 bits de paridad. El ritmo de envío fue de 16200 bit/s.

5. Los códigos RS (Reed, Solomon) y BCH (Bose, Ray-Chaudhuri, Hocquenghem) generalizan los de Hamming [145, 181].

Los códigos RS han sido muy utilizados por la NASA, para transmisión de información en las misiones Galileo, Magellan y Ulysses al espacio profundo, y en la actualizad se usan por doquiera, desde los lectores de CD's hasta los discos duros de los ordenadores.

6. Los códigos geométricos de Goppa $\mathrm{G}_q(D,G)$, interesante generalización de los RS, han permitido obtener familias de códigos *asintóticamente buenas*, esto es, familias que contienen sucesiones infinitas de códigos $[n_i,k_i,d_i]_q$, con $n_i\to\infty$, tales que las sucesiones $\{k_i/n_i, d_i/n_i\}$ de ritmos y distancias mínimas relativas están inferiormente acotadas por sendos números positivos [145, 181, 200, 36].

2.3.1.2 Algunas cotas asintóticas para códigos lineales Para codificar bien, interesan códigos largos para que permitan el envío de muchos mensajes distintos y sea grande su distancia mínima y por ende el número de errores que permite corregir. Dado $\mathcal{C}=[n,k,d]_q$, sea $R(\mathcal{C}):=k/n$ su ritmo y $\delta(\mathcal{C}):=d/n$ su distancia mínima relativa. Un teorema de Manin asegura que el conjunto de puntos límite de $\{(\delta(\mathcal{C}),R(\mathcal{C}))\in[0,1]^2 : \mathcal{C}$ es un código sobre $\mathbb{F}_q\}$ es de la forma $\{(\delta,R)\in[0,1]^2 : \delta\in[0,1], 0\le R\le\alpha_q(\delta)\}$, donde $\alpha_q(\delta)$ es una función continua de $\delta\in[0,1]$, decreciente en $[0,1-q^{-1}]$, y tal que $\alpha_q(0)=1$, $\alpha_q(\delta)=0$ si $1-q^{-1}\le\delta\le 1$ [200].

Sea H_q la función entropía q-aria $H_q(x\in[0,1-q^{-1}]):=x\log_q(q-1)-x\log_q x-(1-x)\log_q(1-x)$. Se conocen cotas para la función $\alpha_q(\delta)$ en el intervalo de interés $\delta\in[0,1-q^{-1}]$ [181, 200, 36], destacando la cota inferior de Gilbert-Varshamov $\alpha_q(\delta)\ge 1-H_q(\delta)$, que asegura la existencia de códigos tan largos como se desee con distancia mínima relativa δ y ritmo R asintóticamente positivos.

2.4 El ordenador clásico: máquinas de Turing

Porque es impropio de los grandes hombres perder horas como esclavos haciendo cálculos que, si se utilizasen máquinas, podrían tranquilamente relegarse a otros. LEIBNIZ

Recuerdo aún el suplicio que me representaba en mis años mozos el trabajar con la regla de cálculo (analógico) para hacer operaciones algo complejas con una mínima precisión. Mayor estima tengo por mi primera calculadora digital; no fue un ábaco, sino una preciosa CURTA fabricada en Liechenstein, que conservo como una reliquia. Su cuidada mecánica permite realizar las cuatro operaciones aritméticas con sencillez; para las raíces cuadradas o cúbicas ya hay que aplicar ciertos algoritmos que consumen

más tiempo y paciencia.[43] Hoy cualquier estudiante maneja calculadoras digitales de bolsillo que en fracciones de segundo le permiten evaluar con precisión suficiente funciones elementales y realizar cálculos aritméticos. Más aún, abundan los ordenadores personales, programables, que pueden realizar tareas más complejas y en mucho menos tiempo que los grandes ordenadores de hace unos años, a los que además superan ampliamente en memoria.

A Charles Babbage (1791-1871) se debe el desarrollo conceptual de la primera calculadora automática digital de uso general, conocida como *Analytical Engine* (1834) [63].[44] Presentó su proyecto en 1840 ante un auditorio de matemáticos e ingenieros en Turín. No pudo verlo realizado, y sus propuestas cayeron en un largo olvido. Un siglo y medio después (1991) se produjo un prototipo en el Reino Unido, *Analytical Engine no. 2*, siguiendo el proyecto de Babbage (una vez redescubiertas sus notas en 1937), que realiza cálculos con precisión de hasta 31 dígitos significativos. Hace las cuatro operaciones aritméticas, implementa la lógica condicional (*if* ... *then* ...), y es muy versátil.[45] Tiene los tres soportes de los ordenadores actuales: el "almacén" o memoria, el "molino" o CPU, y un dispositivo de lectura de datos a través de tarjetas perforadas, como las ideadas en 1804 por Joseph-Marie Jacquard para su uso en los telares.

Vehemente defensora y propagandista de las ideas de Babbage fue la matemática inglesa Augusta Ada King, condesa de Lovelace, hija del gran poeta Lord Byron [121]. Es considerada por muchos como el primer programador de la historia (en su honor, un lenguaje de programación, ADA, lleva su nombre), con su célebre programa para calcular los números de Bernoulli, que aparece en unas notas de su único trabajo sobre la máquina analítica de Babbage.[46] Pero ya Babbage había escrito algunos programas cortos, mucho más simples.

Genéricamente, un ordenador es un dispositivo físico que transforma o procesa información de acuerdo con ciertas reglas. Las máquinas de Alan Mathison Turing constituyen una brillante y poderosa formalización de este concepto.

Se entiende por *computador* clásico una *máquina de Turing* [205],[47] a saber, una terna $T = (Q, A, \delta)$ formada por [216, 185, 95, 211, 137, 4, 167]:

- Un conjunto finito Q de estados internos o estados "mentales" [205] de la unidad de control de la máquina, con varios estados especiales: q_{in}, estado inicial o de arranque, y F, colección de estados finales.

[43] Entendemos por *algoritmo* una sucesión finita de instrucciones concretas a seguir sin ambigüedad alguna, y que necesariamente termina tras la ejecución de un número finito de ellas. Pensemos en un programa de ordenador escrito en el lenguaje que más nos guste. El nombre de algoritmo (y también el de guarismo) proviene del nombre del matemático persa Abu Ja'far Muhammad ibn Musa al-Khwarizmi (*ca*. 780-850), autor del célebre libro HISAB AL-JABR W'AL-MUQABALA, titulo del que emana la palabra *álgebra*. Según Knuth [127], *algorithms are the life-blood of computer science*; y también afirma que *actually a person does not* really *understand something until after teaching it to a* computer, *i.e., expressing it as an algorithm*.

[44] Una máquina suya anterior, construida en 1822, y conocida como *Differential Engine*, era de uso muy limitado; sólo servía para hacer tablas matemáticas, mediante el método de diferencias finitas.

[45] Según Babbage, *it could do everything but compose country dances*. Esta excepción ya no rige para los modernos ordenadores.

[46] *We may say most aptly that the Analytical Engine weaves* algebraic patterns, *just as the Jacquard-loom weaves flowers and leaves.* (Ada).

[47] La genial idea de estas máquinas, que bulle en las tripas de cualquier computador actual, se le ocurrió a Turing un caluroso día de verano en 1935. Las palabras *Turing machine* aparecieron por vez primera en un trabajo de puesta a punto de Alonzo Church [55], otra gran figura del campo de la lógica matemática, que obtuvo simultánea e independientemente de Turing una prueba de la indecibilidad del *Entscheidungsproblem* de Hilbert.

- Un *alfabeto* finito A de símbolos, entre los que está el símbolo "blanco" $\sqcup$. Pensemos en una *cinta* lineal (potencialmente infinita en ambos sentidos) con celdas, en cada una de las cuales está representado alguno de los símbolos en $A-\{\sqcup\}$, o bien está vacía (símbolo $\sqcup$).

- Una función de transición o *regla* $\delta : Q \times A \to Q \times A \times M$, con $M := \{\leftarrow, \rightarrow\}$. Una *cabeza*, cursor (puntero de acceso) de lectura/escritura lee una celda de la cinta, hallando el simbolo $a \in A$; si en ese momento la máquina está en estado $q \in Q$, y $\delta(q,a) = \{q', a', m\}$, entonces la cabeza cambia a por a', luego se desplaza a la celda contigua por la izquierda (si $m = \leftarrow$), o por la derecha (si $m = \rightarrow$), y a continuación el estado interno pasa a ser q'.

El tiempo se supone discretizado en pasos 0, 1, 2, ... Al empezar (tiempo 0), la máquina se halla en el estado especial q_{in} y la cabeza se posa en la celda más a la izquierda donde comienza un dato de entrada (o dato inicial, o simplemente entrada, o dato), consistente en una palabra (finita) x sin blancos, es decir, $x \in (A-\{\sqcup\})^*$. A partir de este instante la máquina sigue sus propias instrucciones paso a paso. Si en algún momento la máquina T llega a un estado interno especial $q_{\text{fin}} \in F$ (se dice entonces que $T(x)$ converge), la máquina se detiene, y como resultado o *salida* $T(x)$ se toma $T(x) = 0$ si esa celda c_{fin} en que está el cursor de lectura en ese momento de parada está vacía, o bien la palabra $y \in (A-\{\sqcup\})^*$ más larga, necesariamente flanqueada por sendos símbolos $\sqcup$, que se encuentra en la cinta y de la que forma parte el símbolo en c_{fin}. Puede muy bien ocurrir que para algún dato de entrada determinado la máquina no se detenga nunca. Escribiremos entonces $T(x)\uparrow$, y diremos que $T(x)$ diverge; si la máquina se detiene, se dice que $T(x)$ converge, lo que denotamos por $T(x)\downarrow$.

Llamemos configuración o descripción instantánea de T a la secuencia aqb, donde q es el estado de la unidad de control, $a \in A^*$ la palabra formada por los símbolos que hay a la izquierda de la posición del cursor, y $b \in A^*$ la palabra formada por todos los símbolos en la cinta tanto debajo del cursor como a su derecha. Suponemos que a la izquierda de a y a la derecha de b la cinta está vacía. Por ejemplo, sea la configuración inicial $q_{\text{in}}010$, correspondiente a la entrada binaria $x = 010$. Si tras unas cuantas operaciones o pasos de tiempo se llega a $1011 \sqcup 01 q_{\text{fin}} 0010 \sqcup 11$, la máquina se detendrá en ese instante y como resultado del quedará cálculo $y = T(x) = 010010$.

Las máquinas de Turing $T = (A, Q, \delta)$ pueden "contarse" o "enumerarse". Para ello lo primero que se hace es suponer, sin pérdida de generalidad, que todos los símbolos de sus alfabetos, de sus estados internos y del par de movimientos del cursor se extraen de un mismo alfabeto numerable. A cada uno de esos símbolos s se el asocia biyectivamente una palabra binaria $e(s)$, de longitud $l = \lceil \log_2(|Q| + |A| + 2) \rceil$. La aplicación $\delta : (q,a) \mapsto \{q', a', m\}$ queda fijada dando todas y cada una de las 5-plas (q, a, q', a', m). Si la totalidad de estas 5-plas para una máquina T es $(q_1, a_1, q_1', a_1', m_1), (q_2, a_2, q_2', a_2', m_2), \ldots, (q_n, a_n, q_n', a_n', m_n)$, representaremos la máquina en cuestión por la palabra binaria autolimitante $E(T) := \overline{ln}e(q_1)e(a_1)\ldots e(a_n)e(m_n)$.[48] Ordenamos luego lexicográficamente los códigos $E(T)$, asignándole a T el *índice* o número de Gödel $n(T) = i$, donde i es el número de posición de $E(T)$ en dicha ordenación. La colección de todas las máquinas de Turing es así $\{T_1, T_2, \ldots, T_n, \ldots\}$.

Las máquinas de Turing hasta ahora consideradas son *deterministas* (MTDs): para cada par q, a la acción subsiguiente $\delta(q,a)$ es única. Cuando no es así, y caben varias alternativas de acción o reglas de transición en cada paso, es decir, cuando $\delta : Q \times A \to$

[48] Recordemos que $\overline{x} := 1^{\ell(x)}0x$, donde $\ell(x)$ es la longitud binaria de x, 1^n indica la cadena $1\ldots1$ de n 1's, y xy representa la concatenación de las cadenas x, y.

$2^{Q\times A\times M}$,[49] se dice que la máquina de Turing es *no determinista* (MTND). Su acción está ramificada en todos los caminos que abre el abanico de opciones en cada paso. Entre las MTNDs destacan las máquinas de Turing probabilistas (MTPs); son aquellas con posibilidad de doble elección en sus reglas de transición, elección que se realiza tirando una moneda no trucada al aire.

Podrá quizás parecernos tosca o primitiva una máquina de Turing. Pero no nos engañemos. Para cualquier cálculo factible por los ordenadores más sofisticados existe alguna máquina de Turing capaz de realizarlo. Es tan poderoso este concepto de máquina de Turing, que se ha convertido en el árbitro de la computabilidad.

2.4.1 Los primeros ordenadores

Hay que remontarse al siglo XVII para encontrar los primeros dispositivos mecánicos de cálculo analógico y digital. De tipo analógico fue un calculador logarítmico, antecesor de las reglas de cálculo, desarrollado por el matemático inglés Edmund Gunter en 1620. De tipo digital es la máquina de Blaise Pascal (1623-1662), el famoso matemático, físico y pensador francés. Construida en 1642, realizaba sumas y restas de números de hasta 8 dígitos.[50] El célebre matemático alemán Gottfried Wilhelm Leibniz mejoró ostensiblemente la máquina de Pascal. El calculador de Leibniz, concluido en 1673, realizaba las cuatro operaciones aritméticas y además extraía raíces cuadradas.

En 1820 aparecieron las primeras calculadoras comerciales, llamadas *aritmómetros*, ideadas por el francés Charles Xavier Thomas de Colmar.

Con el fin de acelerar el escrutinio del censo de EEUU, el estadístico americano Herman Hollerith inventó en 1880 una máquina lectora de tarjetas perforadas. Fundó en 1896 la Tabulating Machine Company, que luego se convertiría en 1924 en la International Business Machines Corporation (IBM). El sistema de lectura y de perforación de Hollerith fue incorporado a las unidades de entrada/salida de los ordenadores hasta su destierro y sustitución a finales de los 70 por los terminales de pantalla.

Ya hemos citado a la máquina analítica de Babbage como el primer calculador de uso general.

Entre 1939 y 1942, la primera calculadora con válvulas electrónicas o tubos de vacío fue diseñada y construida por el físico teórico John Vincent Atanasoff en la Universidad de Iowa, con su estudiante Clifford E. Berry [63]. Conocida como ABC (Atanasoff-Berry Computer), estaba pensada para resolver exclusivamente sistemas de hasta 30 ecuaciones lineales con 30 incógnitas. Contenía 300 tubos de vacío como puertas lógicas para el control y cálculo, realizaba aritmética binaria, usaba condensadores para memoria almacén, y tarjetas perforadas para entrada/salida. Tenía una precisión en sus cálculos que superaba en tres órdenes de magnitud a las calculadoras de su época.

En 1941 el ingeniero alemán Konrad Zuse, con total independencia, construyó el primer ordenador, llamado Z3, controlado por un programa.

A finales de 1943 la calculadora COLOSSUS, de uso específico, entraba en funcionamiento, con 1500 tubos de vacío, en el centro de investigación británico de Bletchley Park. Su objetivo era descifrar los mensajes secretos alemanes generados por la máquina ENIGMA y el *Geheimschreiber* durante la Segunda Guerra Mundial. El propio Turing, y su maestro Mark Newman, participaron en el proyecto.

[49] Se indica por 2^X el conjunto de todos los subconjuntos de X. Otra forma equivalente de introducir una MTND es cambiando la función δ de una MTD por una relación $\Delta \subset (Q\times A)\times(2^{Q\times A\times M})$.

[50] El alemán Wilhelm Schickard, amigo de Johannes Kepler, se adelantó a Pascal, construyendo en 1623-1624 una calculadora mecánica. Desgraciadamente, no se ha conservado información sobre la misma.

En 1944 entró en operación en la Universidad de Harvard el *Automatic Sequence Controlled Calculator* MARK I, diseñado por el matemático americano Howard Hathaway Aiken para realización de cálculos científicos, y construido por IBM a base de relés eléctricos. De 15 m de largo y 2.4 de alto, con 800 km de cables, 3 millones de conexiones, y un peso de 35 t, este ordenador se programaba con una cinta perforada que contenía las instrucciones y datos. Lo usó la US Navy para cálculos de artillería y balística. En 1947 entró en operación el MARK II.

En 1946 se concluyó el ENIAC (*Electronic Numerical Integrator and Computer*) en la Escuela Moore de Ingeniería Eléctrica de la Universidad de Pennsylvania. Ha sido el primer ordenador digital electrónico de uso general y a gran escala, creado por J. Mauchly y J. Presper Ecker Jr., entre otros. De 24 m de largo, 2.5 de alto, y 18,000 válvulas, era capaz de realizar 5000 sumas/segundo, velocidad que hoy puede parecernos ridícula pero que era entonces mil veces más rápida que todos los demás. Había muchas dudas de que el monstruoso ENIAC funcionase, cuando lo normal era esperar que cada varios segundos se fundiese una válvula. La elección de componentes de primera calidad, y el uso de la máquina a potencia media, hizo que las previsiones bajaran a dos o tres fallos por semana. Arrastrado por el matemático Herman Golsdtine, al proyecto ENIAC estuvo también vinculado János Lájos von Neumann, quien en 1945, y posiblemente inspirado en ideas de Mauchly y Eckert sobre el sucesor EDVAC (*Electronic Discrete Variable Automatic Computer*) del ENIAC, escribió el polémico informe *First draft on the report on the EDVAC*, en el que proponía guardar en binario los programas de funcionamiento en la memoria interna del ordenador, de modo que sus instrucciones fuesen modificables sobre la marcha, con el consiguiente aumento de flexibilidad y potencia de cálculo de los ordenadores. Esta concepción organizativa y dinámica de los ordenadores se conoce como arquitectura von Neumann.[51]

Desde el Institute for Advanced Studies en Princeton, von Neumann, en colaboración con Goldstine, desarrolló un tipo de ordenadores con programa almacenado, llamados *johnniacs* en su honor, en los que se inspiró el primer IBM 701.

Mientras, en el Reino Unido, Turing ideaba el ACE (*Automatic Computing Engine*) en 1945, un proyecto mucho más completo y general que el de von Neumann en su informe sobre el EDVAC. Un prototipo simplificado, el Pilot ACE, se fabricaría más tarde en el National Physics Laboratory del RU, funcionando con total éxito. La posterior arquitectura RISC (*reduced instruction set computing*) se inspiraría en la filosofía de Turing sobre el ACE.

2.4.2 Funciones recursivas

Cada máquina de Turing define una función ϕ parcial,[52] a saber, aquella que calcula: si para un dato de entrada $x_{\text{in}} \in (A - \{\sqcup\})^*$ la máquina se detiene, el resultado $T(x_{\text{in}})$ define el valor $x_{\text{out}} := \phi(x_{\text{in}})$ de la función asociada a T.

La función parcial $\phi : x_{\text{in}} \mapsto x_{\text{fin}}$ que calcula T se llama *función parcial recursiva* o *función parcial computable*. Si la máquina llega tras un número finito de pasos a un resultado final para todo dato inicial, la función ϕ asociada a T se llama *total*

[51] El hondo resentimiento de Mauchly y Eckert con la pareja Golstine y von Neumann se debió, por un lado, a razones de crédito no reconocido, y por otro, porque al intentar los primeros patentar el EDVAC para su comercialización, se les denegó por ser del dominio público la idea, tras el informe mencionado de von Neumann. Para colmo, aunque sí pudieron patentar el ENIAC como primer computador digital electrónico automático, un juez invalidaría la patente en 1973, arguyendo que la idea original se remontaba a Atanasoff.

[52] Parcial significa que su dominio no cubre necesariamente todos los datos de entrada posibles. Cabe que para alguno la máquina no se detenga jamás.

recursiva o simplemente *recursiva*.[53] A la enumeración $\{T_j\}$ de las máquinas de Turing corresponde la de sus funciones parciales $\{\phi_j\}$.

2.4.3 Máquina universal de Turing

> *Let us now return to the analogy of the theoretical computing machines... It can be shown that a single special machine of that type can be made to do the work of all. It could in fact be made to work as a model of any other machine. The special machine may be called the universal machine.* TURING

Se demuestra que existe alguna *máquina de Turing universal* U, esencialmente única, capaz de reproducir eficientemente, es decir, con retraso a lo sumo polinómico, el funcionamiento de cualquier T_j, cuando a dicha máquina U se le suministra como entrada la descripción $E(T_j)$ de la máquina T_j amén de la entrada para ésta. Nuestros ordenadores actuales son asimilables a máquinas universales de Turing, equivalentes entre sí.[54]

2.4.4 Problema de la parada

Dada una máquina T, surge la cuestión de si es posible saber de antemano si T va a detenerse tras un número finito de pasos de tiempo por haber llegado a un resultado, o si por el contrario va a estar funcionando sin descanso por no alcanzar nunca esa meta. La respuesta a este famoso *problema de la parada* o *detención* es negativa, esto es, el problema es *indecidible*, como muestra este resultado de Turing [205, 137]: No existe una función recursiva f tal que, para todo x, y, $f(x,y) = 1$ si $\phi_x(y)$ está definida, $f(x,y) = 0$ en caso contrario.[55]

2.4.5 Otros problemas indecidibles

1. Cuando Turing probó su teorema de la parada en 1936, ya hacía cinco años que Kurt Gödel (1931) había demostrado su famoso primer teorema de indecibilidad [97]: en cualquier teoría axiomatizable y firme que contiene a la aritmética de los números naturales existen fórmulas no demostrables dentro de ella. En otras palabras: ninguna axiomatización de la aritmética puede ser a la vez consistente y completa. Con esto contestaba, en sentido negativo, a uno de los interrogantes planteados por Hilbert en su programa de fundamentación de la matemática. Pero había otro problema formulado por Hilbert: el *Entscheidungsproblem* o problema de la decisión. Dado un sistema de axiomas, ¿existe algún procedimiento para decidir si una proposición cualquiera del mismo es cierta o no? Este es el problema al que Turing contestó negativamente en 1936 con su indecibilidad del problema de la parada.

[53] Un ejemplo elemental de función parcial no total es $\phi(\bar{x}) := x$, donde $\bar{x}$ es la notación autolimitante de un entero x en representación binaria. La función ϕ no está definida para $x = 1^n$.

[54] Puede demostrarse que es posible construir U con un alfabeto de 4 símbolos y con 7 estados internos. Se puede hacer también con el alfabeto A, pero con mayor número de estados internos.

[55] Como implementación de f, piénsese en una máquina de Turing T' que ante un dato inicial que engloba la descripción de otra T, dada por su índice x, y un dato inicial y para ésta, responde en tiempo finito si $\phi_x(y)$ está o no definida y por tanto si $T(y)$ converge o no. Veamos que $\nexists f$. Supongamos lo contrario, y sea la función parcial recursiva g definida como $g(x) = 1$ si $f(x,x) = 0$, y no definida en los demás casos. A tal g le corresponderá un número de Gödel z: $g = \phi_z$. Luego $\phi_z(z)$ está definida si y sólo si $f(z,z) = 0$ (por construcción de ϕ_z), lo que está en clara contradicción con las exigencias a f dadas en el enunciado del teorema.

2. De hecho, el número de problemas indecidibles es infinito: piénsese que por ejemplo el conjunto de aplicaciones de $\mathbb{N}$ en $\mathbb{Z}_2$ es no numerable,[56] mientras que el conjunto de máquinas de Turing, y por tanto de funciones parciales recursivas, es numerable.

3. La siguiente función, llamada *BB* (*Busy Beaver*), y debida a T. Rado (1962), tampoco es computable. Se define de este modo: sea C_n el conjunto de las máquinas de Turing T de n estados (aparte del estado q_{in}), alfabeto $A = \{0, 1\}$,[57] y que cumplen $\phi_T(0)\downarrow$, donde ϕ_T es la función parcial recursiva asociada a la máquina T, esto es, se detienen cuando el dato inicial en la cinta es el vacío ε. Se define $BB(n) := \max_{T\in C_n}\{k : \phi_T(0) = 1^k\}$. Es fácil ver que $|C_n| \leq (4(n+1))^{2n}$, por lo que $BB(n)$ está bien definida. Se sabe que $BB(1) = 1, BB(2) = 4, BB(3) = 6, BB(4) = 13, BB(5) \geq 4098, BB(6) \geq 95\,524\,079$. La función *BB* no es computable, pues se demuestra que crece más deprisa que cualquier función computable.

4. De entre los 23 problemas propuestos por David Hilbert en el Congreso Internacional de Matemáticos de 1900 en París, en el número 10 se preguntaba si existía algún algoritmo capaz de contestar sobre si una ecuación diofántica arbitraria tiene o no alguna solución: *10. Entscheidung der Lösbarkeit einer diophantischen Gleichung*. En 1970 el matemático ruso Yu.V. Matijasevich resolvía este problema de Hilbert: no existe tal algoritmo, es decir, la cuestión planteada por Hilbert es indecidible.

5. Supongamos una colección $T = \{t_0, \ldots, t_k\}$ de tipos de baldosas cuadradas, y dos relaciones $H, V \subset T \times T$ de compatibilidad horizontal (vertical). Sea n un entero, y un alicatado $n \times n$ dado por una función $F : \{1, \ldots, n\} \times \{1, \ldots, n\} \to T$ tal que $F(1,1) = t_0$, $(F(i,j), F(i+1,j)) \in H$, $(F(i,j), F(i,j+1)) \in V$. El problema ENLOS de saber si, dados T, H, V arbitrarios existe un embaldosado f para todo n, es indecidible [167].

6. En 1958 Markov probó que el problema de averiguar si dos variedades 4D son o no homeomorfas es indecidible.

7. Quedan importantes problemas abiertos respecto de la decidibilidad. Por ejemplo: dada una matrix $M, n \times n$, de coeficientes enteros, ¿existe algún m tal que $(M^m)^n_1 = 0$?

2.5 Clases de complejidad

Desde el punto de vista de la computación, hay problemas indecidibles como hemos visto, y problemas decidibles o resolubles, que son todos los demás (y que, en pocas palabras, pueden entenderse como aquellos problemas para los que existe algún algoritmo o programa de computación en algún lenguaje que los resuelve). Estos últimos, a su vez, se dividen en problemas fáciles (computacionalmente tratables, viables o factibles), y problemas duros (computacionalmente intratables o inviables). Ejemplos: 1. Elevar un número al cuadrado es un problema fácil, en el sentido de que los recursos que ello exige (concretamente, el tiempo de cálculo) crecen a lo sumo polinómicamente con el tamaño (número de dígitos) del número en cuestión. 2. Descomponer un número en factores primos es un problema actualmente duro, pues con los mejores algoritmos conocidos el tiempo de cálculo para la factorización crece superpolinómicamente con el tamaño del número.

[56] Basta aplicar el argumento diagonal de Cantor. Supongamos que fuera numerable: $\{f_0, f_1, \ldots, f_n, \ldots\}$. Sea la función $g : n \mapsto f_n(n) + 1 \bmod 2$. Debería estar en el conjunto anterior, es decir, $g = f_k$, para algún k. Pero entonces $g(k) = f_k(k) + 1 \bmod 2$, y $g(k) = f_k(k)$. Contradicción.

[57] En la definición de máquina de Turing exigíamos que el alfabeto contuviera siempre el símbolo "blanco" $\sqcup$. Se puede demostrar la equivalencia de las máquinas con $A = \{0, 1, \sqcup\}$ y las máquinas con $A = \{0, 1\}$ pero con mayor número de estados.

Se han inventado las clases de complejidad para agrupar a los problemas atendiendo esencialmente a estos tres aspectos [164]: 1/ su grado de dificultad, medido por el coste o recursos (en tiempo, en espacio, etc.) que exige su resolución, 2/ el tipo de problema (de decisión, de optimización, de número de soluciones, etc.), y 3/ la herramienta de cálculo utilizada (MTD, MTP, MTQ, etc.).[58]

Dada una MTD T, se dice que tiene *complejidad temporal* $t(n)$ si, con un dato inicial arbitrario de longitud binaria n, realiza a lo sumo $t(n)$ pasos antes de detenerse. Del mismo modo, si usa como borrador a lo más $e(n)$ celdas de la cinta (excluidas las necesarias para la entrada y el resultado, que pueden suponerse en otras cintas), diremos que tiene *complejidad espacial* $e(n)$. Diremos que T es polinómicamente acotada en tiempo si $t(n) = O(n^k)$ para algún $k \in \mathbb{N}$.

Se dice que una MTD T *decide* un *lenguaje* L (subconjunto de $(A-\sqcup)^*$, conjunto de palabras o cadenas finitas de un alfabeto A), si su resultado es 1 cuando el dato está en L, y 0 en caso contrario. El problema resuelto por T es por tanto un problema de decisión, o de cálculo de una función predicado, para el que los resultados posibles son 1 ("sí") y 0 ("no"). Se dice también en estos casos que un dato de entrada en L posee la *propiedad* definida por L. Todo lenguaje decibible por alguna MTD se dice recursivo. Se dice que T *acepta* un *lenguaje* L si su salida es 1 cuando la entrada está en L, y diverge en caso contrario. Un lenguaje L aceptado por alguna MTD se dice que es recursivamente enumerable. Es fácil ver que todo L recursivo es recursivamente enumerable.

La clase de complejidad $\mathsf{DTIME}[t(n)]$ ($\mathsf{DSPACE}[s(n)]$) consta de los lenguajes decididos por MTDs y con varias cintas en tiempo máximo $O(t(n))$ (en espacio máximo $O(e(n))$).[59]

Las clases de complejidad $\mathsf{NTIME}[t(n)]$ ($\mathsf{NSPACE}[s(n)]$ se definen de modo similar, pero admitiendo máquinas de Turing no deterministas, y tomando un lenguaje $L \subset (A-\sqcup)^*$ como decidible por la MTND T si para todo dato x, $x \in L$ si y sólo si existe algún camino de computación de la MTND que tiene entrada x y termina con el resultado 1.

Con las clases anteriores se forman estas otras clases de gran importancia:

$$\mathsf{P} := \bigcup_{r=0,1,2,\ldots} \mathsf{DTIME}[n^r], \quad \mathsf{NP} := \bigcup_{r=0,1,2,\ldots} \mathsf{NTIME}[n^r]$$

$$\mathsf{PSPACE} := \bigcup_{r=0,1,2,\ldots} \mathsf{DSPACE}[n^r], \quad \mathsf{NSPACE} := \bigcup_{r=0,1,2,\ldots} \mathsf{NSPACE}[n^r]$$

Mientras los problemas de complejidad P son aquellos cuya solución se consigue en tiempo polinómico con una MTD, o equivalentemente, aquellos problemas para los que existe algún algoritmo (de tiempo de ejecución) polinómico, los de complejidad NP pueden caracterizarse por ser problemas de decisión en los que, dado un dato inicial, es fácilmente (esto es, en tiempo polinómico) verificable que posee la propiedad en cuestión si se dispone de un *certificado* sucinto o *testigo* polinómico apropiado. Por ejemplo, la propiedad COMP de un entero de ser compuesto está en NP, pues dado N como dato y como certificado o testigo un factor f, en tiempo polinómico podemos comprobar que f divide a N y verificar de este modo el carácter compuesto de este

[58] MTQ indica una máquina de Turing cuántica, noción ésta que introduciremos luego.

[59] Una máquina con k cintas – de las que una, sólo de lectura, se reserva para registrar el dato de entrada – se define de forma similar, a través ahora de una función $\delta : Q \times A^k \to Q \times A^k \times M^k$ (caso determinista) o de una relación $\delta : Q \times A^k \to 2^{Q \times A^k \times M^k}$. Una MTD con k cintas y de complejidad temporal (espacial) $t(n) > n$ ($e(n)$) equivale a una máquina de Turing convencional, esto es, de una sóla cinta, de complejidad temporal (espacial) $t^2(n)$ ($e(n)$).

último. Formalmente, podemos redefinir la clase NP como la de aquellos lenguajes L para los que hay una MTD T polinómicamente acotada en tiempo y un polinomio p tales que que

$$x \in L \Longleftrightarrow \exists y \in A^{\star}, |y| \leq p(|x|), T(x,y) = 1.$$

Otro modo de definir la clase NP es como el conjunto de problemas que pueden resolverse en tiempo polinónico mediante un algoritmo no determinista [153], entendiendo por tal un algoritmo que admite instrucciones del tipo

goto both etiqueta 1, etiqueta 2

Nótese que tales hipotéticos programas, si existieran, podrían ejecutar un número exponencial de instrucciones en tiempo polinómico. En el mundo de los ordenadores clásicos, tales algoritmos son una mera construcción teórica, pero en la computación cuántica, pueden ser, en principio, una realidad.[60]

En los problemas $\mathsf{NP}-\mathsf{P}$, la razón de su intratabilidad está en el tamaño exponencial del espacio de búsqueda, y precisamente los algoritmos no deterministas pueden explorar teóricamente todas las opciones en tiempo polinómico.

Como en cada paso temporal se usa a lo sumo una nueva celda (o k nuevas celdas si la MT es de k cintas), es claro que tanto P como NP están en PSPACE. Por otro lado, no es difícil probar que $\mathsf{PSPACE} = \mathsf{NSPACE}$.

En consecuencia $\mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{PSPACE} = \mathsf{NSPACE}$. Se ignora si las inclusiones son propias. Un problema central abierto en la teoría de la computación es probar precisamente la conjetura siguiente: $\mathsf{P} \subsetneq \mathsf{NP}$.

2.5.1 Ejemplos

He aquí algunos ejemplos[61] de problemas en la clase P [216]:

1. ADIC: adición de enteros. Sumar dos números de n bits cada uno requiere $O(n)$ operaciones (con bits).

2. MULT: multiplicación de enteros. Multiplicar en la forma usual dos números de n bits cada uno requiere $O(n^2)$ operaciones, pero acudiendo a la transformada rápida de Fourier puede hacerse el producto con $O(n \log_2 n \log_2 \log_2 n)$ operaciones. Calcular el producto de dos matrices $n \times n$ requiere, por el método ingenuo, $O(n^3)$ multiplicaciones. Métodos sofisticados permiten rebajar a $O(n^{2.376})$.

3. EUCL: algoritmo de Euclides para el m.c.d. El cálculo del m.c.d. de dos números, el mayor con n bits, puede hacerse en $O(n^3)$ operaciones.[62]

4. DET: cálculo del determinante de una matriz. Dada una matrix $n \times n$, su determinante puede calcularse con $O(n^{2.3976\ldots})$ operaciones.

[60] El paralelismo masivo que hace posible el cálculo simultáneo de un número exponencial de casos con los ordenadores cuánticos es un tanto engañoso, porque los resultados están superpuestos, y su actualización exige medir. Por tanto, sin una debida amplificación previa de la amplitud del caso que interese, la probabilidad de obtener el resultado buscado sería exponencialmente pequeña, y las ventajas del paralelismo desaparecerían.

[61] Aunque muchos de los ejemplos en esta subsección no son problemas de decisión, los incluimos por su importancia; corresponden a clases P, NP vinculadas a tipos más amplios de problemas, y definidas de modo análogo al seguido para las cuestiones de decisión.

[62] Ver, sin embargo, [128].

5. SORT: ordenación de una lista. Una lista desordenada de n items puede ordenarse en $O(n\log_2 n)$ operaciones.

6. MODEXP: exponenciación en aritmética modular. El cálculo de $a^x \bmod N$ puede hacer en $O((\log_2 N)^2 \log_2 x)$ operaciones.

7. $\mathrm{kP}_{\mathrm{elípt}}$: multiplicación de puntos sobre curvas elípticas por grandes enteros. Dado un punto P de una curva elíptica sobre un cuerpo F_q ($q = p^r$, con p primo), el cálculo de kP requiere $O((\log_2 q)^3 \log_2 k)$ operaciones.

8. CIRC EUL: averiguar si un grafo admite un circuito euleriano. Dado un grafo $G := (V, L)$ consistente en un conjunto V de vértices v_i y otro L de líneas l^k_{ij} que conectan pares (v_i, v_j) de estos vértices, se llama circuito a una sucesión alternada $v_1 l^1_{12} v_2 l^2_{23} v_3 \ldots l^n_{n1} v_1$ de vértices (no necesariamente distintos todos) y líneas todas distintas, que termina en el mismo vértice de partida. Y se dice que un circuito es euleriano cuando todas las líneas en L figuran en él, y sin repetición [153].

   El ejemplo más famoso de problema CIRC EUL es el de los puentes de Königsberg. Euler se encargó de probar en 1736 que no era posible encontrar un circuito que cruzara los siete puentes de esta ciudad sin repetirse, dándose cuenta de que una condición necesaria para que tal circuito existiera era que el grado de cada vértice (número de líneas incidentes en él) fuese par, lo que no se daba en ese caso. Es también una condición suficiente, por lo que el problema CIRC EUL es tratable, de complejidad polinómica $O(|V|^2)$. (Asociando al grafo una matriz A de adyacencia, en que la entrada a_{ij} es el número de líneas que unen los vértices v_i, v_j, basta ir sumando las filas, y el grafo tendrá un circuito euleriano si y sólo si todas las filas de A tienen suma par.)

Ejemplos de problemas computacionalmente más complejos son [216, 167]:

1. DLOG: cálculo del log discreto. Dados $a, b, n \in \mathbb{N}$, se trata de calcular (si existe) x tal que $a^x = b \bmod n$. La complejidad de este problema es $O(\exp(c(\log_2 n)^{1/3}(\log_2 \log_2 n)^{2/3})$, esto es, subexponencial aunque superpolinómica en el número de bits del módulo.

2. COMP: averiguar si un entero es compuesto. Este problema está en la clase NP, pues dado un presunto divisor no trivial de n como certificado, puede comprobarse en tiempo polinómico si efectivamente lo es, y por tanto, si n es compuesto. La complejidad de comprobar que d es un divisor o no de n es $O((\log_2 n)^2)$.

3. PRIM: averiguar si un entero es primo. Siendo el carácter de primo opuesto al de compuesto, es claro que PRIM $\in$ coNP, donde coNP es la clase de lenguajes L cuyo opuesto o complementario $L^{\mathrm{c}} := (A - \sqcup)^* - L$ es de clase NP. Por tanto es fácil probar que n no está en PRIM, exhibiendo una *descalificación sucinta*, a saber, un divisor de n. No es igual de fácil, sin embargo, dar un certificado sucinto de primalidad, esto es, de pertenencia a PRIM. El certificado (Pratt 1975) ahora para p consiste en dar un $r < p$ y los divisores primos $q_1, q_2, \ldots$ de $p-1$ (con sus certificados de primalidad) y comprobar que efectivamente lo son y que $r^{p-1} = 1 \bmod p$, y $r^{(p-1)/q_j} \neq 1 \bmod p$. Estos certificados completos tienen tamaño polinómico respecto del tamaño de p, y su aplicación requiere tiempo polinómico también. Luego PRIM $\in$ NP $\cap$ coNP.[63]

[63] Si se acepta la hipótesis generalizada de Riemann, se demuestra que PRIM $\in$ P (Miller 1976).

4. FACT: factorización de enteros. Dado $n \in \mathbb{N}$, se trata de hallar algún divisor no trivial de n. El vulgar método de probar si es divisible por los enteros $\leq \sqrt{n}$ tiene complejidad $O(n/\log_2 n)$, que es exponencial en el número de bits. El algoritmo más eficiente hoy conocido (algoritmo GNFS de la criba general con cuerpos de números algebraicos [171, 135]) es subexponencial pero superpolinómico: $O(\exp(c(\log_2 n)^{1/3}(\log_2 \log_2 n)^{2/3})$, con $c = (64/9)^{1/3} + o(1)$.

5. SAT: averiguar si una expresión booleana ϕ en forma conjuntiva normal ($\phi = \bigwedge_1^n C_i$, $C_i := z_{i1} \vee z_{i2} \vee \ldots \vee z_{ir_i}$, con $z_{ij} \in (x_{ij}, \neg x_{ij})$ variables booleanas o sus negaciones) es satisfactible (esto es, existe alguna asignación de verdad a sus variables que la hacen cierta). Este problema es de clase NP. Probar exhaustivamente todas las asignaciones de verdad tiene complejidad $O(n^2 2^n)$.

6. VIAJ(D): averiguar si hay algún recorrido que pase por varias ciudades una sola vez y su trayecto no supere una longitud dada. Este es el famoso problema de decisión del viajante. Dadas n ciudades, sus distancias mutuas $d_{ij} \geq 0$, y una cota o "presupuesto de viaje" C, se trata de ver si existe alguna permutación cíclica π tal que $\sum_{i=1}^n d_{i,\pi(i)} \leq C$. Probar todos los posibles caminos cerrados que pasan una vez, y sólo una, por cada ciudad, requiere $\frac{1}{2}(n-1)!$ ensayos (invertir el sentido de recorrido no cambia la longitud del recorrido), y como para cada ensayo el cálculo del coste es $O(n)$, este problema es de complejidad exponencial $O(\frac{1}{2}n!)$. Pero si nos dan un presunto trayecto solución, su comprobación es de complejidad polinómica en n. Por ello VIAJ(D) $\in$ NP.

7. ASIGN: dadas n "ciudades" y sus distancias mutuas $d_{ij} \geq 0$, se trata de hallar una permutación (no necesariamente cíclica) π que minimice $\sum_{i=1}^n d_{i,\pi(i)}$. Este problema es similar al VIAJ, pero con la posibilidad de repartir las ciudades en subconjuntos disjuntos con un número indeterminado de viajantes, cada uno realizando su vuelta cerrada por las ciudades de uno de esos subconjuntos.

   Se conoce esto corrientemente como el problema de asignación, así llamado porque su aplicación más directa es la de minimizar el coste $\sum_{i=1}^n d_{i,\pi(i)}$ de un reparto o asignación de n tareas a un conjunto de n obreros, siendo ahora $d_{ij} \geq 0$ el coste de la tarea j cuando la lleva a cabo el obrero i. El número de ensayos a realizar es $n!$, y uno pensaría que la complejidad de este problema es exponencial. Sin embargo, existe un algoritmo, llamado *algoritmo húngaro*, que rebaja la complejidad de este problema a $O(n^3)$.

8. GO: jugando al GO. Se supone en tableros $n \times n$, n arbitrario (en el GO normal $n = 19$). Imponemos la regla (que no es del GO ordinario) de que el juego termina tras n^2 jugadas en total, ganando quien más fichas tiene en el tablero (en caso de empate, ganan BLANCAS). Supongamos que tras $k < n^2$ jugadas en total, le toca jugar a NEGRAS, y que hay una configuración arbitraria de piedras blancas y negras sobre el tablero. Problema GO: ¿es esta un configuración ganadora para NEGRAS?

9. CICL HAM: averiguar si un grafo admite un ciclo hamiltoniano. Dado un grafo $G := (V, L)$, se llama ciclo a una sucesión alternada de vértices (todos distintos, salvo el primero y el último) y líneas $v_1 l_{12}^1 v_2 l_{23}^2 v_3 \ldots l_{n1}^n v_1$, que termina en el mismo vértice de partida. Y se dice que un ciclo es hamiltoniano cuando todas los vértices en V figuran en él [153]. Este problema fue sugerido por el problema

"icosiano" propuesto por Hamilton en 1859: hallar un recorrido cerrado por las aristas de un dodecaedro que pase por todos los vértices sin repetir ninguno.

El problema CICL HAM es intratable.

2.5.2 Más sobre las clases P y NP

Obsérvese esta importante diferencia entre P y NP. Si una propiedad L está en P, también su negación L^c lo está, y recíprocamente. (Basta redefinir la máquina T asociada intercambiando las respuestas 0, 1.) En símbolos: $\mathsf{P} = \mathsf{coP}$. Pero si una propiedad está en NP, su negación no tiene en principio por qué ser NP. Sin embargo, no se conocen casos concretos que lo avalen; por ejemplo, la negación de COMP es PRIM (propiedad de ser primo), también en NP (y tal vez en P, como ocurre si la hipótesis generalizada de Riemann es cierta). Se conjetura que $\mathsf{NP} \neq \mathsf{coNP}$; de ser así, se desprendería evidentemente que $\mathsf{P} \neq \mathsf{NP}$.

Denotemos por Σ un alfabeto. Se dice [185] que el lenguaje $L_1 \subseteq \Sigma_1^*$ es *polinómicamente reducible* al lenguaje $L_2 \subseteq \Sigma_2^*$, y escribiremos $L_1 \leq_{\mathrm{P}} L_2$, si existe una función $f : \Sigma_1^* \to \Sigma_2^*$ en P tal que $x \in L_1$ si y sólo si $f(x) \in L_2$. Es fácil convencerse de que $\leq_{\mathrm{P}}$ es una relación transitiva. Cuando $L_1 \leq_{\mathrm{P}} L_2$ y $L_2 \leq_{\mathrm{P}} L_1$, las propiedades L_1, L_2 se dicen *polinómicamente equivalentes* y se escribe $L_1 \equiv_{\mathrm{P}} L_2$.

Se puede probar fácilmente que si $L_1 \leq_{\mathrm{P}} L_2$ y L_2 está en P, también L_1 está en P.

Un lenguaje L_0 dícese NP-*duro* (clase NPD) si $L \leq_{\mathrm{P}} L_0$, $\forall L \in \mathsf{NP}$. Si además $L_0 \in \mathsf{NP}$, diremos que L_0 es NP-*completo* (clase NPC). Obviamente $\mathsf{NPC} \subseteq \mathsf{NPD}$. Más aún, se afirma que $\mathsf{NPC} \subsetneqq \mathsf{NPD}$ [211].

Es claro que si hubiera algún lenguaje NP-*duro*, o NP-*completo*, que estuviera en la clase P, forzosamente toda la clase NP colapsaría a P, esto es, $\mathsf{P} = \mathsf{NP}$, y el problema central de la teoría de la computación estaría resuelto.

Al igual que la clase P consta de los problemas de decisión más fáciles o simples, o como también se dice, problemas computacionalmente *tratables*, el conjunto $\mathsf{NP} - \mathsf{P}$ está formado por los problemas *intratables*, y entre ellos los más difíciles integran la clase NPC. Se demuestra que si L es NP-completo y L^c está en NP, entonces forzosamente se tendría $\mathsf{NP} = \mathsf{coNP}$.

Un famoso teorema de Cook asegura que $\mathsf{NPC} \neq \emptyset$. De hecho, se conocen millares de lenguajes NP-completos [95]. El primer lenguaje conocido en NPC fue SAT (teorema de Cook-Levin), formado por las expresiones satisfactibles en la lógica booleana.

Otro lenguaje NP-completo es el asociado al ya citado problema VIAJ(D): el lenguaje VIAJ(D) consta de aquellas ternas formadas por un conjunto de ciudades $\{C_1, \ldots, C_N\}$, el conjunto de sus distancias mutuas $\{d_{(C_i,C_j)} > 0, d_{(C_j,C_i)} = d_{(C_i,C_j)} : 1 \leq i \neq j \leq N\}$ y una cota $B > 0$, tales que existe algún circuito cerrado que las recorre todas sin repetición y cuyo trayecto total es $\leq B$. Dado un ejemplo concreto de ciudades, distancias y cota, resolver el problema VIAJ(D) equivale a averiguar si este ejemplo pertenece al lenguaje VIAJ(D).

Y otro lenguaje NP-completo, de teoría de los números, es CONG-CUAD, vinculado a este problema de decisión: dados los enteros positivos a, b y un número $0 < c \leq \infty$, ¿existe un entero positivo $x < c$ tal que $x^2 = a \bmod b$?

Es obvio que todos los lenguajes NPC son polinómicamente equivalentes. Si aceptamos que $\mathsf{P} \subsetneqq \mathsf{NP}$, entonces puede demostrarse que hay lenguajes de dificultad intermedia entre P y NPC. Constituyen la clase

$$\mathsf{NPI} := \mathsf{NP} - (\mathsf{P} \cup \mathsf{NPC}) \neq \emptyset.$$

Candidato natural a estar en esta clase intermedia es, por ejemplo, COMP. Pues según dije antes, COMP $\in \mathsf{NP} \cap \mathsf{NP}^{\mathsf{c}}$, y si COMP fuese NP-completo, entonces $\mathsf{NP} = \mathsf{coNP}$ y en consecuencia $\mathsf{P} = \mathsf{NP}$, contra lo que se espera.

La noción de lenguaje completo se extiende a cualquier clase de complejidad X: un lenguaje L_0 dícese X-completo, y escribiremos $L_0 \in \mathsf{XC}$, si todo otro lenguaje L en C es polinómicamente reducible a L_0, en símbolos $L \leq_{\mathrm{P}} L_0$. Por ejemplo, QSAT y GO están en PSPACEC.

2.5.3 Otras clases de complejidad

Terminamos introduciendo nuevas clases de complejidad [167, 211]:[64]

$$\mathsf{EXP} := \bigcup_{r=0,1,2,\ldots} \mathsf{DTIME}[2^{n^r}], \quad \mathsf{NEXP} := \bigcup_{r=0,1,2,\ldots} \mathsf{NTIME}[2^{n^r}].$$

Constan de aquellos problemas resolubles en tiempo exponencial con MTDs o MTNDs, respectivamente. No es difícil convencerse de que PSPACE $\subseteq$ EXP: si una MTD tiene r estados internos, s símbolos en su alfabeto, y usa a lo sumo $p(n)$ celdas para ejecutar un programa con un dato de entrada de longitud binaria n, el número de los pares (p, a) estado-símbolo con los que se encuentra antes de detenerse con el resultado del cálculo es a lo sumo $rs^{p(n)}$, por lo que si el tiempo empleado en dicho cálculo fuese más que exponencial en n, forzosamente se repetiría alguna situación (p, a), y la máquina se metería en un ciclo sin salida, contra la hipótesis. Del mismo modo, si L denota la clase de problemas de decisión cuya solución require espacio logarítmico $O(\log_2 n)$,[65] se tiene $\mathsf{L} \subseteq \mathsf{P}$. En consecuencia, podemos escribir:

$$\mathsf{L} \subseteq \mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{PSPACE} \subseteq \mathsf{EXP} \subseteq \mathsf{NEXP}.$$

Como ejemplos de problemas en EXP (pues el número de jugadas a analizar crece exponencialmente con el tamaño del tablero), y que se cree que no son de clase NP, tenemos los relacionados con los juegos GO, DAMAS y AJEDREZ en campos $n \times n$: ¿existen estrategias del primer jugador siempre ganadoras?

El problema llamado SUC CIRC VAL pertenece a EXPC – P, y otro, conocido como SUC CIRC SAT, está en NEXPC – P. Por tanto $\mathsf{P} \subsetneq \mathsf{EXP}$. En general, esta inclusión propia se sigue del teorema de jerarquía temporal, que afirma que $\mathsf{TIME}(f(n)) \subsetneq \mathsf{TIME}(f(n)\log_2^2 f(n))$. Análogamente, el teorema de jerarquía espacial, que afirma que $\mathsf{SPACE}(f(n)) \subsetneq \mathsf{SPACE}(f(n)\log_2 f(n))$, implica que $\mathsf{L} \subsetneq \mathsf{PSPACE}$. Pero se ignora cuál de las inclusiones en la cadena larga anterior es propia.

No acaba aquí la clasificación. Hay problemas todavía más "monstruosos" en su complejidad. Por ejemplo, vinculado a la aritmética de Presburger hay un problema al menos doblemente exponencial (complejidad temporal 2^{2^n} en el tamaño n del dato inicial).

[64] La teoría cuántica de campos con términos topológicos no abelianos puede en principio permitir simular computadores analógicos que resuelvan problemas NP-duros e incluso #P-duros en tiempo polinómico [83]. Esta última clase se obtiene cuando dado un problema de decisión de complejidad NP, nos preguntamos para cuántos certificados iniciales la respuesta es "sí"; por ejemplo, contar cuántas satisfacciones booleanas tiene una fbfcp (fórmula bien formada del cálculo proposicional) es un problema #P-completo. La evaluación del polinomio de Jones en raíces primitivas de la unidad de orden ≥ 5 es #P-duro.

[65] Como el propio dato inicial ya ocupa un espacio n, debemos ser más precisos: se supone que la máquina de Turing que define un problema en esta clase tiene dos cintas, una de lectura en la que sólo se escribe el dato inicial, y otra, inicialmente vacía, que se usa exclusivamente para el cálculo en sí, y de la que éste va a cubrir $O(\log_2 n)$ celdas.

2.5.4 Complejidad con MTPs

En cálculos con MTPs aparecen asociadas nuevas clases de complejidad, llamadas aleatorias. Destacan estas [216]:

1. RP: clase polinómica aleatoria. Dado un $0 < \varepsilon < 1$, RP consta de los lenguajes L que una MTP T, que trabaja siempre (para todo dato inicial) en tiempo polinómico, decide con error $\leq (1-\varepsilon)$. Estos lenguajes se llaman polinómicos Monte Carlo. Expresado de otro modo,

$$x \in L \implies \text{prob}(T(x) = 1) \geq \varepsilon$$
$$x \notin L \implies \text{prob}(T(x) = 1) = 0.$$

Quiere esto decir que todos los caminos computacionales que la MTP T pueda seguir a partir de un dato $x \notin L$ terminan en rechazo ($T(x) = 0$), mientras que si $x \in L$, entonces al menos una fracción ε de los caminos posibles terminan en aceptación ($T(x) = 1$). Por tanto no puede haber falsos positivos (pues si $x \notin L$ el rechazo es unánime), y a lo sumo puede haber una fracción $1-\varepsilon$ de falsos negativos (casos en que $x \in L$ y sin embargo el camino seguido termina en rechazo). Repitiendo el cálculo con el mismo $x \in L$ un número de veces $n \geq \lceil \log_2 \delta / \log_2(1-\varepsilon) \rceil$, donde $0 < \delta < 1$, podremos conseguir que la probabilidad de n falsos negativos consecutivos sea $\leq \delta$ y por tanto tan pequeña como queramos eligiendo adecuadamente δ, o lo que es lo mismo, que la probabilidad de que en esa serie de n ensayos obtengamos alguna aceptación de x sea $\geq (1-\delta)$ y por tanto tan cercana a 1 como deseemos. (Por eso el valor de ε en la definición de RP es irrelevante, y generalmente se toma de entrada $\varepsilon = \frac{1}{2}$.) En casos de verdadera "mala suerte" podría ocurrir que series muy largas no contuvieran ninguna aceptación; por eso se dice a menudo que tal T decide L en tiempo "esperado" polinómico.

2. ZPP: clase polinómica aleatoria con probabilidad cero de error. Se define como $\mathsf{ZPP} := \mathsf{RP} \cap \mathsf{coRP}$, y consta por tanto de aquellos lenguajes L para los que existen sendas MTPs, $T_{\mathrm{RP}}, T_{\mathrm{coRP}}$, que trabajan siempre en tiempo polinómico y cumplen

$$x \in L \implies \text{prob}(T_{\mathrm{RP}}(x) = 1) \geq \tfrac{1}{2},\ \text{prob}(T_{\mathrm{coRP}}(x) = 0) = 0,$$
$$x \notin L \implies \text{prob}(T_{\mathrm{RP}}(x) = 1) = 0,\ \text{prob}(T_{\mathrm{coRP}}(x) = 0) \geq \tfrac{1}{2}.$$

Estos lenguajes se dice que son polinómicos Las Vegas: son Monte Carlo, y sus complementarios también. En otras palabras, tienen dos algoritmos Monte Carlo, uno sin falsos positivos, y otro sin falsos negativos, por lo que con suerte cualquier dato de entrada es decidible de forma exacta: basta que el algoritmo sin falsos positivos diga "sí", o que el que no tiene falsos negativos diga "no". Si hay mala suerte, tendremos que repetirlo varias veces y decidir por mayoría con error tan pequeño como se quiera, tras un tiempo ¡esperado! polinómico. Ejemplo: PRIM está en ZPP. El algoritmo de Miller-Selfridge-Rabin (test fuerte de pseudoprimalidad, 1974) es del tipo coMonte-Carlo, esto es, PRIM está en coRP (de hecho, la probabilidad de falsos positivos, esto es, que "un primo probable" no lo sea, es $\leq 1/4$) . Que está en RP es mucho más complicado, y se debe a Adleman y Huang (1987) su demostración, basada en la teoría de variedades abelianas (generalización a más dimensiones de las curvas elípticas).[66]

3. BPP: clase polinómica aleatoria con probabilidad acotada de error. Dado $0 < \varepsilon < \frac{1}{2}$, BPP consta de aquellos lenguajes L para los que existe una MTP T que trabaja

[66] Dado un entero N, existe un algoritmo determinista de primalidad, debido a Adleman-Pomerance-Rumely-Cohen-Lenstra (1980-81), de complejidad $O((\log_2 N)^{c \log_2 \log_2 \log_2 N})$, donde c es una constante. Un ordenador típico de los de hoy tarda unos 30 s para N de 100 dígitos decimales, unos 8 min si N tiene 200 dígitos, y un tiempo prudencial en el caso de 1000 dígitos.

siempre en tiempo polinómico y cumple

$$x \in L \implies \text{prob}(T(x) = 1) \geq \tfrac{1}{2} + \varepsilon,$$
$$x \notin L \implies \text{prob}(T(x) = 1) \leq \tfrac{1}{2} - \varepsilon.$$

Los lenguajes BPP son tal vez los que mejor representan la noción de cálculos realistas. Son aceptados y rechazados por una MTP con posibilidad de error. Pero este error es $\leq (\frac{1}{2} - \varepsilon)$ tanto en la aceptación como en el rechazo. Como antes, el valor concreto de ε es irrelevante, y acostumbra a tomarse $\varepsilon = \frac{1}{4}$. La repetición del algoritmo con el mismo x permite amplificar la probabilidad de acierto, y, acudiendo al voto de la mayoría, decidir con error tan pequeño como se quiera en un tiempo (esperado, salvo casos de mala suerte) polinómico. No se sabe si BPP está en NP. Pero es claro que RP $\subseteq$ BPP, así como BPP $=$ coBPP. En general:

$$\mathsf{P} \subseteq \mathsf{ZPP} \subseteq \mathsf{RP} \subseteq (\mathsf{BPP}, \mathsf{NP}) \subseteq \mathsf{PSPACE} \subseteq \mathsf{EXP} \subseteq \mathsf{NEXP}.$$

2.6 Circuitos lógicos

Las máquinas de Turing son (polinómicamente) equivalentes a *circuitos lógicos, booleanos* o *combinatorios*, y *uniformes*, representables por grafos finitos, dirigidos y acíclicos, con líneas de entrada, con vértices internos, nodos o puertas lógicas, y con líneas de salida [4, 173, 167, 101, 164].[67] Un circuito C de éstos, con m (n) líneas de entrada (salida), evalúa una función $f_C : x \in \{0,1\}^m \mapsto f(x) \in \{0,1\}^n$; por cada línea de entrada se introduce un bit argumento de la función, y los bits del resultado aparecen en las líneas de salida. Basta discutir circuitos con $n = 1$, y que por tanto resuelven problemas de decisión, pues el caso general equivale al cálculo de una colección de n de estas funciones, y es por tanto realizable mediante un conjunto de n circuitos de esos.

Ejemplos de puertas lógicas binarias son los conectores AND ($\wedge$, conjunción, $x \wedge y = xy$) y OR ($\vee$, disyunción, $x \vee y = x + y - xy$), y de puerta unaria el conector NOT ($\neg$, negación, $\neg x = 1 - x$). Cualquier otra de las 16 puertas booleanas $\{0,1\}^2 \mapsto \{0,1\}$ es combinación de estos conectores básicos. En general, dada cualquier función $f : x \in \{0,1\}^m \mapsto f(x) \in \{0,1\}$, podemos escribir $f = f^{(1)}(x) \vee f^{(2)}(x) \vee \ldots$, con

$$f^{(r)}(x) := \begin{cases} 1 & \text{si } x = x^{(r)} \\ 0 & \text{casos restantes} \end{cases}$$

donde $\{x^{(1)}, x^{(2)}, \ldots\} := f^{-1}(1)$. Por otro lado,

$$f^{(r)}(x) = x'_1 \wedge x'_2 \wedge \ldots \wedge x'_m, \quad x'_k := \begin{cases} x_k & \text{si } x_k = 1 \\ \neg x_k & \text{si } x_k = 0 \end{cases}$$

De este modo hemos expresado f en lo que se llama forma disyuntiva normal a través de OR, NOT y AND. (Nótese que implícitamente se ha utilizado también la operación COPY o FANOUT: $x \in \mathbb{Z}_2 \mapsto xx$, pues cada $f^{(r)}$ requiere su propia copia de x sobre la que actuar.)

Así, por ejemplo:

[67] La condición de uniformidad se cumple cuando la circuitería que calcula las funciones con datos iniciales de tamaño $n = 1, 2, \ldots$ sea diseñable en tiempo polinómico mediante una máquina de Turing. De esta manera se evita esconder la complejidad del problema a resolver en las propias "tripas"del circuito. De no imponer esa uniformidad, habría incluso circuitos que calcularían el problema no computable de la parada.

- La suma booleana $\oplus : \{x,y\} \mapsto x \oplus y := x + y \bmod 2$ puede representarse como

$$x \oplus y = ((\neg x) \wedge y) \vee (x \wedge (\neg y)).$$

  Esta operación es realizada por la puerta lógica conocida como XOR (*exclusive* OR) o CNOT (*controlled* NOT), que discutiremos luego.[68]

- La operación NAND $\uparrow$: $\{x,y\} \mapsto x \uparrow y := 1 - xy$ puede escribirse como

$$x \uparrow y = \neg(x \wedge y) = (\neg x) \vee (\neg y).$$

- Análogamente NOR $\downarrow$: $\{x,y\} \mapsto x \downarrow y := (1-x)(1-y)$ puede escribirse como

$$x \downarrow y = \neg(x \vee y) = (\neg x) \wedge (\neg y).$$

Los conectores COPY y NAND (o COPY y NOR) se bastan para generar los demás: nótese que $\neg x = x \uparrow x = x \uparrow 1$, $x \wedge y = (x \uparrow y) \uparrow (x \uparrow y)$, $x \vee y = (x \uparrow x) \uparrow (y \uparrow y)$. Más aún, si podemos generar *ancillae* o bits constantes auxiliares (0 o 1), entonces la puerta NAND/NOT: $(x,y) \mapsto (1-x, 1-xy)$ es *universal*, es decir, con ella, aplicada sucesivamente a pares de bits, puede calcularse cualquier función. Obsérvese que, en efecto, NAND/NOT calcula NAND (olvidándonos del primer bit del resultado), NOT (olvidándonos del segundo bit del resultado), y realiza COPY si se toma $y = 1$ y se aplica luego NOT al par de bits resultantes.

La equivalencia entre máquinas de Turing y circuitos booleanos uniformes permite discutir la complejidad computacional en lenguaje de circuitos. Por ejemplo, la clase P consta de aquellos problemas de decisión $f = \{f_n : n = 1,2,\ldots\}$, donde n indica la longitud binaria del dato inicial, solubles mediante circuitos $\{C_n\}_1^\infty$ cuyo tamaño $s(C_n)$ (número de puertas lógicas) está polinómicamente acotado: $s(C_n) \leq p(n)$, donde $p(n)$ es un polinomio. Se dice en este caso que el problema en cuestión tiene *circuitos pequeños*. En la clase NP caen aquellos problemas $f = \{f_n : n = 1,2,\ldots\}$ de decisión tales que existen *circuitos no deterministas* $\{C_{n,m}\}_{n,m}$ pequeños con esta propiedad: $f_n(x) = 1$ si y sólo si existe y, de longitud m polinómica en n, de modo que $C_{n,m}(x,y) = 1$.

El ejemplo SAT ya citado de problema NPC es formulable, en este lenguaje intuitivo de circuitos, como el problema de *satisfacer* un circuito C, esto es, de hallar un dato x tal que $C(x) = 1$.

2.6.1 Puertas lógicas reversibles

Las puertas binarias estudiadas AND y OR son irreversibles, pues pasan de 2 bits a 1 bit. Luego por el principio de Landauer [130], operando a temperatura T, consumen una energía $k_B T \log 2$ por cada bit borrado. Si queremos que nos salga gratis la computación tendremos que utilizar puertas reversibles. Cualquier función $f : x \in \{0,1\}^m \mapsto f(x) \in \{0,1\}^n$ puede extenderse a una función invertible. Por ejemplo, $f : (x,0^n) \in \{0,1\}^{m+n} \mapsto (x, f(x)) \in \{0,1\}^{m+n}$; o también $f_r : (x,y) \in \{0,1\}^{m+n} \mapsto (x, y \oplus f(x)) \in \{0,1\}^{m+n}$.

Hay 4 puertas unarias, dos reversibles (id, NOT) y dos irreversibles ($x \mapsto 0$, $x \mapsto 1$). De las 256 puertas binarias, sólo $4! = 24$ son reversibles. Destaca la puerta CNOT (controlled NOT) o XOR (exclusive OR), definida como $(x,y) \mapsto (x, x \oplus y)$. Deja intacto

[68] A veces se sobrentiende por el contexto la aritmética mod 2, y se escribe simplemente $+$ en lugar de $\oplus$.

el primer bit (bit de control), e invierte el segundo bit (bit blanco) siempre que el de control sea 1 (de ahí CNOT). Es claro que $\mathrm{CNOT}(x,y) = (x, \mathrm{OR}(\mathrm{AND}(\mathrm{NOT}x, y), \mathrm{AND}(x, \mathrm{NOT}y)))$, relación que indica cómo implementar CNOT con las puertas básicas AND, OR y NOT, y FANOUT para desdoblar el x de entrada en (x,x,x), y el y en (y,y). Otra puerta binaria reversible es SWAP: $(x,y) \mapsto (y,x)$.

La acción de las puertas reversibles unarias y binarias es afín. Por eso con este tipo de puertas es imposible reproducir el efecto de puertas n-arias no lineales como la puerta T de Toffoli, o puerta CCNOT (*controlled controlled* NOT), o la puerta F de Fredkin[69] o *intercambiador controlado*.[70] Se definen así:

$$\mathrm{T} : (x,y,z) \mapsto (x,y,z \oplus (xy)),$$

que invierte el tercer bit (blanco) si y sólo si los dos primeros bits (de control) son 1. Nótese que T es la extensión reversible $\mathrm{AND_r}$ de la puerta irreversible AND. Y

$$\mathrm{F} : (x,y,z) \mapsto \begin{cases} (x,y,z) & \text{si } x = 0, \\ (x,z,y) & \text{si } x = 1, \end{cases}$$

que intercambia los bits (blancos) segundo y tercero si el primer bit (de control) es 1.

La puerta ternaria de Toffoli es universal: toda puerta reversible es construible mediante puertas T, siempre que podamos echar mano de ancillae a la entrada e ignorar bits de salida. De igual modo, la puerta ternaria de Fredkin es universal, y también la puerta SHEFFER, definida como $(x,y) \mapsto \neg(x \vee y) = 1 - x - y + xy$ [209].

Puede demostrarse que todo cálculo irreversible puede realizarse también de forma reversible, sin cambio de clase de complejidad P, NP o PSPACE.

2.6.1.1 Cálculo y energía El tiempo y el espacio exigidos por un cálculo al agrandar el argumento son índices de su complejidad. ¿Lo será también la energía consumida en su realización? Sorprendentemente no lo es: en principio es posible calcular sin gasto energético alguno. Pero esto exige que la computación sea reversible. De lo contrario, crece la entropía y esto conlleva una disipación de energía. Por ejemplo, como ya hemos dicho, las puertas ordinarias AND y OR son irreversibles: se entra en ellas con dos bits y se sale con uno sólo, por lo que no hay marcha atrás en su acción. Borran, "machacan" por así decirlo, un bit, y esto supone una pérdida de un bit informativo, es decir, un aumento de la entropía en al menos $k_\mathrm{B} \log 2$.

De aquí el principio de Landauer [130, 19, 173]: cada bit borrado supone un consumo mínimo de energía de $k_\mathrm{B} T \log 2$, siendo T la temperatura media del ambiente. Los computadores ordinarios consumen hoy día mucho más, del orden de 500 veces este mínimo, por cada operación lógica [164]. Es sorprendente que el 5% del consumo energético de los EEUU se lo llevan los ordenadores [213, 214]. Es una carga realmente pesada, que sin duda se agravará, por aumento del número de usuarios, a pesar de que el avance tecnológico lleve a procesadores de menor consumo.

Si no se borra ningún bit (cálculo reversible) el gasto en principio puede ser nulo. Los circuitos reversibles adecuados a este fin se forman con las puertas reversibles antes mencionadas (Toffoli, Fredkin). Y decíamos hace un momento que todo cálculo irreversible puede hacer de forma reversible y con igual eficiencia. Entonces, ¿por qué no calculamos sin gasto de energía?

[69] A Ed Fredkin se debe el interés de Richard Phillips Feynman por la simulación de la física con ordenadores.

[70] En realidad, deberían llamarse puertas de Petri-Toffoli y Petri-Fredkin, pues el primero en descubrir tanto la puerta CNOT, como estas dos puertas ternarias y su universalidad, fue Petri en 1965 [169, 101].

Por el ruido esencialmente. Este introduce errores en los bits, que hay que corregir, lo que se consigue añadiendo bits redundantes que luego hay que borrar para hacer sitio en la memoria donde se ha guardado la información sobre los bits erróneos y su corrección, antes de seguir corrigiendo nuevos bits defectuosos, y en este continuo menester se gasta, como ya sabemos, energía. Podemos pensar en la corrección de errores como una forma de mantener constante la entropía del ordenador, ordenándolo tan pronto como el ruido lo desordena. Es como la acción de un diablillo de Maxwell. Pero este ser tiene una memoria en la que se registran los datos de las medidas que tiene que realizar sobre el sistema para detectar cada error, esto es, para obtener el síndrome del error a corregir y proceder a su limpieza; esa memoria se va cargando y cuando llega a su capacidad límite (que suponemos finita como la de todo ente físico), tiene que borrarla toda, arrojando entropía al exterior, para registrar nuevos síndromes y continuar con su misión correctora. En este proceso, la disminución en la entropía del sistema que supone la corrección de errores se ve más que superada por el desorden producido sobre todo lo que hay (diablillo, medio ambiente y el propio ordenador), de modo que la entropía total crece, de acuerdo con la segunda ley de la termodinámica.

2.7 Otras "máquinas" de calcular

Las máquinas de Turing son puramente digitales y secuenciales. Pero existen ordenadores con arquitectura paralela, calculadoras analógicas, etc. ¿Influye esto sobre las clases de complejidad? No. Respecto de los primeros, sus resultados son reproducibles con ordenadores secuenciales con un factor polinómico en el coste. Y en relación con los cálculos analógicos, que en principio permitirían manejar un continuo de números, el ruido y la precisión finita hace que en la práctica se comporten como si estuvieran discretizados.

Mención aparte merece el uso de moléculas ADN como soporte computacional [2, 3]. Se ha aplicado al problema DIR HAM: dada una colección de N vértices, y un conjunto finito de líneas dirigidas (pares de vértices ordenados), averiguar si, dados dos vértices, existe una sucesión de esas líneas que los conecte entre sí, sin pasar por el mismo vértice intermedio dos veces. Este problema es NPC. Su solución mediante ADN es polinómica en tiempo pero exponencial en espacio. La complejidad total (tiempo más espacio) no ha cambiado. También se ha propuesto este "computador" ADN para atacar el problema SAT [138], y se ha implementado en la práctica [184].

3 Una década de "qubitomanía"

La teoría cuántica de la información, que extiende la teoría clásica, es fruto esencialmente de la década pasada.

Ya hemos dicho que la información tiene naturaleza física. Se imprime en soporte físico (ya sea la pared de la cueva de Altamira, ya sea un disco magneto-óptico), se articula en vibraciones sonoras, hertzianas, etc., no puede transmitirse a velocidad superior a la de la luz en vacío, y está sometida a las leyes naturales, en particular a las reglas cuánticas. Precisamente éstas, a través de su linealidad (con el paso del bit al qubit), enmarañamiento de estados (subsistemas cuya individualidad queda difuminada en el todo), no localidad (naturaleza holística de los estados) y principio de indeterminación (existencia de magnitudes físicas incompatibles) hacen posibles nuevas y poderosas herramientas de transmisión y tratamiento de la información, así como una eficiencia

de cálculo realmente prodigiosa.[71]

El avance ha sido notable en el ámbito de la criptografía (el arte de esconder la información), donde ha proporcionado sistemas absolutamente seguros para la distribución cuántica de claves. La naturaleza misma sale garante de la inexpugnabilidad del secreto: a mayor aleatoriedad, mejor seguridad. No sólo hay un alto interés militar y estratégico en esto. Nuestra sociedad gira cada vez más en torno a la información digital; ingentes cantidades de dinero se mueven virtualmente en transacciones bancarias cuya seguridad se apoya en sistemas de encriptado sobre los que el asedio es constante, e informes confidenciales y números personales de tarjetas de compra viajan por la red expuestos a la piratería organizada, con el consiguiente riesgo de que nuestra intimidad sea violada y nuestra economía sangrada por manos ajenas. De ahí el interés en el desarrollo de un sistema absolutamente seguro de protección de datos.

Irónicamente, los quanta no sólo hacen posible esta protección total, sino que ponen de manifiesto la vulnerabilidad de los criptosistemas basados en la existencia de problemas computacionalmente duros para los ordenadores clásicos, pero que dejan de serlo para los ordenadores cuánticos. Estos se caracterizan por funcionar de acuerdo a las reglas cuánticas y por un paralelismo masivo que permite en principio abordar cálculos que, aun no siendo teóricamente vedados para los ordenadores actuales, exigirían de éstos no sólo un tiempo medido en eones, sino también una memoria que sobrepasaría la capacidad de todo el Universo. El desarrollo de la computación cuántica constituye en este momento uno de los campos más activos y punteros de investigación. No son pocos los problemas técnicos a resolver, relacionados con la extraordinaria fragilidad de la coherencia de los estados cuánticos. Pero al igual que la sociedad usuaria de los mastodónticos ordenadores de finales de los 40, con miles de tubos de vacío y decenas de toneladas de peso, no se imaginaba[72] que medio siglo después cualquier colegial dispondría de máquinas de calcular mucho más ligeras y potentes, somos por naturaleza optimistas (*man muss Optimist sein*, decía Planck) y queremos pensar que el ingenio de los científicos logrará vencer finalmente las dificultades para construir ordenadores cuánticos de potencia adecuada. Con ellos el hombre habrá dado un paso de gigante en el entendimiento de la naturaleza. Si el pasado siglo XX puede llamarse siglo de la información, al siglo de ahora probablemente se le conocerá como el siglo de la tecnología cuántica.[73]

Comparto con muchos otros la creencia en el beneficio mutuo de la simbiosis quanta e información. El propio conocimiento de los fundamentos de la física puede beneficiarse de la teoría de la información [131, 132], y en la física experimental de alta precisión el tratamiento cuántico de la información puede resultar sumamente útil para alejar un tanto las barreras cuánticas en las mediciones, como sin duda hará falta en el análisis de los datos que registre el detector LIGO III de ondas gravitacionales en su tercera fase,[74] por allá al 2008 [176]. Al igual que la fisicalización de la información ha producido sin duda elevados dividendos, es también muy probable que una perspectiva informática nos ayude a entender mejor aspectos oscuros de la física. Preskill [174, 176] ha recogido algunos temas físicos sobre los que la información cuántica podría incidir de modo importante, entre los que destacan el enredo y posibles estados colectivos asociados en materia condensada, y la gravedad cuántica, con su principio holográfico que, al codificar toda la información en la frontera del sistema, parece un

[71] En esta parte y en la subsección sobre criptografía cuántica se usa bastante material de la referencia [86].

[72] Decía en 1943 Thomas Watson, presidente de IBM: *I think there is a world market for maybe five computers*.

[73] *Man muss "Quantumist" sein*.

[74] LIGO, acrónimo de *Laser Interferometer Gravitational Wave Observatory*.

desafío a la localidad de las leyes físicas.

3.1 Bits versus qubits

Si el bit, o c-bit, es la unidad de información clásica, la unidad de información cuántica es el *qubit* (mejor fuera escribir *q-bit*, por bit cuántico),[75] la información almacenable en un sistema cuántico cuyo espacio de estados es 2-dimensional (qubit). Por ejemplo, un spin 1/2, la polarización de un fotón, átomos con 2 estados relevantes, etc., son qubits.

Toda información clásica es codificable en binario. Por ejemplo, con 8 bits ($2^8 = 256$ posibilidades) tenemos de sobras para asignar un número en binario a cada signo del teclado y así digitalizar cualquier texto, por ejemplo, el Quijote, representándolo por una cadena de bits o por una cadena de condensadores cargados/descargados. Midiendo la carga de éstos podemos reconstruir la obra de Cervantes.

Con qubits haríamos lo mismo, pero con un cuidado extremo a la hora de leer. Porque si por ejemplo los estados base $|0\rangle, |1\rangle$ de los qubits con que salvamos el Quijote son $|+\rangle_z$ y $|-\rangle_z$, pero luego a la hora de leer nos equivocamos y medimos polarizaciones $|+\rangle_x$ y $|-\rangle_x$, los resultados obtenidos serán aleatorios, el Quijote será irreconocible, y lo que es peor, no habrá manera de deshacer el entuerto, siendo preciso codificar de nuevo la genial novela. Por tanto, los bits son robustos, y los qubits sumamente frágiles ante cualquier intento de inspección. La obtención de información sobre un sistema cuántico generalmente lo perturba.

Otra distinción importante entre los elementos de información clásicos y cuánticos está en el proceso de copiado. Cualquier estado clásico de un sistema es copiable; estamos hartos de verlo (copias de un modelo prototipo, de una efigie, de una fotografía, de un escrito, de un fichero digital, etc.). Supongamos, sin embargo, que queremos copiar un estado cuántico. Puede ocurrir que conozcamos dicho estado (por ejemplo, que es un electrón moviéndose con tal momento y polarizado en tal dirección) y entonces esta información basta para preparar otro sistema en ese mismo estado. Si por contra desconocemos el estado a copiar, estamos perdidos, pues con el único ejemplar que nos dan ningún conjunto de medidas compatibles (salvo las que dejaran el estado incólume, y que evidentemente ignoramos cuáles son) puede revelarnos toda la información necesaria para determinar el estado y así poderlo reproducir. En el caso clásico, por contra, podemos medir sobre el sistema cuanto necesitemos para su copia macroscópica, sin deterioro apreciable del estado a reproducir.

La imposibilidad de clonación cuántica, que discutiremos a continuación, tiene virtudes esenciales para proteger la información (criptografía), o para evitar la falsificación de moneda (billetes cuánticos).

Hay otras diferencias más profundas y con mayor impacto potencial tecnológico. El número de estados codificables con N bits es 2^N, y cada uno queda fijado a través de sólo un número binario. Pero el número de estados codificables con N qubits es infinito, a saber, cualquier combinación lineal de los 2^N estados base, y por tanto, su especificación requiere conocer 2^N amplitudes. Para $N = 300$, este número es del orden del número de grados de libertad del Universo visible. Mientras la capacidad de memoria de un procesador clásico es linealmente proporcional a su tamaño, la de un procesador cuántico (registro de qubits) crece exponencialmente con N. Esto es un índice de la complejidad de los qubits. Luego es de esperar que un ordenador que

[75] Denominación propuesta por Benjamin Schumacher en 1995.

opere sobre qubits podrá en principio realizar hazañas impensables para un ordenador clásico.

La sutileza del enredo, la posibilidad de esconder la información difuminándola de modo que ninguna medición local pueda revelarla, ofrece también posibilidades nuevas a la información. Mientras que un libro clásico puede leerse página tras página, línea tras línea, palabra tras palabra, si el libro fuera cuántico, lo más probable es que la información conseguida con ese tipo de lectura fuera escasa, al residir en correlaciones entre todas sus páginas. El enredo produce correlaciones no locales sin análogo clásico, que no pueden crearse mediante operaciones locales y comunicaciones clásicas entre las partes. Esta peculiaridad sirve para proteger la información almacenada en sistemas enredados ante ataques localizados. Podríamos arrancar una página del libro cuántico sin afectar a su comprensión. No es de extrañar que el enredo sea el mayor responsable de las ventajas casi mágicas de la comunicación y computación cuánticas. En el enredo se fundamentan algunos protocolos cuánticos, unos de aplicación en criptografía y corrección de errores para la computación cuántica, y otros sin análogo clásico, así como la codificación cuántica densa, y la teleportación cuántica.

Si bien la polarización de un haz de luz proporciona una realización clásica de un qubit, es claro que un sistema de dos o más qubits carece de realización óptica, pues sus estados enredados no pueden simularse clásicamente.

Finalmente, hay otros aspectos importantes y aplicaciones en las que, por razones de espacio y tiempo, no voy a entrar: cuantificación y purificación del enredo [39], computación cuántica topológica [165], computadores cuánticos tolerantes a fallos [173], sincronización cuántica de relojes [54, 116], y juegos cuánticos [154].

3.1.1 Imposibilidad de clonación cuántica

No es posible clonar de forma exacta estados cuánticos no ortogonales [215, 67]. Seré más preciso:

1/ La linealidad de la MQ exige que no existan dispositivos que puedan clonar estados cuánticos desconocidos y arbitrarios.

2/ La unitariedad de la evolución en MQ implica que no es posible clonar estados cuánticos distintos y no ortogonales.

Aunque no sabemos cómo clonar un estado desconocido $a|0\rangle + b|1\rangle$, sí es posible conseguir estados de la forma $a|00\ldots0\rangle + b|11\ldots1\rangle$. Si Φ es una máquina lineal capaz de clonar estados $|0\rangle$ y $|1\rangle$ (fácil, pues de estos estados conocemos su preparación), basta aplicar dicha Φ al estado $a|0\rangle + b|1\rangle$.

3.1.2 Registros de qubits y puertas lógicas cuánticas

El espacio de Hilbert de un qubit es $\mathbb{C}^2$. El qubit, además de poder estar en dos estados base $|0\rangle, |1\rangle$, puede presentarse también en una infinidad de otros estados dados por superposición lineal coherente $\alpha|0\rangle + \beta|1\rangle$. El espacio de Hilbert de n qubits es $\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}$, y sus vectores base naturales son $|0\rangle \otimes \ldots \otimes |0\rangle = |0\ldots0\rangle$, $|0\rangle \otimes \ldots \otimes |1\rangle = |0\ldots1\rangle$,..., $|1\rangle \otimes \ldots \otimes |1\rangle = |1\ldots1\rangle$. Supondremos para esta base, también conocida como base computacional, la ordenación lexicográfica. Cuando convenga, escribiremos abreviadamente $|x\rangle$ para indicar $|x_{n-1}\ldots x_0\rangle$, con $x = 2^{n-1}x_{n-1} + \ldots + 2x_1 + x_0$.

Una *puerta lógica cuántica* sobre una colección o *registro cuántico* de k qubits es cualquier operador unitario en el espacio de Hilbert $\mathbb{C}^{2^k}$ asociado [65, 4, 88]. Por ejemplo, aparte de la identidad, tenemos sobre 1 qubit las puertas 1-arias X (o U_{NOT}), Y, Z, dadas, en la base natural $\{|0\rangle, |1\rangle\}$, por las matrices σ_j de Pauli: $U_{\text{NOT}} := X :=$

σ_1, $Y := -i\sigma_2$, $Z := \sigma_3$. Las puertas monarias son fáciles de implementar (por ejemplo, sobre fotones polarizados, con láminas $\frac{1}{2}\lambda, \frac{1}{4}\lambda$).

En los ordenadores clásicos, las puertas lógicas que procesan la información son elementos no lineales basados en la tecnología de los semiconductores, como los transistores, verdaderas "neuronas"del computador; en los ordenadores cuánticos o "*qomputadores*", las puertas lógicas se consiguen con interacciones no lineales entre las magnitudes cuánticas.

El elemento básico de un qomputador es la puerta sobre 2 qubits conocida como CNOT o XOR: $(x,y) \mapsto (x, x \oplus y)$.[76] Cuando el dato inicial x es superposición lineal de los vectores base 0, 1, entonces el resultado $(x, x \oplus y)$ está enredado. Esta puerta es representable por la matriz $U_{\text{CNOT}} = |0\rangle\langle 0| \otimes 1 + |1\rangle\langle 1| \otimes U_{\text{NOT}}$. La implementación en laboratorio de puertas 2-arias es difícil, pues requiere poner en interacción fuerte y controlada dos qubits espacialmente separados. Una brillante manera de conseguirlo con iones fríos en una trampa lineal se debe a Cirac y Zoller [56].

La puerta T de Toffoli, o puerta CCNOT o C^2NOT (controlled controlled NOT) actúa sobre registros de 3 qubits, y viene representada por el operador unitario U_{T} dado por $U_{\text{T}} = |0\rangle\langle 0| \otimes 1 \otimes 1 + |1\rangle\langle 1| \otimes U_{\text{CNOT}}$. El intercambiador controlado o puerta F de Fredkin actúa como el siguiente operador unitario U_{F} sobre registros de 3 qubits: $U_{\text{F}} = |0\rangle\langle 0| \otimes 1 \otimes 1 + |1\rangle\langle 1| \otimes U_{\text{SWAP}}$, donde U_{SWAP} intercambia los bits ($U_{\text{SWAP}}|a\rangle \otimes |b\rangle := |b\rangle \otimes |a\rangle$).

No hace falta decir que estas puertas lineales unitarias no sólo actúan sobre los estados bases, sino también sobre cualquier combinación lineal de estos.

Todas las puertas clásicas tienen su contrapartida cuántica. Por eso toda computación clásica puede ser hecha también en un ordenador cuántico. Pero hay puertas cuánticas exóticas, sin análogo clásico.

Una puerta monaria no clásica es $\sqrt{\text{NOT}}$, que, como su nombre indica, aplicada dos veces equivale a NOT. Es la puerta puramente cuántica que describe el efecto sobre los estados base de sistema atómico de 2 niveles de un pulso láser cuya duración es la mitad de la necesaria para excitar o desexcitar, y que por tanto deja al átomo en un estado indefinido, superposición de los dos estados base con amplitudes de igual módulo. Viene dada por $U_{\sqrt{\text{NOT}}} = 2^{-1/2} e^{-i\pi/4}(1 + i\sigma_1)$.

Otra puerta sin análogo clásico es la puerta Hadamard H sobre 1 qubit, dada por $U_{\text{H}} = 2^{-1/2}(\sigma_1 + \sigma_3) = iR(\mathbf{n}, \pi)$, donde $\mathbf{n} := 2^{-1/2}(\mathbf{e}_1 + \mathbf{e}_3)$. Su extensión tensorial a n qubits, aplicada al estado $|0\ldots0\rangle$, produce la combinación lineal $2^{-n/2}\sum_{x=0}^{2^n-1}|x\rangle$ de todos los estados base con igual amplitud, y se conoce como puerta de Walsh-Hadamard. Su efecto sobre el estado base $|x\rangle$ es la combinación lineal $\sum_y (-1)^{x\cdot y}|y\rangle$, donde $x \cdot y := \sum_j x_j y_j \bmod 2$.

3.2 Máquinas de Turing cuánticas y circuitos cuánticos

Se debe a Deutsch [64] el concepto general de máquina cuántica de Turing (MTQ). Con anterioridad, Benioff [14, 15, 16] había considerado los procesos cuánticos como método para construir MTs reversibles, y luego Feynman [79, 80] había propuesto un "simulador cuántico universal" que carecía de la versatilidad esperada de un qomputador.

Una versión moderna [32, 33] de lo que es una MTQ es la siguiente. Una MTQ M es una terna $T = (Q, A, \delta)$ formada por: 1/ Un conjunto finito Q de estados de

[76] En general, si U es una puerta n-aria, se define la puerta CU (controlled U) como $CU : |x\rangle|y\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^{2^n} \mapsto |x\rangle(\delta_{0,x}|y\rangle + \delta_{1,x}U|y\rangle)$.

la unidad de control de la máquina, con dos estados especiales: q_{in}, estado inicial o de arranque, y $q_{\text{fin}} \neq q_{\text{in}}$, un estado final. 2/ Un *alfabeto* finito A de símbolos, entre los que está el símbolo "blanco" $\sqcup$. Pensemos en una *cinta* lineal (potencialmente infinita en ambos sentidos) con celdas, en cada una de las cuales está representado alguno de los símbolos en $A - \{\sqcup\}$, o bien está vacía (símbolo $\sqcup$). 3/ Una función de transición cuántica $\delta : Q \times A \times Q \times A \times M \to \tilde{\mathbb{C}}_{[0,1]}$, con $M := \{\leftarrow, \rightarrow\}$, y donde $\tilde{\mathbb{C}}_{[0,1]}$ es el subconjunto de $\mathbb{C}$ formado por los números complejos z de módulo ≤ 1 para los que existe un algoritmo determinista que calcula Re z, Im z, con precisión $\leq 2^{-n}$ en tiempo polinómico en n.[77]

La MTQ M tiene una cinta doblemente infinita, etiquetada por $\mathbb{Z}$, y una *cabeza* o cursor de lectura/escritura que se mueve sobre esa cinta. Una configuración o descripción instantánea c de M consiste en dar el contenido total de la cinta, la posición del cursor, y el estado de la unidad de control. El conjunto C_M de configuraciones subtiende un espacio de Hilbert $\mathcal{H}_M$ asociado a M, del que es C_M una base ortonormal. Nótese que tras cada paso temporal una configuración c da lugar, en general, a una superposición lineal $\sum_i \alpha_i c_i$ de configuraciones, donde c_i es una de las configuraciones alcanzables desde c en una actuación de M, y α_i es la correspondiente amplitud de probabilidad $\delta(q, \sigma, q_i, \sigma_i, m_i)$. Sólo un número finito de configuraciones interviene en esas superposiciones lineales. Se exige de M que su acción sobre $\mathcal{H}_M$ sea unitaria, como corresponde a la evolución temporal de todo sistema cuántico cerrado.

También en el caso cuántico existen MTQs universales, que simulan eficientemente el efecto de cualquier MTQ sobre un dato inicial arbitrario [64, 217, 32, 33].

Del mismo modo que una MTD equivale a una familia de circuitos booleanos uniformes, un teorema fundamental de Yao [217] nos permite reemplazar una MTQ por una familia equivalente de circuitos cuánticos uniformes, lo que indudablemente facilita la descripción y análisis de la computación cuántica.

Los circuitos cuánticos [65] son circuitos lógicos (grafos acíclicos y dirigidos), en el que los nodos son *puertas cuánticas* (operadores unitarios en subespacios de k qubits), el dato de entrada es un vector base inicial de un espacio de n qubits, y el resultado es la cadena de bits clásicos que resulta al medir sobre el estado final del sistema de n qubits [4].

Es fácil probar que dada una función clásica f de m bits a n bits, calculable mediante un circuito clásico C_{c} booleano, existe un circuito cuántico C_{q} que calcula la operación unitaria sobre $m+n$ qubits $|i, j\rangle \mapsto |i, f(i) \oplus j\rangle$, con un número $\#C_{\text{q}}$ de puertas que depende linealmente de $\#C_{\text{c}}$. En consecuencia, todo cálculo clásico puede hacerse también cuánticamente, y con igual o mejor eficacia [4]; es decir, $\mathsf{P} \subseteq \mathsf{QP}$, donde QP es la clase de problemas solubles en tiempo polinómico mediante un circuito cuántico [65]. Fue toda una revelación el descubrimiento de que el problema FACT de la factorización es de clase QP [191]. Si FACT resulta ser de complejidad esencialmente exponencial, tendríamos un ejemplo de mejora exponencial en la eficiencia de la computación cuántica sobre la clásica. Y no cabe esperar más: fijada una precisión, cualquier circuito cuántico C_{q} es simulable por otro clásico C_{c} con un número de puertas $\#C_{\text{c}}$ que crece a lo sumo exponencialmente con $\#C_{\text{q}}$ [57].

3.2.1 Puertas cuánticas universales

Un conjunto de puertas cuánticas dícese *universal* si el grupo unitario que engendran (o subgrupo unitario minimal que lo contiene) en el espacio de Hilbert de n qubits es

[77] La razón de restringirse a $\tilde{\mathbb{C}}$ es para evitar que se cuele alguna amplitud incomputable.

denso en U(2^n) bajo la topología uniforme, para todo n. Cuando cualquier elemento de U(2^n) puede simularse por la acción de un número finito de puertas del conjunto dado, se dice de éste que es *exactamente* universal.

Es fácil probar que toda matriz unitaria $k \times k$ es producto de $\frac{1}{2}k(k-1)$ matrices unitarias cada de las cuales actúa sobre un subespacio 2-dimensional subtendido por 2 vectores de la base [178]. Por eso basta considerar la universalidad sobre pares de qubits.

Las puertas 1-arias, junto con la binaria CNOT, forman un conjunto (infinito) exactamente universal [70, 196, 139, 10]. Cualquier puerta binaria entre un par de qubits en un sistema de n qubits se puede expresar mediante $O(n^2)$ puertas unarias y CNOTs. Combinado con lo anterior, se desprende que cualquier puerta unitaria sobre N qubits se puede escribir como producto de $O(4^n n^2)$ puertas unarias y CNOTs. De hecho, basta con $O(4^n n)$ puertas de esas puertas [125].

El primer conjunto discreto universal conocido se debe a Deutsch, en su trabajo seminal sobre computadores cuánticos [64, 75]. Consta de un conjunto de cuatro matrices de U(2) y sus inversas, dependientes de un ángulo múltiplo irracional de π. Luego se han conocido otros conjuntos más simples. Por ejemplo, el conjunto $\{$H,C$V\}$ formado por la puerta 1-aria de Hadamard y la puerta 2-aria CV, donde $V := |0\rangle\langle 0| + \mathrm{i}|1\rangle\langle 1|$ (puerta fase), y el conjunto $\{$H,W,CNOT$\}$, con $U_W := \mathrm{e}^{\mathrm{i}\pi/8}(\mathrm{e}^{-\mathrm{i}\pi/8}|0\rangle\langle 0| + \mathrm{e}^{\mathrm{i}\pi/8}|1\rangle\langle 1|)$ la llamada puerta $\pi/8$, son universales [123, 57, 44].

Una puerta cuántica sobre 3 qubits, universal por sí sola, es la D de Deutch [65], del tipo rotación (controlada)^2: $U_{\mathrm{D}} := |0\rangle\langle 0| \otimes 1 \otimes 1 + |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes 1 + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes S(\tau)$, donde $S(\tau) := \mathrm{i}\cos\frac{1}{2}\pi\tau(|0\rangle\langle 0| + |1\rangle\langle 1|) + \mathrm{sen}\frac{1}{2}\pi\tau(|0\rangle\langle 1| + |1\rangle\langle 0|)$, con τ un irracional fijo y arbitrario. El conjunto $\{$H,W^2,CNOT, T$\}$ es también universal.

La aproximación en ε de puertas genéricas sobre n qubits a través de un conjunto universal discreto es muy poco eficiente, requiriendo un número de puertas N de este conjunto que crece exponencialmente con n, como se desprende de estos hechos [164, 88]: 1/ El teorema de Solovay-Kitaev (la aproximación en δ de una matriz arbitraria en U(2) a través del conjunto $\{$H,$W\}$ puede hacerse con $O(\log_2^c \delta^{-1})$ factores, siendo $c \approx 2$). 2/ Cualquier matriz en U(n) puede expresarse como producto de $O(n4^n)$ de puertas monarias y CNOTs. Y 3/ Si U_j son operadores unitarios que aproximan a U_j, el error $||U_1 \ldots U_r - \bar{U}_1 \ldots \bar{U}_r|| \leq \sum_i ||U_i - \bar{U}_i||$. Por tanto, $N = O(n4^n \log_2^c(n4^n/\varepsilon))$.

3.3 Codificación cuántica y teorema de Schumacher

Sea ahora un "alfabeto" $A := \{|\phi_i\rangle, p_i\}_{i=1}^{|A|}$ consistente en un conjunto de estados cuánticos puros distintos (no necesariamente ortogonales) y sus probabilidades ($\sum_i p_i = 1$). Le asignamos el operador densidad $\rho(A) := \sum_i p_i |\phi_i\rangle\langle\phi_i|$. Un mensaje emitido por una fuente de señales cuánticas es una secuencia $\phi_{i_1 \ldots i_n} := |\phi_{i_1}\rangle|\phi_{i_2}\rangle \ldots |\phi_{i_n}\rangle$ de "letras" o "símbolos", cada uno producido con probabilidad p_{i_j} independientemente de los otros. La colección de mensajes de n símbolos es representable por el operador densidad $\rho^{\otimes n}$, que vive en un espacio de Hilbert de dimensión máxima $|A|^n = 2^{n\log_2|A|}$. Surge naturalmente de nuevo la cuestión de si es posible comprimir la información contenida en $\rho^{\otimes n}$. Y la respuesta, hallada por Schumacher [187], es similar a la del primer teorema de Shannon: asintóticamente ($n \gg 1$) el estado $\rho^{\otimes n}$ es comprimible, con *fidelidad*[78] F (probabilidad de que el estado descodificado coincida con el estado anterior a la codi-

[78] La fidelidad (o probabilidad de transición de Uhlmann [206]) entre dos estados ρ, ρ' se define como $F(\rho, \rho') := (\mathrm{Tr}\sqrt{\sqrt{\rho}\rho'\sqrt{\rho}})^2$, y mide el grado de parecido entre ambos. Se demuestra que F es el máximo de $|\langle\phi|\phi'\rangle|^2$ sobre todas las purificaciones ϕ, ϕ' de ρ, ρ' [113]. Es simétrica: $F(\rho, \rho') = F(\rho', \rho)$.

ficación) arbitrariamente cercana a 1, a un estado en un espacio de Hilbert de dimensión $2^{nS(\rho)}$, donde $S(\rho) := -\mathrm{Tr}(\rho \log_2 \rho)$ es la entropía de von Neumann de un estado cuántico normal ρ.[79] En otras palabras, es comprimible a $nS(\rho)$ qubits. Luego $S(\rho)$ puede interpretarse como el número medio de qubits de información cuántica esencial por letra del alfabeto. Este resultado de compresión cuántica es también óptimo.

La demostración sigue la pauta de la del teorema clásico [187, 117, 173].

3.3.1 Información de Holevo

Si el alfabeto $A := \{\rho_i, p_i\}_{i=1}^{|A|}$ consiste en estados mezcla, el problema de la compresibilidad de los mensajes se complica. Para medir ésta adecuadamente, la entropía von Neumann $S(\rho := \sum_i p_i \rho_i)$ debe dejar paso a otro concepto más general, la llamada *información de Holevo* del alfabeto o colectivo $A := \{\rho_i, p_i\}_{i=1}^{|A|}$ [136, 104, 173]: $\chi(A) := S(\rho) - \sum_i p_i S(\rho_i)$. La información de Holevo se asemeja a la información mutua clásica; del mismo modo que $I(X:Y)$ indica cómo se reduce la entropía de X cuando se conoce Y, $\chi(A)$ representa la reducción de la información sobre ρ dada por la entropía $S(\rho)$ cuando se conoce el método de preparación del estado $\rho = \sum_i p_i \rho_i$.[80]

No es difícil ver que, suponiendo mutuamente ortogonales los estados ρ_i del alfabeto, esto es, $\mathrm{Tr}(\rho_i \rho_j) = 0$ para $i \neq j$, el estado $\rho^{\otimes n}$ es asintóticamente $(n \gg 1)$ comprimible a un estado de $n\chi(A)$ qubits, con fidelidad tendiendo a 1. Además, este resultado es óptimo.

Cuando los estados no son ortogonales, los resultados son parciales: se sabe que no existe asintóticamente una compresión fiel por debajo de $\chi(A)$ por letra del alfabeto, pero sigue abierto el problema de si una compresión de $\chi(A)$ qubits/letra es o no es accesible en el límite $n \to \infty$.

3.4 Capacidades de un canal cuántico

De un canal cuántico de transmisión podemos considerar su capacidad C para transmitir datos clásicos, su capacidad Q para transmitir con exactitud estados cuánticos, y sus capacidades $Q_{1,2}$ mixtas para transmitir estados cuánticos, también intactos, pero con la asistencia de un canal clásico paralelo entre emisor y receptor.

Dado un canal cuántico $\mathcal{R}$, en general ruidoso, el segundo teorema de Shannon sugiere definiciones asintóticas precisas de las capacidades clásica $C(\mathcal{R})$ y cuántica $Q(\mathcal{R})$ [29]. Según que los procesos de (des)codificación sean clásicos o cuánticos, se pueden distinguir hasta cuatro tipos especiales de capacidades clásicas: $C_{\mathrm{cc}}(\mathcal{R})$, $C_{\mathrm{cq}}(\mathcal{R})$, $C_{\mathrm{qc}}(\mathcal{R})$, $C_{\mathrm{qq}}(\mathcal{R}) = C(\mathcal{R})$. Es claro que $C_{\mathrm{cc}} \leq \{C_{\mathrm{cq}}, C_{\mathrm{qc}}\} \leq C_{\mathrm{qq}}$.

Las capacidades cuánticas asistidas $Q_{1,2}(\mathcal{R})$ se definen de modo análogo a $Q(\mathcal{R})$, pero con un protocolo interactivo de codificación-descodificación que puede incluir operaciones locales arbitrarias a la entrada y a la salida, y recurrir a un canal clásico

[79] La entropía de von Neumann es la compañera cuántica de la de Shannon. Tiene la entropía de von Neumann conocidas propiedades de concavidad, subaditividad fuerte y triangularidad [203, 90, 91]. Las dos primeras se dan también en la teoría clásica de la información. Pero la tercera es peculiar; mientras en la teoría de Shannon la entropía de un sistema compuesto no es nunca menor que la de cualquiera de sus partes (el todo contiene más información que una parte), cuánticamente no es así: los estados EPR (Einstein-Podolsky-Rosen *à la* Bohm) $2^{-1/2}(|aa'\rangle + |bb'\rangle)$, donde a, b y a', b' son sendos pares ortornormales, proporcionan un contraejemplo manifiesto [73, 37].

[80] La información de Holevo tiene estas propiedades: 1/ $\chi(A) \geq 0$. 2/ $\chi(A) = S(A)$ cuando todos los estados ρ_i son puros. 3/ $\chi(A)$ es cota superior a la información clásica $\mathrm{Acc}(A)$ extraible del conjunto A: $\mathrm{Acc}(A) \leq \chi(A)$ (*cota de Holevo*). Esta cota superior es accesible si los estados ρ_i que componen ρ son ortogonales entre sí.

de comunicación en dirección de entrada a salida (subíndice 1), o en ambos sentidos (subíndice 2).

Se puede demostrar que $Q = Q_1$ [28, 29]; es decir, el envío de mensajes clásicos desde origen a destino no aumenta la capacidad del canal. Por otro lado, es evidente que $Q \leq Q_2$, y el uso de estados ortogonales para transmitir cbits lleva a $Q \leq C$. Pero se ignora si puede o no ocurrir que $C < Q_2$, o que $C_{cc} < Q$. Se conocen canales para los que $Q < Q_2$, y otros para los que $Q_2 < C$.

Por su definición asintótica, no sorprende que el cálculo de estas capacidades sea difícil en general. Se conocen en algunos casos, como en el *canal de borrado cuántico*, en el que hay una probabilidad p de que el canal sustituya el qubit por un símbolo de borrado ortogonal a los estados $\{|0\rangle, |1\rangle\}$, y la probabilidad complementaria $1-p$ de que el qubit pase intacto. Para este canal $C = Q_2 = 1-p$, las cuatro capacidades clásicas coinciden, y $Q = \max\{0, 1-2p\}$ [27, 29].[81] Otro canal sencillo interesante es el *canal despolarizador*, que mantiene intacto el qubit con probabilidad $1-p$ y lo cambia por otro qubit aleatorio en el resto de los casos; se sabe que las capacidades de este canal satisfacen [27, 29]: i/ $C, Q, Q_2 > 0$ para $q < 0.25408$, ii/ $Q = 0, C, Q_2 > 0$ si $\frac{1}{3} < q < \frac{2}{3}$, iii/ $Q = Q_2 = 0, C > 0$ si $\frac{2}{3} \leq q < 1$, iv/ $C = Q = Q_2 = 0$ si $q = 1$.

A diferencia del caso clásico, en el que la capacidad puede calcularse maximizando la información mutua entre salida y entrada en un solo uso del canal, las capacidades, clásica o cuánticas, de los canales cuánticos, que contemplan la posibilidad de codificar enmarañando varios estados de entrada sucesivos, y descodificar con mediciones conjuntas sobre varios estados de salida, no permiten, por lo general, un cálculo similar. Sin embargo, en el caso de C_{cq}, se sabe que $C_{cq}(\mathcal{R}) = \sup_\rho \chi(\mathcal{R}(\rho))$ [29]. Esta información ha permitido ver que hay canales cuánticos cuya capacidad clásica C_{cq} con codificación clásica y descodificación cuántica sobrepasa a su capacidad C_{cc} correspondiente a la información mutua máxima que puede enviarse con un solo uso del canal.

Finalmente, mediante enredo previo entre emisor y receptor se mejora la capacidad de transmisión. Sean C_E, Q_E las capacidades clásica y cuántica de un canal cuántico con asistencia de enredo. Consecuencia directa de la codificación densa y la teleportación cuántica que luego describiremos son la relación $C_E = 2C$ para canales cuánticos sin ruido, y la relación $Q \leq Q_E = \frac{1}{2}C_E$ para todo canal cuántico [30]. La presencia de ruido hace que la mejora por entrelazamiento que experimenta la capacidad clásica pueda incluso ser muy superior.

3.5 Corrección cuántica de errores

No procede imitar sin más en el caso cuántico los métodos clásicos de corrección de errores, pues el mero hecho de tratar de ver qué qubits se han visto afectados de error daña irremediablemente la información. Ni podemos tampoco hacer ristras de estados cuánticos iguales, pues la linealidad prohíbe la clonación de estados desconocidos y arbitrarios. De ahí el pesimismo inicial sobre el funcionamiento de un computador cuántico [207, 133]. ¿Qué hacer? En 1995 Shor [192] ofreció afortunadamente una primera solución, mostrando un sistema de codificación (de 9:1 bits) capaz de detectar y corregir un bit erróneo arbitrario. Pronto se hallaron otros códigos más simples, como el 7:1 de [197, 198, 51], y el 5:1 de [28].[82] No podemos hacer ni mínima justicia a todas las contribuciones notables que se han publicado en este último lustro sobre

[81] En particular, $Q = 0$ si $p \geq 1/2$; de no ser así, se puede argüir que la clonación cuántica sería posible.

[82] Se ha implementado ya el 5:1 con tecnología RMN sobre moléculas de ácido transcrotónico marcado con ^{13}C, sistema en el que los 5 qubits son los 4 núcleos ^{13}C, y el spin del grupo metilo [126].

este asunto. Es un campo en pleno desarrollo, que, tal como ocurriera con los códigos clásicos, también ha encontrado conexión inesperada con las matemáticas puras [193].

La idea subyacente es esconder la información en subespacios de $\mathbb{C}^{2^n}$ con el fin de protegerla contra la descoherencia y los errores que afectan sólo a unos pocos qubits. Para ello, si nuestro sistema es de k qubits (llamados "lógicos"), un código cuántico corrector de errores (CQCE) codifica sus estados mediante una inyección lineal isométrica $\pi : \mathbb{C}^{2^k} \hookrightarrow \mathbb{C}^{2^n}$, donde $n > k$. El subespacio imagen de π lo denotaremos por $\mathcal{Q}$, y sus elementos se llaman estados (o palabras) código. Los $n-k$ qubits adicionales auxilian en la tarea de proteger la información. La aplicación π debe enmascarar la información deslocalizándola, con el fin de que los errores (que generalmente se producen de forma localizada sobre uno o varios, aunque pocos, qubits) la alteren en nada o lo menos posible [173, 199, 4].

Un sistema de n qubits, en un estado inicial puro ψ, no está absolutamente aislado, y tras interaccionar con el medio ambiente en estado a_{in}, sufre una transformación del tipo $\psi \otimes a_{\text{in}} \mapsto \sum_r (E_r \psi) \otimes a_r$, donde los operadores $E_r, 0 \leq r \leq 2^{2n}-1$, son los operadores de Pauli (elementos del conjunto $\mathcal{P}^{(n)} := \{1, X, Y, Z\}^{\otimes n}$), y los estados a_r del ambiente no son necesariamente ortogonales ni normalizados. Llamando *peso* de un elemento de $\mathcal{P}^{(n)}$ al número de factores tensoriales no triviales que tiene, si ψ es un estado código cada término $(E_r\psi) \otimes a_r$ representa generalmente un componente con un número de errores igual al peso de E_r.

Dada una colección de errores $\mathcal{E} \subset \mathcal{P}^{(n)}$ formada por todos los operadores de Pauli de peso $\leq t$, de un CQCE capaz de corregir todos los errores en $\mathcal{E}$ dícese que enmienda hasta t errores. Para ello es necesario y suficiente que, dada una base ortonormal cualquiera $\{|\bar{i}\rangle\}$ del subespacio código $\mathcal{Q}$ se cumpla $\langle \bar{j}|E_s^\dagger E_r|\bar{i}\rangle = m_{sr}\delta_{ji}$, con m una matriz autoadjunta arbitraria, y $E_{r,s} \in \mathcal{E}$. Esta condición expresa algo natural: 1/ que dadas dos palabras código ortogonales $|\bar{i}\rangle, |\bar{j}\rangle$, los conjuntos corruptos $E_r|\bar{i}\rangle, E_s|\bar{j}\rangle$ deben ser también ortogonales (de lo contrario se perdería la distinguibilidad perfecta de dichas palabras), y 2/ que $\langle \bar{i}|E_s^\dagger E_r|\bar{i}\rangle$ no puede depender de $|\bar{i}\rangle$ (de lo contrario la detección de un error daría información sobre el estado código, con su consiguiente perturbación). Si $m = \text{id}$, el código se llama *no degenerado*, y los subespacios de error $E_r\mathcal{Q}, 1 \neq E_r \in \mathcal{E}$ son ortogonales al subespacio código $\mathcal{Q}$ y perpendiculares entre sí; basta en este caso hacer una medida (posible por la citada perpendicularidad) que determine en qué subespacio se encuentra el (sistema de n qubits)$\otimes$ambiente, digamos con el resultado $(E_r\psi) \otimes a_r$, y luego aplicar al estado resultante del sistema el operador unitario $E_r^\dagger$, para recobrar al estado ψ liberado de su error. En el caso degenerado, un síndrome de error no singulariza a éste, y la estrategia de recuperación es algo más complicada.

La *distancia* d de un CQCE se define como el menor peso de un operador de Pauli tal que $\langle \bar{j}|E|\bar{i}\rangle \neq c_E\delta_{ji}$. En notacion análoga a la de los CCCEs, escribiremos $[[n,k,d]]_2$ para denotar un CQCE binario (es decir, con qubits), de parámetros n, k, d. Es claro que un código $[[n,k,d]]_2$ permite corregir $t := \lfloor (d-1)/2 \rfloor$ errores.

Existen también cotas para los CQCEs $[[n,k,d]]_2$ similares a las mencionadas para los CCCEs [76, 173]. En particular, la cota asintótica cuántica de Gilbert-Varshamov: $R \geq 1 - H_2(2t/n) - (2t/n)\log_2 3, \quad n \gg 1$. Esta cota permite probar la existencia de CQCEs asintóticamente buenos. Cuestión diferente (y abierta) es su construcción explícita.

3.5.1 Ejemplo de CQCE: códigos CSS

Sean $\mathcal{C}_1$ un CCCE lineal y binario del tipo $[n, k_1, d_1]_2$, y $\mathcal{C}_2$ un subcódigo $[n, k_2, d_2]_2$ de $\mathcal{C}_1$, con $k_2 < k_1$. Sea $\mathcal{C} := \mathcal{C}_1/\mathcal{C}_2$ el espacio cociente, de dimensión $2^{k_1-k_2}$.

Definamos un CQCE $\mathcal{Q} \subset \mathbb{C}^{2^n}$, de dimensión 2^k, con $k = k_1 - k_2$, subtendido por los vectores

$$|\overline{w}\rangle := 2^{-k_2/2} \sum_{v \in \mathcal{C}_2} |w+v\rangle, \quad w \in \mathcal{C}$$

Nótese que esta definición no depende del representante w elegido, y que los vectores $|\overline{w}\rangle$ así construidos forman un sistema ortonormal.

Se demuestra que este código cuántico reconoce y corrige $t_b := \lfloor (d_1-1)/2 \rfloor$ errores de inversión de bit, y $t_f := \lfloor (d_2^\perp - 1)/2 \rfloor$ errores de inversión de fase, donde $d_2^\perp$ es la distancia del código $\mathcal{C}_2^\perp$ dual de $\mathcal{C}_2$. Asimismo, la distancia d de este código cuántico satisface $d \geq \min(d_1, d_2^\perp)$.

Los CQCEs $[[n, k, d]]_2$ así construidos se llaman códigos CSS (Calderbank-Shor-Steane) [197, 198, 51, 173].

El ejemplo más simple e ilustrativo de código CSS es el código $[[7, 1, 3]]_2$ de Steane, o código cuántico de 7 qubits. Se obtiene tomando como $\mathcal{C}_1$ el código de Hamming $H_2(1)$ del tipo $[7, 4, 3]_2$, y como $\mathcal{C}_2$ su dual, que es del tipo $[7, 3, 4]_2$, y coincide con el subcódigo par (es decir, formado por las palabras código de peso par) de $\mathcal{C}_1$. Corrige un error X de inversión de bit, y un error Z de inversión de fase, y por tanto también un error mixto Y, pero no un error doble de inversión de bit (o de fase). Una base de estados código es

$$\begin{aligned}
|\overline{0}\rangle := 8^{-1/2}(&|1010101\rangle + |0110011\rangle + |0001111\rangle + |0000000\rangle + \\
&|1100110\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle), \\
|\overline{1}\rangle := 8^{-1/2}(&|0100101\rangle + |1000011\rangle + |1111111\rangle + |1110000\rangle + \\
&|0010110\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle).
\end{aligned}$$

3.6 Teleportación cuántica

La reproducción de estados clásicos (sea una fíbula etrusca, un cuadro de Goya, o un billete de banco) nunca ha presentado dificultades insalvables a los expertos. Basta con observar minuciosamente durante el tiempo que haga falta el original, procurando no estropearlo, para extraer cuanta información requiera su copiado. Esta observación cuidadosa no altera de forma perceptible el estado. Pero si el original a reproducir es un sistema cuántico en un estado ϕ desconocido, cualquier medida (incompatible con P_ϕ) que se haga sobre el sistema para averiguar algo sobre ϕ perturbará el estado de modo incontrolable, destruyendo el original. Además, incluso disponiendo de un número ilimitado de copias del estado, su determinación exigiría infinitas medidas.

Por ejemplo, supongamos que Alice tiene un qubit (digamos un spin $\frac{1}{2}$), que Bob necesita, pero Alice no dispone de ningún canal cuántico para enviárselo.[83] Si Alice conoce el estado preciso de su qubit (por ejemplo, si sabe que su spin $\frac{1}{2}$ está orientado en la dirección **n**), basta que le de a Bob por carta (canal clásico) esa información (componentes de **n**) para que éste se prepare un qubit exactamente igual al que tiene Alice. Pero si esta desconoce el estado, puede optar por confesárselo así a Bob, a quien

[83] Es costumbre usar los nombres de Alice y Bob para referirse a dos personajes que se comunican para intercambiar información; Eve es un tercer personaje, "malévolo", que intenta captar esa información a cuyo acceso está vetado, para conocerla y/o modificarla.

no le quedará más recurso que prepararse su qubit de forma aleatoria, consiguiendo una fidelidad del 50 %. Pero también Alice puede intentar ser más cooperativa, haciendo por ejemplo sobre su qubit una medida de $\mathbf{n}\cdot\sigma$, con $\mathbf{n}$ elegido de forma cualquiera, y transmitiendo a Bob tanto las componentes del vector $\mathbf{n}$ como el resultado $\varepsilon = \pm 1$ obtenido. Armado de esta información, Bob se prepara su qubit en el estado $\frac{1}{2}(1+\varepsilon\mathbf{n}\cdot\sigma)$. La fidelidad media así conseguida es mayor que antes: $\frac{2}{3}$. Sin embargo, no es suficiente.

Si Alice y Bob comparten un par EPR, existe un protocolo, ideado por Bennett *et al.* [25], y conocido como *teleportación cuántica*, que recurriendo al entrelazamiento de estados y a la no localidad permite a Bob reproducir un estado cuántico en posesión de Alice y desconocido, con tan sólo 2 cbits de información enviados por Alice a Bob a través de un canal clásico. Este procedimiento destruye necesariamente el estado que tiene Alice (de lo contrario se violaría la imposibilidad de clonación cuántica, consecuencia de la linealidad y/o unitariedad de la mecánica cuántica). Veamos con algún detalle el protocolo en cuestión.

Sea $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ el qubit en posesión de Alice, con $\alpha = \cos\frac{1}{2}\theta$, $\beta = e^{i\phi}\mathrm{sen}\frac{1}{2}\theta$. Y sea $|\Phi\rangle := 2^{-1/2}(|00\rangle + |11\rangle)$ el estado EPR compartido por Alice y Bob, de modo que Alice tiene el primero de sus qubits, y Bob el segundo. El estado inicial es por tanto $|\psi\rangle\otimes|\Phi\rangle$, del que localmente Alice puede manipular sus dos primeros bits y Bob el tercero.

Paso 1. Alice aplica al estado inicial el operador unitario $U := ((U_{\mathrm{H}}\otimes 1)U_{\mathrm{CNOT}})\otimes 1)$, actuando con la puerta CNOT sobre los dos primeros qubits y con la puerta Hadamard H sobre el primero. Resulta así el estado

$$\tfrac{1}{2}(|00\rangle\otimes|\psi\rangle + |01\rangle\otimes X|\psi\rangle + |10\rangle\otimes Z|\psi\rangle + |11\rangle\otimes Y|\psi\rangle),$$

donde X, $Y := XZ$, Z son las puertas monarias σ_1, $-i\sigma_2$, σ_3.

Paso 2. Alice mide a continuación los dos primeros qubits, obteniendo $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ con probabilidades del 25 % cada caso.[84] Comunica a Bob el resultado obtenido, mandándole para ello dos cbits: el par de dígitos binarios 00, 01, 10, 11 que lo caracterizan. Como consecuencia de la medición hecha por Alice, el primer bit ha dejado de estar en el estado original $|\psi\rangle$, mientras que el tercer qubit se proyecta en $|\psi\rangle, X|\psi\rangle, Z|\psi\rangle, Y|\psi\rangle$, respectivamente.

Y paso 3. Tan pronto como Bob recibe la información clásica que le manda Alice, no tiene más que actuar sobre su qubit (el tercer qubit del sistema total) con la puerta correspondiente 1, X, Z, Y, para conducirlo al estado $|\psi\rangle$ pretendido.

Obsérvese que en este teleporte se envía un estado cuántico desconocido desde un lugar (del que desaparece) a otro (donde surge) sin que atraviese en realidad el espacio intermedio. No se viola con ello la causalidad. Hay una parte de la información que se transmite instantáneamente. Es la información puramente cuántica. La parte restante que falta para la conclusión del teleporte, viaja clásicamente, al estilo ordinario no superlumínico. Nótese también que en este proceso "incorpóreo" es la información sobre el estado cuántico del qubit, y no el sistema físico, lo que ha pasado de Alice a Bob. No ha habido transporte de materia, energía o información a velocidad superior a la de la luz.

No deja de ser sorprendente en la teleportación cuántica que toda la información para reproducir el estado $|\psi\rangle = (\cos\frac{1}{2}\theta)|0\rangle + e^{i\phi}(\mathrm{sen}\frac{1}{2}\theta)|1\rangle$ (información que es infinita, pues requiere fijar un punto (θ,ϕ) en la esfera de Bloch, con precisión infinita, y por

[84] Los pasos 1+2 equivalen a hacer una medición Bell sobre el estado inicial, que pone en correlación los estados Bell del primer par de qubits en disposición de Alice con sendos estados del qubit que tiene Bob.

tanto con infinitos bits) se consiga con tan sólo 2 cbits si se comparte un estado EPR, que por su lado sólo genera un número infinito de bits aleatorios y correlacionados.

Los argumentos anteriores muestran que, suponiendo que Alice y Bob disponen cada uno de la mitad de un par EPR, para que Bob pueda lograr un estado como el estado desconocido que tiene Alice, debe recibir 2 cbits de información. Sin embargo, si Alice conoce el estado de su qubit, digamos $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, pero Bob no, un solo cbit basta para que Bob pueda reproducir ψ con un 50 % de probabilidad [168]: sea ahora el estado EPR compartido $|\Psi\rangle := 2^{-1/2}(|01\rangle - |10\rangle) = 2^{-1/2}(|\psi\psi'\rangle - |\psi'\psi\rangle)$, donde $|\psi'\rangle$ es ortogonal a $|\psi\rangle$. Alice hace una medición von Neuman sobre el subsistema 1 de $|\Psi\rangle$ en la base $|\psi\rangle, |\psi'\rangle$. Si obtiene $|\psi'\rangle$ (probabilidad $\frac{1}{2}$), su medición proyectará $|\Psi\rangle$ sobre $|\psi'\psi\rangle$; enviando a continuación a Bob con un cbit la información de su resultado, Bob ya sabe que su mitad del EPR está en el estado $|\psi\rangle$. Pero si Alice obtiene $|\psi\rangle$ (probabilidad $\frac{1}{2}$), proyectará $|\Psi\rangle$ sobre $|\psi\psi'\rangle$, y tras comunicar a Bob con un cbit el resultado, este sólo sabrá que su mitad está en el estado ortogonal al que tenía Alice. Así pues este procedimiento funciona en el 50 % de los casos.

La distancia informativa entre el teleporte cuántico y clásico no es notable para sistemas de baja dimensionalidad, aunque crece exponencialmente con esta. Se demuestra, por ejemplo, que si Alice y Bob disponen de una lista común de ternas ortogonales aleatorias y de números aleatorios, entonces hay un protocolo clásico de teleporte de modo que basta la transmisión de 2.19 cbits de Alice a Bob para teleportar clásicamente desde aquella a este un estado cuántico de spin conocido por Alice y desconocido por Bob [53].

Llamando *ebit* al recurso informático formado por un par EPR compartido, y denotando por $a \triangleleft b$ que el recurso a es implementable gastando el recurso b, son claras estas relaciones: 1 cbit $\triangleleft$ 1 qubit (para transmitir 1 cbit basta enviar 1 qubit en uno de dos estados ortogonales), 1 ebit $\triangleleft$ 1 qubit (para disponer de 1 ebit basta producir un par EPR y enviar la mitad al otro socio). En esta formulación, el teleporte cuántico nos permite escribir: 1 qubit $\triangleleft$ 1 ebit + 2 cbits [20].

El teleporte cuántico fue realizado por primera vez experimentalmente con fotones en dos laboratorios en 1997 [40, 38]. Esto es al menos lo que sus autores proclaman, aunque se alzan voces críticas discordantes [50, 208, 49] (ver, sin embargo, [41, 42]). En el experimento del grupo de Roma [38] el estado inicial a teleportar desde Alice a Bob es una polarización de un fotón, pero no es una cualquiera, sino que coincide con la del miembro del par EPR de fotones compartido en posesión de Alice. En los experimentos del grupo de Innsbruck, sin embargo, el estado teleportado sí es arbitrario; se consigue su teleporte con una fidelidad alta de 0.80 ± 0.05,[85] pero con una eficiencia reducida (un 25 % de los casos).

No parece fácil implementar el protocolo teórico de modo que sea 100 % efectivo. El operador de Bell (que distingue entre los cuatro estados Bell de 2 qubits) no se puede medir si no median interacciones cuánticas importantes entre ambos qubits (como ocurre con la puerta CNOT utilizada en el protocolo expuesto), lo que es prácticamente imposible con fotones. Pero con átomos en cavidades EM las esperanzas son buenas.

También se ha realizado el teleporte de estados que forman parte de sistemas enredados [166].

Mención aparte merece el teleporte cuántico de estados de sistemas de dimensión infinita [84] (concretamente, el teleporte de estados ópticos coherentes apoyándose en pares EPR de estados estrujados). En este experimento, cuya fidelidad es del $0.58 \pm$

[85] Esta fidelidad supera el valor 2/3 correspondiente al caso en que Alice midiera su qubit y comunicara a Bob clásicamente el resultado.

0.02 (superior al máximo de $\frac{1}{2}$ esperable sin uso del enredo), un nuevo personaje, el *verificador* Victor, suministra a Alice un estado que él conoce, pero ella no. Tras proceder a su teleporte desde Alice a Bob, Victor verifica a la salida del protocolo si el estado en posesión de Bob es similar al que él proporcionó a Alice. En este sentido, el experimento se distingue de todos los anteriores, y lleva a sus autores a reclamar la prioridad en la realización del teleporte.

El teleporte cuántico, que sin duda se extenderá a estados enredados de sistemas distintos (fotones y átomos, iones y fonones, etc.), podría tener cruciales aplicaciones en los futuros computadores cuánticos y enlaces entre los mismos (por ejemplo, combinado con la *destilación* previa de buenos pares EPR), así como, por ejemplo, en la producción de memorias cuánticas mediante teleporte de la información sobre sistemas como fotones a otros sistemas como iones atrapados y bien aislados en cavidades [20, 40].

3.7 Codificación densa

Por un canal cuántico podemos enviar también información clásica: para mandar la palabra 10011, basta que Alice prepare 5 qubits en los estados $|1\rangle$, $|0\rangle$, $|0\rangle$, $|1\rangle$, $|1\rangle$, los envíe por el canal cuántico a Bob, y este mida cada uno en la base $\{|0\rangle, |1\rangle\}$. Cada qubit transporta un cbit, y en soledad es lo más que puede hacer. Pero si Alice y Bob comparten de antemano un estado enredado, mediante un sólo qubit desde Alice a Bob se pueden enviar 2 cbits de información.

El entrelazamiento es efectivamente un recurso informático que permite formas más eficientes de cifrar información [31]. Una de ellas se conoce como *codificación cuántica densa* (o codificación superdensa). Veamos un ejemplo. Supóngase un estado EPR de dos fotones. Uno de los fotones va a Alice, el otro a Bob. Aquella realiza sobre la polarización del fotón que le llega alguna de estas cuatro operaciones: identidad, inversión (es decir, H$\leftrightarrow$V, o D$\leftrightarrow$I), cambio de fase en π, y producto de estas dos últimas. Hecho eso, reenvía el fotón hacia Bob. Este mide el estado del par. Hay cuatro resultados posibles (los cuatro estados de Bell). Luego así se ha conseguido mandar 2 bits de información sobre una sola partícula de 2 estados, esto es, mediante 1 qubit. Es el doble de lo que se puede conseguir clásicamente. De aquí el nombre de codificación densa. Además si Eve intercepta el qubit, no puede obtener de él ninguna información, pues su estado es $\frac{1}{2}I$. Toda la información está en el estado entrelazado, y la mitad de éste está en posesión de Bob. En realidad, Alice ha enviado a Bob 2 qubits, pero el primero de ellos hace tiempo, como parte del estado entrelazado inicial. Esto les ha permitido comunicarse luego de modo más eficiente, recurriendo al estado enredado que compartían.

La codificación densa viene a ser un proceso inverso al teleporte. En este la comunicación de dos cbits permite reproducir un qubit, en aquella, la comunicación de un qubit transporta dos cbits de información. En fórmula: 2 cbits $\triangleleft$ 1 ebit + 1 qubit.

Un protocolo que implementa detalladamente lo dicho puede ser este [179]: una fuente EPR suministra a Alice y Bob estados EPR del tipo $|\Phi\rangle := 2^{-1/2}(|00\rangle + |11\rangle)$, uno de cuyos miembros va a Alice y el otro a Bob, que los guardan. A Alice le proporcionan 2 cbits, que representan los números 0, 1, 2, 3 como 00, 01, 10, 11.

Paso 1. Codificación. Según cual sea este número, Alice realiza sobre su mitad EPR la operación unitaria $I, Z = \sigma_3, X = \sigma_1, Y = -i\sigma_2$, que lleva el estado EPR en cuestión a 00+11, 00-11, 10+01, -10+01. Hecho ésto, envía su mitad a Bob.

Paso 2. Descodificación. Bob, tras recibirla, somete el par EPR primero a una operación CNOT, de modo que el estado pasa a ser 00+10, 00-10, 11+01, -11+01. Mide a

continuación el segundo qubit; si encuentra 0, ya sabe que el mensaje ha sido 0 o 1, y si halla 1, el mensaje ha sido 2 o 3. Es decir, ha obtenido el primer bit del mensaje. Para conocer el segundo, Bob aplica seguidamente Hadamard sobre el primer qubit, con lo que el estado pasa a ser 00, 10, 01, 11, y midiendo el primer qubit, si encuentra 0, sabrá que el mensaje ha sido 0 o 2, y si halla 1, el mensaje ha sido 1 o 3, es decir, habrá obtenido el segundo bit del mensaje.

Un experimento de esta naturaleza se ha hecho en Innsbruck [149], usando como fuente de fotones entrelazados la conversión paramétrica a la baja que produce un cristal no lineal de betaborato de bario: fotones UV se desintegran (aunque con probabilidad pequeña) en un par de fotones más suaves, con polarizaciones que en cierta configuración geométrica están entrelazadas. En dicho experimento se consiguió enviar 1 qutrit/qubit, es decir, $\log_2 3 = 1.58$ cbits por qubit.

En un experimento posterior, en que los qubits son los spines del ^{1}H y ^{13}C en una molécula de cloroformo $^{13}CHCl_3$ marcada con ^{13}C, y se usan técnicas de RMN para inicializar, manipular y leer los spines, los autores afirman haber conseguido alcanzar los 2 cbits por qubit [77].

En general, si un substrato físico para la información puede prepararse en N estados distintos y por tanto permite codificar N mensajes diferentes, usando una preparación inicial consistente en disponer cada uno de una mitad de un estado enredado compartido, se pueden enviar hasta N^2 mensajes distintos. Además, la preparación inicial ha podido tener el sentido inverso al envío posterior; por ejemplo, Bob envía a Alice la mitad del estado enredado, quedándose él con la otra mitad, y luego Alice lo usa para enviarle a Bob la información deseada. Esto puede tener interés si la transmisión en una dirección es mucho más costosa que en la otra. Al ser previo a la comunicación el reparto del estado enredado, se puede aprovechar tiempos de transmisión barata para aquél.

Por otro lado, la interceptación del mensaje que va de Alice a Bob no proporciona ninguna información al que escucha, pues está enredado con la parte del sistema EPR que tiene Bob. Luego es automáticamente una emisión encriptada (salvo si Eve intercepta el par original y el mensaje y los reemplaza).

3.8 Criptografía clásica y cuántica

La criptología hunde sus raíces en el pasado [118]. Ya en el siglo V a.C. los militares de Esparta trasmitían y descifraban mensajes secretos; precisamente uno de estos, roto por Gorgo, esposa de Leónidas, llevaría a éste al paso de las Termópilas para detener, al frente de los espartanos, y con el sacrificio de su vida, el cruce de las tropas persas.

María Estuardo, reina de Escocia, perdió su cabeza porque Sir Francis Walsingham (fundador del Servicio Secreto británico) descifró un mensaje en clave donde se hablaba de planear la muerte de Isabel de Inglaterra, y EEUU entró en la I Guerra Mundial porque los servicios de inteligencia ingleses descifraron un telegrama de Zimmermann en que ofrecía ventajas territoriales a Méjico si se aliaba con Alemania.

Pero es a mediados de este siglo, en la década de los 40, cuando se convierte la criptografía en parte de la teoría de la información a través de los trabajos seminales de Shannon.

La criptografía trata de transformar información haciéndola ininteligible para quienes no estén autorizados para lo contrario. Las estrategias desarrolladas por estos últimos para desvelar la información oculta constituyen el criptoanálisis, y las actividades de ambos mundos opuestos y en continua pugna integran la criptología.

3.8.1 Criptología elemental

El cifrado cesáreo (atribuido a Julio César) es un *cifrado de transposición*: cada signo se desplaza una misma cantidad a lo largo del alfabeto (módulo la longitud de éste). Así

QR NRLNRB CFIF JF

no es más que

TU QUOQUE FILI MI

con una transposición de -3 aplicada a éste.

El criptosistema CESAR es sumamente vulnerable por cualquier aficionado, pues basta aplicar todas las transposiciones posibles hasta conseguir algo que tenga sentido.[86]

Los aficionados a las novelas policíacas recuerdan seguramente cómo Sherlock Holmes, en el relato THE ADVENTURE OF THE DANCING MEN, descifra cinco mensajes a partir de las 62 figuras que los integran (estudiando su frecuencia, pues se sabe, por ejemplo, que en inglés la E es la letra más frecuente, incluso en textos cortos) y con ello cifra otro (COME HERE AT ONCE) mediante el cual atrae a un peligroso gángster de Chicago a donde le espera la policía.

Este procedimiento se conoce como *cifrado con sustitución monoalfabética*. No es tampoco nada seguro, a pesar de que el número de ensayos ciegos es mucho mayor que para el cifrado de trasposición. Se le ataca de modo algo más sutil, estudiando, como en el caso anterior, las frecuencias de los distintos símbolos. En inglés, del análisis de unas 100,000 letras de texto de diversas fuentes, se ha visto que las frecuencias (en %) de las distintas letras del alfabeto son las representadas en la Tabla 1.

E	T	A	O	I	N	S	H	R	D	L	C	U
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8
M	W	F	G	Y	P	B	V	K	J	X	Q	Z
2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.2	0.15	0.1	0.1

Tabla 1: Frecuencias (en %) de las letras en inglés, ordenadas de mayor a menor.

Los criptanalistas profesionales se apoyan también en la distribución frecuencial de poligramas (conjuntos de varias letras contiguas en el texto), generalmente digramas y trigramas, para destripar la clave de sustitución. Se sabe, por ejemplo, que en inglés los digramas más frecuentes son, de más a menos, TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ..., y en cuanto a los trigramas, THE, ING, AND, HER, ERE, ENT, THA, NTH, ä.

3.8.2 Criptografía clásica

Como dijimos antes, la criptografía forma parte importante de la teoría de la información desde 1949, a partir de los trabajos pioneros de Shannon en los Bell Labs. Probó éste que existen cifrados inexpugnables, o sistemas de secreto perfecto [189]. De hecho, alguno de éstos se conocía desde 1918 (mas no que fuera inquebrantable):

[86] Sin embargo, a César pudo servirle para comunicarse con su amigo Cicerón y otros.

el sistema *one-time pad* (ONETIMEPAD), o de cuaderno de un sólo uso. Se conoce también como cifrado VERNAM [210], pues fue ideado por el joven ingeniero Vernam (de la ATT) en diciembre de 1917 y propuesto a la compañía en 1918 [118]; con el sistema de Vernam se automatizaba por vez primera tanto el cifrado como el descifrado de los mensajes.

3.8.2.1 Cuaderno de "usar y tirar" El cifrado basado en un cuaderno con hojas de un sólo uso consiste en que el texto *ordinario* a cifrar se convierte en una sucesión de números $p_1, p_2, \ldots, p_N$ y luego se usa una *clave* $k_1, k_2, \ldots, k_M$, $M \geq N$, de números aleatorios con los que se combinan aquellos en aritmética modular $p_j + k_j = c_j \bmod B$, donde B es el número máximo de símbolos distintos (2 en binario, 10 para dígitos, 28 para letras, etc.), para producir un texto *cifrado* o *criptograma* $c_1, c_2, \ldots, c_N$. Tanto el que escribe (Alice) como el destinatario (Bob) tienen que tener la misma clave de números aleatorios, de modo que al recibir Bob el criptograma, deshace el algoritmo con esa clave y así recupera el texto original.

Posibles frecuencias en el texto fuente (en las que se apoyan los quebrantacódigos para descifrar) quedan borradas por la clave aleatoria.

La longitud de la secuencia de aleatorios debe ser mayor o igual que la del texto fuente, y no debe usarse más de una vez.[87] Shannon demostró que si la clave es de menor longitud que el texto es posible extraer información del mensaje cifrado [189]. Estos requerimientos hacen muy gravoso el procedimiento cuando es mucha la información a encriptar. Además no es fácil disponer de secuencias de números verdaderamente aleatorios.[88]

Este sistema de cifrado fue usado por diplomáticos alemanes y rusos en la segunda guerra mundial, y por el espionaje soviético durante la guerra fría. Su nombre popular de *one-time pad* se debe a que las claves estaban escritas en un cuaderno o bloc, y cada vez que se utilizaba una, se arrancaba la correspondiente hoja del cuadernillo donde figuraba y se destruía. Se cuenta que el uso continuado de la misma clave permitió desenmascarar las redes de espionaje de Rosenberg y de Fuchs [106]. También lo usó el Che Guevara para comunicarse en clave desde Bolivia con Fidel Castro [24]. Y es rutina para las comunicaciones a través del "teléfono rojo"entre la Casa Blanca y el Kremlin.

Aunque invulnerable, el criptosistema VERNAM tiene el inconveniente de exigir claves tan largas al menos como el texto a cifrar. Por eso se usó únicamente para cifrar información sumamente valiosa, reemplazándose para menesteres menos delicados por encriptación con claves más cortas aunque quebrantables. Precisamente el acicate por romper mensajes secretos propiciaría el desarrollo de los ordenadores.

3.8.2.2 Sistema PKC De aquí el interés del PKCS (*Public Key Cryptographic System*), ideado a mediados de la década de los 70 por Diffie y Hellman en Stanford

[87] Interceptados dos mensajes cifrados con la misma clave, su suma módulo 2 elimina esta y hace posible desencriptar con cierta facilidad los mensajes [61].

[88] Los números *random* generados por los ordenadores son, en realidad, pseudoaleatorios. Pasan muchos de los tests de aleatoriedad, como equidistribución de dígitos, falta de correlaciones ostensibles, etc., pero son de hecho secuencias deterministas, pues están obtenidas mediante el cálculo de una función concreta. Ya lo advertía von Neumann: *Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.* Entre los más corrientes están los generadores congruenciales lineales. A veces son muy poco aleatorias estas secuencias, y se recurre a otros generadores más seguros llamados de registro desplazado. De todos modos, no hay que fiarse de un solo generador cuando se hacen cálculos donde se usen números aleatorios, siendo aconsejable repetirlos con generadores distintos.

[68, 69, 103], implementado en el MIT por Rivest, Shamir y Adleman [180],[89] y de uso muy frecuente, por ejemplo en internet.

Se basa en el uso de dos claves: la persona X da una clave pública, a disposición de cualquiera, y otra privada que no da a conocer, y que es la inversa de la anterior. La primera la utiliza cualquier persona R para mandarle a X mensajes cifrados; cuando X los recibe, los descifra con su clave privada. Es claro que ésto sólo tiene interés si exclusivamente X sabe deshacer el cifrado.

¿Cómo se consigue ésto? De una forma sutil e inteligente: el sistema PKC utiliza, para encriptar mensajes, funciones de dirección única (o unidireccionales) con "trampilla", es decir, funciones inyectivas de complejidad P, es decir, *tratables* (computacionalmente), cuyas inversas son prácticamente *intratables*,[90] esto es, muy costosas de evaluar salvo si se dispone de información adicional como algún certificado sucinto (presunto problema $\mathsf{NP}-\mathsf{P}$). Entre estas funciones inversas destacan la factorización de enteros, y el cálculo de logaritmos discretos en cuerpos finitos y sobre curvas elípticas [129, 211]. El sistema PKC se permite el lujo de dejar a la vista pública tanto el algoritmo de encriptación como media clave sin que se resienta en la práctica su seguridad; contrasta ostensiblemente con el sistema DES, donde a pesar de hacerse público sólo el algoritmo, su vulnerabilidad ha quedado demostrada [72].

3.8.2.3 Sistema RSA Uno de los modos más interesantes de implementación del PKCS es el método RSA (Rivest, Shamir, Adleman), basado en la dificultad de factorizar números grandes [180]. Se usa, en particular, para proteger las cuentas electrónicas bancarias (por ejemplo, frente a transferencias bancarias ordenadas por via electrónica).

La clave pública de X consiste en un par de números enteros $(N(X), c(X))$, el primero muy grande, digamos de 200-300 dígitos, y el otro en el intervalo $(1, \phi(N(X)))$ y coprimo con $\phi(N(X))$, siendo ϕ es el indicador o función indicatriz de Euler ($\phi(n)$ es el número de coprimos con n en el intervalo $[1, n]$).

Tras transformar el remitente R su mensaje M en secuencia de números (binarios, decimales, o en la base que se convenga), lo rompe en bloques $B < N(X)$ de longitud máxima, cifra cada bloque B según

$$B \mapsto C := B^{c(X)} \bmod N(X)$$

y manda la secuencia de criptogramas $C(B)$ a X. Denotemos esta operación de cifrado como $M \mapsto P_X(M)$, indicando por el símbolo P_X que se ha hecho con la clave pública de X.

El destinatario X descifra cada $C(B)$ como

$$C(B) \mapsto B := C(B)^{d(X)} \bmod N(X)$$

donde el exponente $d(X)$ para el descifrado es la clave privada, y que no es otro que la solución a

$$c(X)d(X) = 1 \bmod \phi(N(X))$$

Esa solución es

$$d(X) = c(X)^{\phi(\phi(N(X)))-1} \bmod \phi(N(X)).$$

[89] Parece ser que el Servicio Secreto Británico conocía este sistema, pero como material clasificado (secreto militar), antes de que lo Diffie y Hellman lo descubrieran. Había sido ya inventado en 1975 por James Ellis, Clifford Cocks y Malcolm Williamson en los Government Communications Headquarters (GCHQ). Así lo ha reconocido oficialmente el Gobierno Británico en diciembre 1997.

[90] No se conocen funciones indiscutiblemente unidireccionales; las hay, sin embargo, que probablemente lo sean, y que lo son en la práctica con los algoritmos conocidos hasta el momento.

El descifrado lo indicaremos por $P_X(M) \mapsto S_X(P_X(M)) = M$, donde el símbolo S_X alude a la clave privada o secreta de X.

En principio, cualquiera puede calcular $d(X)$, pues se conocen $c(X)$ y $N(X)$, y así romper el secreto. Y aquí es donde entra ahora la astucia de X. Para ponérselo pero que muy difícil a Eve, mejor es que se atenga a ciertas normas, entre las que destacan las siguientes:

- Debe X escoger el módulo $N(X)$ como producto de dos primos enormes y aleatorios (de al menos un centenar de dígitos cada uno) p_1, p_2, y no muy próximos entre sí (basta que las longitudes de sus expresiones difieran en unos pocos bits), pues de lo contrario a Eve, que conoce $N(X)$, no le costaría mucho encontrar dichos factores. Hay que evitar tomar primos que estén en tablas o sean de formas muy especiales. Algoritmos de primalidad como el probabilista de Miller-Rabin [155, 177], o el determinista APRCL, descubierto por Adleman, Pomerance y Rumely, y simplificado y mejorado por Lenstra y Cohen [1, 59, 60], facilitan la elección de p_1, p_2.

- Como X conoce p_1, p_2, sabe ya que calcular $\phi(N(X))$ como $(p_1-1)(p_2-1)$. Ahora tiene que escoger X un entero $d(X)$ (su clave privada) al azar en el intervalo $(1, \phi(N(X)))$, coprimo con $\phi(N(X))$, y calcular la clave pública $c(X)$ mediante $c(X) = d(X)^{\phi(\phi(N(X)))-1} \bmod \phi(N(X))$, o mejor aún, usando el clásico algoritmo de Euclides.

- El número $d(X)$ no debe ser pequeño, para evitar que se pueda encontrar por prueba y error. Por eso conviene comenzar fijando la clave privada. Pero también hay que procurar que $c(X)$ no resulte demasiado pequeño, pues de lo contrario la interceptación de un mismo mensaje enviado a varios destinatarios con la misma clave pública aunque distintos módulos podría conducir sin mucho esfuerzo a su descifrado [186].

Cualquier persona que sólo conozca $N(X)$ pero no sus factores, aparentemente[91] tendrá primero que factorizar $N(X)$ para calcular $\phi(N(X))$, y con ello poder hallar el exponente para descifrar; pero factorizar un número de 250 dígitos le llevaría a una estación de trabajo de 200 MIPS unos 10 millones de años con el mejor algoritmo hoy conocido [107].

El sistema PKC permite también "autentificar" digitalmente los mensajes, y añadirles una "firma electrónica" o "digital" [144, 129, 201, 211].

3.8.2.3.1 Los números RSA En 1977 Martin Gardner publicó un mensaje cifrado en sus MATHEMATICAL GAMES de *Scientific American* usando el método RSA, con la promesa de recompensar con 100$ (pagaderos por el grupo de Rivest *et al.* en MIT) a quien lo descifrara [94]:

$$96869613754622061477140922254355882905759991124574319874695120930816298225145708356931476622883989628013391990551829945157815154$$

Este criptomensaje había sido obtenido a partir de una frase en inglés y el diccionario

[91] "Aparentemente", porque se ignora si existen o no procedimientos alternativos para descifrar $C(B)$ que no pasen por la obtención del exponente inverso, o si el cálculo de éste exige forzosamente conocer los factores primos de N.

$$\text{Espacio} \mapsto 00,\ \text{a} \mapsto 01,\ \text{ä} \ldots,\ \text{z} \mapsto 26,$$

por el método RSA, y clave pública (RSA-129, 9007), donde RSA-129 era el siguiente número de 129 dígitos

RSA-129 =
114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

El descifrado requería factorizar RSA-129 en sus dos factores primos de 64 y 65 dígitos cada uno. Se estimaba entonces que el tiempo para conseguirlo sería al menos de unos 4×10^{16} años. En 1994 nuevos algoritmos de factorización[92] y el trabajo en red de un millar de estaciones de trabajo permitió lograrlo en unos 8 meses, tras un tiempo de cálculo de 5000 MIPS-años, mediante el algoritmo de la criba cuadrática (QS). Esos factores son

349052951084765094914784961990389813341776463849338784399082057 7
$\times$
327691329932667095499619881908344614131776429679929425397982885 33

conociendo los cuales es inmediato hallar el mensaje original [9]: `the magic words are squeamish ossifrage`.

Dos años después se rompió el RSA-130 mediante el algoritmo de factorización más potente hasta la fecha: la criba general de cuerpos de números (GNFS), y en un tiempo de computación casi un orden de magnitud menor que el empleado para el RSA-129. Finalmente, en agosto de 1999 se ha ultimado la factorización del RSA-155, también mediante GNFS y tras unos 8000 MIPS-años.[93] Tiene 512 bits y es producto de dos primos de 78 dígitos. Para darnos una idea de la magnitud de este problema, en su solución se han empleado 35.7 años de CPU para hacer la criba, repartidos entre unas trescientas estaciones de trabajo y PCs, y 224 horas de CPU de un CRAY C916 y 2 Gbytes de memoria central para hallar las relaciones entre las filas de una monstruosa matriz de 6.7 millones de filas y otros tantos de columnas, y una media de 62.27 elementos no nulos por fila.

Hace unos pocos años se daba como muy seguro el uso de módulos de 512 bits. Hoy, tras el desarrollo del algoritmo GNFS de factorización, se recomienda usar módulos de (768, 1024, 2048) bits para uso (personal, corporativo, y de extrema seguridad).

Si bien el problema de factorización sigue siendo en la actualidad un problema computacionalmente duro, nadie está seguro de que no pueda surgir el día de mañana algún matemático con un algoritmo radicalmente más rápido con el que los computadores clásicos existentes puedan factorizar en tiempo polinómico. De hecho, la computación cuántica ha despertado enormes expectativas en este sentido, al abrir las puertas a un método de factorización de tiempo polinómico, conocido como algoritmo de Shor [191, 75], y que pende como espada de Damocles sobre los sistemas de encriptación. ¡Por eso la CIA sigue de cerca los avances en teoría de los números y de la computación! En un encuentro científico celebrado no hace mucho tiempo en Turín, Shor, tras presentar su algoritmo, apostaba públicamente que la factorización de números de 500

[92] Existen métodos eficientes, como los basados en la criba cuadrática (QS) [170, 96, 171], en curvas elípticas (EC) [134], y en la criba general de cuerpos de números (GNFS) [135, 171]. Sus complejidades son subexponenciales, pero superpolinómicas. A partir de 120-130 dígitos, parece ser que la criba de cuerpos de números aventaja a las otras.

[93] Agradezco a los Profs. A.K. Lenstra y H.te.Riele por su información acerca de los últimos RSAs factorizados.

dígitos se lograría antes con un computador cuántico que con otro clásico.[94] Aunque las dificultades tecnológicas a vencer para construir un computador cuántico medianamente complejo son enormes,[95] es alto el interés en hallar sistemas de distribución de claves cuya seguridad no se fundamente en la dificultad práctica de factorizar enteros grandes.

3.8.3 Criptografía cuántica

La física cuántica ofrece un método seguro para cifrar, garantizado por las propias leyes físicas. Ha nacido con ello la criptografía cuántica o "*qriptografía*". Se basa en los principios de complementariedad e incertidumbre, y en la indivisibilidad de los quanta. El pionero ha sido Stephen Wiesner, quien ya en 1969[96] sugirió, entre otras cosas, cómo fabricar billetes de banco infalsificables, billetes de banco cuánticos [212]. A mediados de los 80 Bennett y Brassard [23] idearon un criptosistema cuántico basado en el principio de Heisenberg, que pronto se implementaría experimentalmente mandando con fotones polarizados información secreta a 30 cm de distancia [22]. Este sistema (conocido como protocolo BB84) usa estados cuánticos no ortogonales para evitar su clonación por un posible escucha; por emplear 4 estados distintos, se llama también *esquema de cuatro estados*. El empleo de correlaciones cuánticas no locales con pares de fotones enredados por conversión paramétrica a la baja fue propuesto luego por Ekert [74]; en este sistema E91 serían las desigualdades de Bell [11, 12, 13] las encargadas de proteger la seguridad. De ahí su calificativo de *esquema EPR*. Aquí nos limitaremos a comentar un protocolo de dos estados llamado B92 (Bennett 1992) y a mencionar brevemente las realizaciones experimentales de estas ideas.

3.8.3.1 Billetes con seguro cuántico Un billete de banco a prueba de falsificadores podría ser un billete con un número, y una pequeña colección (digamos veinte) de fotones, aprisionados indefinidamente en celdas individuales de paredes perfectamente reflectoras, y con polarizaciones secretas e individualmente aleatorias $\leftrightarrow, \updownarrow, \circlearrowright, \circlearrowleft$, que el banco emisor guardaría en secreta correspondencia con el número de identificación.

El banco por tanto podría en cualquier momento comprobar la legitimidad del billete, sin estropearlo, pues sabría cómo colocar los polarizadores para ver la polarización de cada fotón sin destruirla. Cualquier falsificador que intentase copiar un billete, sin embargo, desconocedor de en qué direcciones se polarizaron los fotones, rompería la polarización inicial proyectándola en alguna de las dos correspondientes al polarizador que eligiera para medir [212, 18].

3.8.3.2 QKD: distribución cuántica de claves Si bien lo de los billetes cuánticos puede parecer una fantasía, no lo son los sistemas de distribución cuántica de claves de alguno de los tipos existentes, como los citados protocolos BB84, B92 y EPR. Proporcionan una forma de compartir dos personas claves absolutamente secretas, y por tanto es el complemento ideal al cifrado Vernam.

[94] Nadie aceptó la apuesta.

[95] Como bien recuerda Preskill [172], es arriesgado aventurar nada en este campo; hace cincuenta años se pronosticaba que *"Where a calculator on the ENIAC is equipped with 18,000 vacuum tubes and weighs 30 tons, computers in the future may have only 1,000 tubes and perhaps only weigh 1 1/2 tons"* (Popular Mechanics, Marzo 1949), y el futuro ha sobrepasado con creces estas expectativas. Cualquier reloj digital tiene una potencia de cálculo comparable a la del histórico ENIAC.

[96] Su trabajo fue publicado finalmente en 1983, tras haber sido rechazado por la revista a la que se sometió por vez primera. Una versión no publicada del mismo apareció en 1970.

Alice y Bob quieren intercambiar información secreta, sin necesidad de intermediarios para llevar cuadernillos de claves de uno al otro, y sin temor a que rompan su código. Para ello deben compartir una clave, sólo conocida por los dos. Proceden según un protocolo de comunicaciones, o conjunto de pasos a seguir para o bien detectar cualquier escucha no autorizada, o en caso contrario, para establecer la clave secreta que sólo ellos compartirán para cifrar y descifrar.

3.8.3.3 Protocolo B92, o esquema de dos estados Este protocolo [17] usa sistemas en dos estados no ortogonales. Consta de cuatro pasos.

Paso 1: Alice y Bob generan sendas secuencias aleatorias de bits 0, 1. Por ejemplo,

```
Alice 10111110001111010110010100111011100101010110...
Bob   00010100011100001011001111101001001010000...
```

Paso 2: Alice prepara estados de spin $\frac{1}{2}$ asociados a cada uno de sus bits, de acuerdo con esta tabla:

$$0 \mapsto \mathrm{A} := |\uparrow\rangle \quad \text{(spin hacia arriba)}$$
$$1 \mapsto \mathrm{D} := |\rightarrow\rangle \quad \text{(spin hacia la derecha)}$$

Por ejemplo:

```
Alice 10111110001111010110010100111011100101010110...
      DADDDDDAAADDDDADADDAADADAADDDADDDAADADADDA...
```

Paso 3: Alicia manda a Bob cada estado de spin que ha preparado por un canal cuántico (canal sin influencia del medio sobre los estados cuánticos), y Bob mide sobre ellos ya el proyector $P_{\text{Izquierda}}$, ya P_{aBajo}, según su propia secuencia de bits:

$$0 \mapsto P_{\mathrm{I}}$$
$$1 \mapsto P_{\mathrm{B}}$$

Por ejemplo:

```
Bob 00010100011100001011001111101001001010000...
    IIIBIBIIIBBBIIIIBIBBIIBBBBBIBIIBIIBIBIIIII...
    NSNSNNNSSNSSNNSNNNNSNNNNNSNSNNSNSNNNNSNNN...
```

y se apunta los resultados (S si el estado de spin "pasa la cuestión", N si el estado falla, es decir, no pasa la pregunta). Cuando el bit de Bob es distinto del de Alice, el resultado es siempre N. En los demás casos, un 50% es S y el otro 50% es N.

```
Alice 10111110001111010110010100111011100101010110...
Bob   00010100011100001011001111101001001010000...
      NSNSNNNSSNSSNNSNNNNSNNNNNSNSNNSNSNNNNSNNN...
      -0-1---00-11--0-----0-----1-1--1-0----0---...
```

Paso 4: Bob manda una copia pública de la secuencia de sus resultados (S, N) a Alice, pero no de los proyectores que ha medido. Cualquiera puede tener acceso a esta secuencia de resultados. Y tanto Alice como Bob mantienen sólo aquellos bits de sus secuencias para los que el resultado de Bob ha sido S:

```
Alice 10111110001111010110010100111011100101010110...
Bob   00010100011100001011001111101001001010000...
      -S-S---SS-SS--S-----S-----S-S--S-S----S---...
      -0-1---00-11--0-----0-----1-1--1-0----0---...
```

Luego la clave destilada es

0100110011100…

Estos bits mantenidos constituyen la clave binaria a compartir para cifrar (Alice) y descifrar (Bob) como tablilla de un solo uso. En media, la longitud de esta clave es la cuarta parte de cada secuencia inicial.

3.8.3.3.1 Efectos de una escucha ¿Qué ocurre si hay una escucha no autorizada por parte de Eve? Supongamos que Eve conoce los tipos de preparaciones y medidas que Alice y Bob van a hacer, pero no sus secuencias aleatorias iniciales. Supongamos asimismo que Eve puede entrar en el canal cuántico, y medir y/o modificar los estados que quiera de los que por allí pasan. Del canal público admitiremos que puede escuchar, pero no interferir (de lo contrario, podríamos echar mano de un protocolo de autentificación que permitiera a Alice saber que nadie ha cambiado la clave que le manda Bob, por ejemplo utilizando un trozo remanente de clave secreta no empleada con anterioridad).

En primer lugar, no cabe pensar en “pinchar”; si Eve pudiera clonar estados, le bastaría con hacerse copias de lo que pasa por el canal cuántico, sin alterar el original, para conocer los estados preparados por Alice y de ahí, tras escuchar el envío final de Bob, reconstruir la clave secreta. Pero la unitariedad de la mecánica cuántica prohíbe la clonación de estados no ortogonales como los usados por Alice.

El análisis completo de los efectos de la escucha es largo y complejo. En el caso elemental de que Eve sea poco sofisticada y se limite a interceptar cada estado, actuar sobre él para intentar extraer información del mismo, y luego enviar otro en su lugar, la escucha se manifiesta en la variación que produce en el ritmo de generación de la clave, en el ritmo de errores en una porción de los S, y en la proporción de 0 *vs*. 1 en una porción de las S.

Supongamos, por ejemplo, que Eve decide medir P_{A} en cada uno de los estados que “escucha”de Alice, enviando a Bob el estado resultante. Todos los estados A de Alice pasarán como A, pero también lo harán un 50% de los D de Alice (mientras el otro 50% pasarán como B). Luego Eve sólo es capaz de identificar con total certeza aquellos estados de Alice que pasan la medida de Eve como B (y por tanto son estados D de Alice), es decir, el 25% de todos los estados de Alice. Pero esto a costa de dañar el material clave de Alice y Bob: por ejemplo, Bob hallará una descompensación entre S y N; mientras en ausencia de escucha la proporción S:N = 1:3, con la escucha que hemos supuesto por parte de Eve la proporción pasa a ser S:N = 3:5.

En la práctica, tanto la fuente emisora como el equipo receptor y el canal de transmisión presentan ruido, lo que necesariamente estropea el perfecto encaje de las secuencias de bits destiladas por Alice y Bob, aunque no haya ninguna Eve fisgoneando. Es preciso, pues, convivir con el error, siempre que este se mantenga en unos límites tolerables. En estas circunstancias Eve intentará actuar con discreción procurando que los efectos de su escucha no disparen la alarma.

Los protocolos BB84, B92 y EPR son seguros bajo ataques elementales, qubit a qubit, de Eve. Pero los criptoanalistas como Eve suelen ser bastante más finos en su perversidad que lo que el simple análisis anterior podría sugerir. Conscientes de las sutilezas cuánticas, no se conforman con pinchar el canal cuántico qubit a qubit, de forma incoherente; saben que el ataque coherente a ristras de qubits, con sondas analizadas tras el intercambio público de información entre Alice y Bob, puede serle mucho más provechoso. Demostrar la seguridad de un protocolo bajo cualquier tipo

de ataque imaginable por parte de la malévola y brillante Eve no es empresa baladí, ni manca de interés, sobre todo si se tiene en cuenta que otros protocolos amparados en la física cuántica y tenidos por incondicionalmente seguros han caído por tierra, como por ejemplo el protocolo cuántico del *compromiso a un bit*: Alice envía algo a Bob con su firme compromiso de haber elegido un bit *b* que Bob desconoce por completo, pero que luego Alice puede mostrarle cuando él lo reclame. El recurso a estados enredados EPR hace posible que cualquier miembro de la pareja sea deshonesto (que una tramposa Alice cambie al final su compromiso sin que Bob se entere, o que un truhán Bob obtenga alguna información sobre *b* sin tener que preguntarle a Alice) [150, 151, 46].

Se dispone de una demostración de la seguridad incondicional de la QKD a través de canales ruidosos y hasta cualquier distancia, mediante un protocolo basado en la compartición y purificación de pares EPR, y en la hipótesis de que las partes (Alice y Bob) disponen de computadores cuánticos tolerantes a faltas [143]. Asimismo, se afirma la seguridad incondicional del protocolo BB84 [152].

3.8.3.4 Realización práctica de QKD El protocolo BB84 se ha implementado por vez primera en el IBM T.J. Watson Research Center (1989-1992) con fotones polarizados guiados por un tubo con aire de 32 cm [45, 22].

En 1995 se realizó experimentalmente el protocolo B92, también con fotones polarizados, transmitidos esta vez a lo largo de una fibra óptica de 23 km uniendo bajo las aguas del lago Lemán las ciudades de Ginebra y Nyon [157, 158].

El uso de estados de polarización de fotones para largas distancias tiene un inconveniente, y es su pérdida en la transmisión por la fibra debido a que la birrefringencia en las partes no rectas de la fibra transforma los estados de polarización lineal en estados de polarización elíptica, y además produce dispersión de modos de polarización ortogonales. De ahí el interés en otros modos de codificar los estados, como por ejemplo mediante fases en lugar de polarizaciones. Un grupo de la British Telecom en UK lo ha conseguido (1994) con fibra óptica a lo largo de 30 km, usando interferometría con fotones de fase determinada [148]. No hay dificultades mayores en llegar hasta unos 50 km. En 1999 un grupo de Los Álamos ha llegado por este procedimiento a 48 km [109, 108, 110]. Por eso puede ser usado para conectar con seguridad diversas agencias del Gobierno en Washington. Cubrir distancias superiores a 100 km requerirá el uso de repetidores seguros en los que se pueda generar material clave para la retransmisión.

De nuevo con el protocolo B92, se ha conseguido en 1998 transmitir cuánticamente clave secreta, a un ritmo de 5 kHz y a lo largo de 0.5 km en aire a plena luz del día, mediante fotones polarizados [108, 111]. En un futuro inmediato puede ser utilizado este procedimiento para generar claves secretas compartidas tierra-satélite que permitan proteger la confidencialidad de las transmisiones.

Finalmente, a finales de 1999 se ha logrado distribuir clave a lo largo de 1 km mediante un esquema variante del EPR y BB84, con pares de fotones enredados, a un ritmo de 0.4-0.8 kHz y error en los bits de un 3%. La famosa Venus “Von Willendorf”,[97], debidamente digitalizada, sirvió de mensaje [112].

3.9 “Qomputación”

Desde el modesto PC hasta el más potente superordenador, todos los ordenadores actuales se basan en los principios de la máquina de Turing, ideada por este inglés

[97] Estatua prehistórica (24-22 ka a.C.) hallada en Willendorf (Austria) en 1908.

en 1935. Pero desde hace unos pocos años se cuestiona la unicidad del modelo, y se han propuesto nuevos conceptos computacionales que van más allá de la tesis de Church-Turing según la cual todo lo "naturalmente" computable puede hacerse con una máquina de Turing y un programa adecuado. En último término, la física es la que determina qué es computable y qué no lo es. Como dice Deutsch: *Computers are physical objects, and computations are physical processes. What computers can or cannot compute is determined by the laws of physics alone, and not by pure mathematics.*

Recordemos la tesis original de Church-Turing (C-T): *La clase de funciones computables mediante alguna máquina de Turing, y la clase de funciones calculables mediante algún algoritmo, coinciden*.[98] Mientras que la primera clase está perfectamente definida, la segunda queda un tanto borrosa, como lo es la definición intuitiva de algoritmo o procedimiento: i/ conjunto finito de instrucciones precisas o inambiguas, ii/ su ejecución procede de forma que a cada instrucción sigue otra bien determinada, y iii/ se llega siempre a una instrucción final tras la realización de un número finito de ellas.

No se conoce excepción alguna a esta tesis de Church-Turing, pero tampoco se trata de un teorema. El futuro podría revelar procesos físicos que calculen algo que las máquinas de Turing no puedan hacer.

La exclusión de las máquinas de Turing cuánticas no afecta a la tesis C-T, pues todo lo que éstas calculan es también calculable con los ordenadores clásicos (aunque con menor eficiencia en determinados casos).

Cuando importan los recursos, y el coste polinómico es la señal de eficiencia, se refuerza la tesis C-T a lo que se llama la tesis fuerte de Church-Turing: *Cualquier modelo de computación es simulable en una MTP de modo eficiente*. El algoritmo de Shor arroja, sin embargo, intensas sombras sobre esta tesis fuerte.

Finalmente, Deutsch modificó en 1985 la tesis de C-T, elevándola a principio físico [64]: *Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means.*

3.9.1 Complejidad de los problemas

Sabemos que hay tres tipos de problemas: fáciles, duros e incomputables. De todos hemos visto ejemplos. Surge la cuestión de si pueden existir ordenadores que "calculen lo incalculable". Y como la respuesta reside en la física, la cuestión equivale a preguntarse si existen procesos físicos no computables. De ser así, bastaría montar un ordenador "sobre la chepa"de tal proceso para tener un computador capaz de calcular algo incalculable.

De poco nos sirve saber si un problema es soluble si el hallar su solución exige eones de tiempo o memorias del tamaño de la Tierra. Esto es lo que ocurre con los problemas duros o intratables. La simulación de sistemas cuánticos en ordenadores clásicos es uno de ellos: el espacio de los estados tiene una dimensión que crece exponencialmente con el tamaño del sistema a simular. Manin [146, 147], Benioff [14], y Feynman [79], se percataron de que esa simulación en ordenadores clásicos o máquinas de Turing era un problema de complejidad exponencial.[99] Feynman supo ver que esta dificultad podía ponerse al servicio del cálculo: un ordenador que

[98] *Every function which would naturally be regarded as computable can be computed by the universal Turing machine*. (Turing).

[99] Manin cita este párrafo de Poplavskii (1975): *The quantum-mechanical computation of one molecule of methane requires* 10^{42} *grid points. Assuming that at each point we have to perform only 10 elementary operations, and that the computation is performed at the extremely low temperature* $T = 3 \times 10^{-3}$ *K, we would still have to use all the energy produced on Earth during the last century.*

trabaje como un sistema cuántico podrá ser capaz de realizar cálculos más complejos que los ordenadores clásicos. Las bases teóricas de los qomputadores se deben a Deutsch [64]. Constan de registros cuánticos (colecciones de qubits coherentes), y puertas lógicas cuánticas (operaciones unitarias sobre los estados de los registros), con una red cuántica de conexiones que permiten tomar las salidas de unas puertas y llevarlas como entrada a otras, y al final uno o varios procesos de medición sobre los estados de los registros. El "paralelismo masivo" hay que entenderlo bien. La forma de actuar una función $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ en los ordenadores cuánticos es así: se le asocia una puerta lógica $U_f : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle$, en particular $U_f : |x\rangle \otimes |0\rangle \mapsto |x\rangle \otimes |f(x)\rangle$. Obsérvese por tanto que del resultado no se deducen todos y cada uno de los $f(x)$. Están todos ahí, pero superpuestos con enredo. Una medida bit a bit del primer registro proporcionará un valor de x y dejará el segundo registro en el estado correspondiente a $f(x)$. Pero es un tipo de información la que da que no se encuentra con ordenadores clásicos: es una información global, repartida entre todos los sumandos del estado enredado, y que requiere un tratamiento especial para ser extraída, una medida no diagonal en la base computacional $|x\rangle|y\rangle$. Lo veremos luego al presentar los algoritmos cuánticos más conocidos.

No se sabe aún qué tipo general de problemas pueden resolverse mejor con los cuánticos que con los clásicos. Se conocen casos particulares, como el de la factorización, o el cálculo de logaritmos discretos. Sería un gran estímulo probar que hay algún problema NPC soluble en tiempo polinómico con un ordenador cuántico. Muchos dudan de que la eficacia de la computación cuántica llegue a tanto.

3.9.2 Límite cuántico a la miniaturización

Según la ley empírica de Gordon Moore (cofundador de Intel), que recoge la evolución de los computadores en los últimos 30 años, cada 18 meses se duplica la velocidad de cálculo de los ordenadores y se reduce a la mitad el tamaño de los dispositivos lógicos con que los computadores almacenan y procesan información (o si se prefiere, el número de transistores en un chip clásico se multiplica por 2 cada 18 meses, mientras que el número de átomos para almacenar un bit se reduce a la mitad). A este paso, el fin de la miniaturización está muy próximo; para el año 2017 esos dispositivos lógicos alcanzarán, según la mencionada ley, tamaño atómico o molecular, y su comportamiento ostensiblemente cuántico será inevitable.[100] Se estima que en un par de décadas, por allá al 2020, los ordenadores operarán a unos 40 GHz, tendrán una memoria RAM de 160 Gb, y un consumo como el actual (unos 40 W) [213, 214].

Esta barrera física a la evolución de los computadores clásicos se torna en virtud insospechada gracias a las características cuánticas. En primer lugar, los bits o sistemas lógicos de dos estados (condensadores clásicos) dan paso a los qubits o sistemas cuánticos bidimensionales, donde aparte de los estados 0 (fundamental) y 1 (excitado) poseen otros estados intermedios, que ni son 0 ni 1, sino ambos a la vez, flotando en una niebla indefinida entre estos dos valores. Esto permite que los computadores cuánticos sean mucho más eficientes en principio que los clásicos.

[100] La tecnología actual permite construir detalles en los microchips inferiores a 0.25 μm. Los Pentium III tienen reglas de diseño de 0.18 μm, y se están desarrollando la tecnología de las 0.13 μm para los Pentium IV.) Con un orden de magnitud más pequeño, el efecto túnel podrá hacer que los electrones salten de unos hilos a otros (ver S. Benjamin y A. Ekert, en http://www.qubit.org/intros/nano/nano.html). Esto puede ocurrir ya en el 2012 (Nature, supplement, Dec 1999).

3.9.3 Ventajas de los ordenadores cuánticos

Aunque los dispositivos semiconductores de los ordenadores clásicos deben sus propiedades a la física cuántica, estos son clásicos en el sentido de que la información que procesan se registra en sistemas macroscópicos de 2 niveles. La diferencia entre computadores clásicos y cuánticos estriba en cómo se registra y se manipula la información, en si la base lógica es la lógica de Boole o la lógica cuántica.

El paralelismo masivo en los computadores cuánticos permite en principio una potencia de cálculo que sobrepasa con creces las posibilidades clásicas. Con 300 qubits la dimensión del espacio de estados es $2^{300} = 2 \times 10^{90}$, y por tanto el número de operaciones en paralelo realizadas supera al número de átomos del Universo visible. Con un centenar de qubits un ordenador cuántico ideal podría ya competir favorablemente con los mayores ordenadores hoy existentes; y unos miles de qubits bastarían para simular con precisión suficiente la cromodinámica y gravitación cuánticas [140].

Los ordenadores cuánticos, teóricamente, factorizan a más velocidad, buscan en bases de datos con mayor rapidez, y simulan de modo más eficiente que los ordenadores clásicos a los sistemas cuánticos.

3.9.4 Infortunios de los ordenadores cuánticos

El problema de la descoherencia es muy serio. Si T es el tiempo de relajación de 1 qubit (desexcitación), y t el tiempo de operación de una puerta lógica, $R = T/t$ (figura de mérito) debe ser grande para que el computador funcione: ha de ser al menos del orden del (número de qubits)$\times$(número de actuaciones de puertas). Para factorizar un número de 4 bits harían falta unas 20,000 operaciones de puertas sobre unos 20 qubits; así que R debería superar 400,000, cifra muy optimista para los modernos sistemas ópticos. Y no digamos para un número de 400 bits: R escala al menos como el (tamaño)^3, y tendría que ser R del orden de 4×10^{11}, impensable por el momento, pues con t del orden de 10^{-4} s (como en la trampa de iones del NIST[101]), el tiempo de relajación debería superar el año [102]. Podría pensarse, para los computadores basados en trampas de iones, en aumentar la intensidad de los pulsos láser inductores de las transiciones, con el fin de disminuir t; pero esto conlleva una disminución de T, por la posibilidad de provocar transiciones no deseadas al estado excitado que por caída espontánea arruinarían la coherencia del qubit. De no remediarse el problema de la descoherencia, más allá de la factorización de un número de unos pocos bits no se podrá llegar.

Pero aunque nunca se lograra fabricar computadores cuánticos complejos, su estudio y simulación con unos cuantos bits proporcionará sin duda una visión y entendimiento más profundo de la teoría más antiintuitiva jamás descubierta por el hombre.

3.9.4.1 ¿Es el cerebro un qomputador? Algunos autores, entre los que destaca el matemático y relativista Roger Penrose, se empeñan en sostener que el cerebro funciona como un ordenador cuántico. Por ejemplo, Penrose sitúa en los microtúbulos la acción cuántica y la consciencia. Sin embargo, los investigadores convencionales en procesos cognoscitivos que trabajan sobre modelos de redes neuronales pueden seguir tranquilos con sus investigaciones sobre bases clásicas. Se demuestra que los tiempos de coherencia de las neuronas (10^{-20} s) y de los microtúbulos (10^{-13} s) son más de 10 órdenes de magnitud menores que los tiempos dinámicos de los procesos cognoscitivos (10^{-2}-10^{0} s). También el disparo de las neuronas es clásico (tiempos del orden de

[101] National Institute of Standards and Technology.

10^{-4}-10^{-3} s), así como el de las excitaciones de polarización en microtúbulos (10^{-7}-10^{-6} s). Luego no parece razonable esperar coherencia, es decir, un comportamiento cuántico en el cerebro [202].

3.9.5 Ordenadores cuánticos en miniatura

El procesado de información cuántica se viene haciendo a nivel elemental desde hace medio siglo; por ejemplo, una transición estimulada entre 2 niveles es un caso de operación NOT, y una transición forzada en un sistema de 4 niveles simula la puerta XOR o CNOT.

En 1995 Cirac y Zoller [56] propusieron un método elegante e ingenioso para realizar un computador cuántico con unos cuantos qubits (de 10 a 40): iones muy fríos (temperaturas inferiores al mK) con un par de estados relevantes y de larga vida (por ejemplo estados hiperfinos con vidas de millares de años), atrapados y dispuestos en línea en una trampa de Paul con alto vacío (10^{-8} Pa), y un láser con varios subhaces obtenidos mediante divisores y moduladores acústico-ópticos (dos subhaces incidentes sobre cada ión) con los que pueden simularse cualesquiera puertas monarias. Para la puertas binarias se recurre a la interacción culombiana entre los iones, que provoca los modos de vibración traslacionales de la ristra iónica en el potencial de la trampa tan pronto como uno de ellos se mueve, por ejemplo bajo la acción de un haz láser.

Desgraciadamente, no parece viable esta técnica para ir más allá de unas decenas de iones, por lo que su aplicación a la factorización no podrá competir con la eficacia de los ordenadores clásicos.[102]

Hay otras propuestas alternativas, como la basada en resonancia magnética nuclear (RMN), en la que los qubits son estados de spin de núcleos en moléculas, manipulados mediante campos magnéticos oscilantes. En este método se manejan del orden de $O(10^{20})$ spines, y se miden polarizaciones medias del líquido que los alberga. Con esta técnica RMN en líquidos se han simulado puertas binarias y ternarias, se han implementado la transformación de Fourier cuántica y la teleportación, y se han realizado experimentos en que intervienen hasta 7 qubits. Pero no parece factible ir con ella mucho más allá de 10 qubits [88].

Finalmente, hay un proyecto interesante, debido a Kane, para construir un ordenador cuántico con tecnología convencional de estado sólido [119, 120, 88]. De momento, no ha habido implementación experimental alguna de este tipo de qomputador basado en el silicio.

3.9.6 Algunos algoritmos cuánticos

Un algoritmo cuántico es un proceso físico que realiza alguna tarea computacional apoyándose en un sistema cuántico. Usa qubits en lugar de bits, y puertas unitarias en lugar de puertas clásicas booleanas. La evolución cuántica es intrínsecamente más compleja (en el sentido de la teoría de la complejidad computacional) que la evolución clásica. Mientras cualquier estado de los 2^N de un conjunto de N bits queda especificado por N bits, el estado de N qubits requiere especificar los 2^N números que representan las amplitudes de la superposición. Por eso un sistema cuántico tiene una capacidad exponencialmente mayor que uno clásico para almacenar información. Pero

[102] Se estima (J. Preskill, conferencia titulada *Quantum Information and Quantum Computation*, 18 mayo de 1996, en http://www.theory.caltech.edu/people/preskill/index.html) que para factorizar un número de $n =$ 130 dígitos haría falta una trampa con 2160 iones, y habría que aplicar a este registro unos 30×10^9 pulsos láser. El número de iones crece linealmente con n, y el número de pulsos lo hace como n^3.

esta información está escondida, y sólo es extraíble una parte muy pequeña de ella. El resto es inaccesible. A pesar de ello, la poca que se puede extraer es en ocasiones de una calidad excepcional, pues su obtención clásica requeriría un esfuerzo exponencialmente mayor. Precisamente los algoritmos cuánticos buscan revelar esa información difuminada por el todo.

La MQ hace también que el procesado de la información sea exponencialmente más efectiva que la clásica. Por ejemplo, la acción de una puerta monaria U sobre un estado enredado de N qubits requeriría clásicamente el cálculo de 2^{N-1} matrices unitarias, una para cada estado base computacional de los $N-1$ qubits restantes. Cuánticamente, sin embargo, la puerta U supone una sola actuación.

Para explotar las potencialidades de los ordenadores cuánticos se han ideado algoritmos específicos, entre los que destacan los siguientes:

- Algoritmo XOR de Deutsch [64], o "cómo matar dos pájaros de un tiro".[103]
- Algoritmo de Grover [99, 100], o "cómo hallar una aguja en un pajar".
- Algoritmo de Simon [195], o "cómo averiguar, en tiempo polinómico, el período de una cierta función".
- Algoritmo de Shor [191], o "cómo factorizar en tiempo polinómico".

El algoritmo de Grover supone una mejora cuadrática sobre el método clásico de búsqueda, y los otros tres mejoran exponencialmente los algoritmos clásicos conocidos. Todas estas mejoras son esencialmente debidas al enredo.[104]

Son escasos los algoritmos cuánticos conocidos. ¿Falta de imaginación? ¿O falta de problemas cuya solución pueda acelerar de forma esencial la computación cuántica? Shor deja en el aire la respuesta [194].

3.9.6.1 Algoritmo de Grover Los algoritmos de Grover y de Shor (este lo veremos luego) son las joyas de los algoritmos cuánticos conocidos. A pesar de su limitado poder de aceleración, el algoritmo de Grover es sumamente importante. El problema a resolver es el de encontrar el elemento (que por sencillez suponemos único) de una lista que cumple una cierta condición. Ejemplo: nos dan una guía de teléfonos y un número, y nos piden buscar a quién corresponde. Si la lista tiene N entradas, necesitaremos una media de $\frac{1}{2}N$ búsquedas hasta dar con el titular de ese número telefónico. El algoritmo de Grover rebaja el número de consultas a $O(\sqrt{N})$, como vamos a ver. Se demuestra que este resultado del algoritmo de Grover es óptimo para listas genéricas, totalmente desestructuradas [21, 220].

Puede formularse el problema que nos concierne así: Nos dan un oráculo que calcula una función $f(x), x = 1, \ldots, N$, de la que sabemos que es un predicado, es decir, sus respuestas son siempre 0 o 1, y que sólo toma el valor 1 para un único valor x_0 del argumento. Se trata de conocer x_0. Sólo puede mejorarse la aceleración cuadrática del algoritmo de Grover dando más información sobre el colectivo en el que hay que buscar, y utilizándola inteligentemente, como en el caso de funciones periódicas con

[103] Este algoritmo se conoce también como algoritmo de Deutsch-Jozsa [66]. Su presentación ha sido mejorada en [58].

[104] Lloyd [141] ha demostrado que el algoritmo de búsqueda no requiere el enredo, y puede realizarse con igual eficiencia $O(\sqrt{N})$ que el de Grover tanto con ondas clásicas como cuánticas, gracias tan sólo a la interferencia. Lo único es que su implementación tiene un coste exponencialmente mayor en recursos que el de Grover, a saber, $O(N)$ versus $O(\log_2 N)$.

el algoritmo de Shor. Sugieren estos resultados que la computación cuántica puede encontrarse con un grado de dificultad comparable con el de la computación clásica en lo que se refiere al problema central de ver si las clases P y NP son iguales.

Formemos un registro de $n = \lfloor \log_2 N \rfloor + 1$ qubits. Sean los operadores unitarios de Grover $U_{x_0} := 1 - 2|x_0\rangle\langle x_0|$, $U_{k_0} := 1 - 2|k_0\rangle\langle k_0|$, donde $|x_0\rangle$ es el elemento de la base computacional asociado al número en binario que representa al entero x_0, y $|k_0\rangle := |k = 0\rangle$ es el elemento $2^{n/2}\sum_0^{2^n-1}|i\rangle$ de la base dual Fourier.

Formemos el núcleo de Grover $G := -U_{k_0}U_{x_0}$. Entonces [87, 88]:

$$|\langle x_0|G^m|k_0\rangle|^2 > 1 - O(2^{-n}), \text{ si } m \approx (\pi/4)2^{n-1}.$$

La iteración del núcleo de Grover sobre el estado de población uniforme $|k_0\rangle$ va amplificando la presencia del estado buscado $|x_0\rangle$, de modo que la probabilidad de encontrar $|x_0\rangle$ crece hasta aproximarse a 1, para luego apartarse variando sinusoidalmente. Luego la iteración de G sobre $|k_0\rangle$ un número conveniente de veces nos lleva a un estado sobre el que la lectura en la base computacional (medida de todos los qubits) conduce casi con seguridad al estado buscado $|x_0\rangle$.

Puede dar la impresión de que el algoritmo de Grover presupone conocer la solución x_0 buscada, ya que usa el operador U_{x_0}. No es así, pues la acción de este operador se implementa mediante un circuito (la puerta que calcula el predicado) que comprueba, para cada entero k, si coincide o no con x_0, es decir, si $f(k) = 1$ o 0, y en consonancia deja invariante $|k\rangle$ o lo multiplica por -1, según el caso. Una cosa es *conocer* la solución, y otra, muy distinta, *reconocerla*. El oráculo del algoritmo de Grover se limita a reconocerla cuando se la encuentra.

Este algoritmo tiene extensión elemental al caso en que $|f^{-1}(1)|$ es un entero $k \geq 1$ conocido [43]. También se puede generalizar al cálculo de la media y la mediana de un conjunto de números, y de su máximo y mínimo [71]. Y combinado con el algoritmo de Shor para hallar períodos permite calcular el número k de soluciones a la búsqueda en lugar de sus lugares concretos [48].

3.9.6.2 Algoritmo de Shor Escribía el genial Gauss (art. 329 de DISQUISITIONES ARITMETICÆ, 1801): *El problema de distinguir entre los números primos y los compuestos, y de descomponer estos últimos en sus factores primos, es uno de los más importantes y útiles de toda la aritmética ... La dignidad de la ciencia misma exige que se exploren todas las vías para encontrar solución a problema tan distinguido y celebrado.*

Ya vimos que la cuestión de la primalidad está en ZPP, por lo que a efectos prácticos es un problema tratable. No ocurre lo mismo con el problema de la factorización, a pesar de que los últimos treinta años han sido testigos de un progreso muy considerable en esta cuestión.

Todos conocemos algoritmos elementales (dividir sucesivamente por los enteros $2, \ldots, \lfloor\sqrt{N}\rfloor$) que permiten dilucidar si un entero N es primo o compuesto, y en el último supuesto, hallar sus factores primos. Pero la eficiencia de esos algoritmos es muy pobre (requiere un tiempo exponencial en la longitud de N), de modo que con ellos, cuando el entero tiene unas decenas de dígitos en base 10, incluso un ordenador actual podría tardar eones en llegar a una respuesta.

Ya citamos anteriormente los mejores algoritmos conocidos; son todos subexponenciales, pero superpolinómicos.

A principios de los 70 el límite práctico estaba en números a factorizar de unos 20 dígitos decimales. El método de Fermat-Kraitchik (fracciones continuas) es de com-

plejidad $T \sim O(\exp[c\,(\log N \log\log N)^{1/2}])$, con $c = \sqrt{2} = 1.414\ldots$. Su primer éxito (1975) fue la factorización del número de Fermat F_7:[105]

$$F_7 := 2^{2^7} + 1 = 59649589127497217 \times 5704689200685129054721$$

Este algoritmo de factorización basado en fracciones continuas elevó en 1980 el límite a unos 50 dígitos.

Esta longitud pasaría a unos 120 dígitos con el algoritmo de la criba cuadrática [170, 96, 171] en 1990. La complejidad de este nuevo algoritmo es también $T \sim O(\exp[c\,(\log N \log\log N)^{1/2}])$, pero con $c = 3/2\sqrt{2} = 1.06066\ldots$. Entre sus éxitos figura la ya citada factorización, en 1994, del número RSA-129 de 426 bits.

En la actualidad el mejor algoritmo disponible es el GNFS o criba general de cuerpos de números [135, 171]; como dije anteriormente, con este potente método se consiguió factorizar en 1999, tras 8000 MIPS-años, el número RSA-155 (512 bits).

Sabemos que su complejidad es $O(\exp(c\,(\log N)^{1/3}(\log\log N)^{2/3})$, con $c = (64/9)^{1/3} + o(1) = 1.922999\ldots + o(1)$. Tomando como referencia el tiempo de 8000 MIPS-años empleado en factorizar el número RSA-155, y suponiendo aplicable la ley empírica de Moore[106] (duplicación de la potencia de cálculo cada 18 meses) durante una veintena de años más, puede obtenerse la Tabla 2 para los tiempos de factorización con 1000 estaciones de trabajo crecientes en potencia según la ley de Moore (a partir de 800 MIPS en el 2000).

$l(N)$	512	1024	2048	4096
t_{fact}(2000)/año	0.01	10^5	10^{14}	10^{26}
t_{fact}(2010)/año	10^{-4}	10^3	10^{12}	10^{24}
t_{fact}(2020)/año	10^{-6}	10	10^{10}	10^{22}

Tabla 2: Tiempos de factorización (en años) con el algoritmo GNFS, de enteros N de $l(N)$ bits, con potencias de cálculo del año 2000 y las previsibles para el 2010 y 2020.

Es fácil ver que con el algoritmo GNFS la factorización de un entero de 2000 dígitos decimales con un ordenador del tamaño del Sistema Solar llevaría más del tiempo de vida del Sol en la secuencia principal. A la vista de estas cifras, es claro que los criptógrafos cuya seguridad descansa en la dificultad de factorizar enteros de unos centenares de dígitos pueden dormir tranquilos unos cuantos años, hasta que en algún momento surja alguien que invente un algoritmo mucho más eficaz que el GNFS. Ese alguien se llama Peter Shor,[107] y el momento histórico fue 1994.

En 1994 Shor intentó hallar algún problema que no fuera académico y a cuya solución el formalismo cuántico proporcionase una ventaja esencial. Se dio cuenta de que la factorización (tan importante en criptografía) era reductible a un problema de hallar un período, y se inspiró en los resultados de Simon que antes hemos mencionado y que

[105] Se sabe que $F_{0,1,2,3,4}$ son primos. Euler factorizó F_5: $F_5 = 641 \times 6700417$. Se conjetura que todos los $F_n, n \geq 5$, son compuestos. Para F_{5-11} se conoce su factorización completa, e incompleta para F_{12-32} (con excepción de los casos $n = 14, 20, 22, 24$, para los que sólo se sabe que F_n es compuesto). Se desconoce si F_{33-35} son o no primos. Hasta el momento se sabe de 190 números de Fermat que son compuestos, siendo F_{382447} el mayor de ellos (es divisible por el primo $3 \times 2^{382449} + 1$).

[106] Dentro de un par de décadas se alcanzará el límite atómico/molecular en el proceso de miniaturización de los componentes electrónicos, por lo que supondremos que esa ley es válida sólo hasta el 2020, aproximadamente.

[107] Premio Nevalinna en el Congreso Internacional de Matemáticas, Berlin 1998.

mostraban cómo la computación cuántica ayudaba al cálculo eficiente del período de una función periódica.[108]

Sea $N \geq 3$ el entero impar a factorizar. Sea a un entero arbitrario en $(1, N)$. Lo podemos suponer coprimo con N (de lo contrario el $\mathrm{mcd}(N, a)$ sería un divisor f no trivial de N, y reanudaríamos la discusión partiendo de N/f). Sea $r := \mathrm{ord}_N a$ el orden de a mod N, esto es, el menor entero tal que $a^r = 1 \bmod N$. Pueden ocurrir tres casos: 1/ r es impar; 2/ r es par y $a^{r/2} = -1 \bmod N$; y 3/ r es par y $a^{r/2} \neq -1 \bmod N$. Este último caso es el que interesa, pues, de darse, $\mathrm{mcd}(N, a^{r/2} \pm 1)$ proporcionan evidentemente factores no triviales de N: en efecto, $a^{r/2} - 1$ no es múltiplo de N por ser r el orden de a mod N, y $a^{r/2} + 1$ tampoco lo es por hipótesis. Como su producto sí es múltiplo de N, forzosamente cada uno de ellos debe compartir con N algún factor primo.

Se demuestra que, fijado $N \geq 3$ entero impar arbitrario, la probabilidad de que, escogido a al azar entre los enteros en $(1, N)$ coprimos con N, cumpla el supuesto 3/, es decir, sea de orden r mod N par y $a^{r/2} \neq -1 \bmod N$, es $\geq 1 - 2^{-k+1}$, donde k es el número de primos distintos en la factorización de N. Por otro lado, la probabilidad de que $a \in (1, N)$ sea coprimo con N es $p(N) \geq \mathrm{e}^{-\gamma}/\log\log N$ para $N \gg 1$, siendo $\gamma = 0.5772156649\ldots$ la constante de Euler [75]. Luego, salvo si N es potencia de un solo primo (caso que no consideraremos, por ser de factorización trivial [60]), la probabilidad de que un a aleatorio en $(1, N)$ cumpla $\mathrm{mcd}(a, N) > 1$ o bien sea coprimo con N y conduzca al caso 3/ es $\geq 1 - p(N) + \frac{1}{2}p(N) = 1 - \frac{1}{2}p(N)$. Eligiendo aleatoriamente algunos valores para $a \in (1, N)$ podremos conseguir así con alta probabilidad un divisor no trivial de N, a través del $\mathrm{mcd}(a, N)$ (si $\mathrm{mcd}(a, N) > 1$), bien a través del $\mathrm{mcd}(N, a^{r/2} \pm 1)$ (si $\mathrm{mcd}(a, N) = 1$).

Ejemplo: sea $N = 16163174827$, y $a = 15436641538$, tomado al azar en $(1, N)$. Se cumple $\mathrm{mcd}(N, a) = 1$. El orden de a mod N es $r = 4040725654$. Evidentemente r es par, y $a^{r/2} = 1221625641 \bmod N$. Luego estamos en el caso 3/; como $\mathrm{mcd}(N, a^{r/2} - 1) = 87509$ y $\mathrm{mcd}(N, a^{r/2} + 1) = 184703$, concluimos que 87509 y 184703 son divisores de N.

¿Dónde se esconde el elevado coste de la factorización en este procedimiento? En el cálculo del orden r, para el que los algoritmos clásicos conocidos tienen eficiencias no polinómicas. Y aquí es donde interviene la brillante idea de Shor, que se apoya en las interferencias cuánticas para desentrañar el valor de $\mathrm{ord}_N a$, convirtiendo el problema en uno de complejidad BQP (que luego definiremos).

El algoritmo de Shor, como el de Simon, consigue explotar la periodicidad a través del paralelismo masivo de la computación cuántica para encontrar lo que se busca de un modo eficiente. (Es como en la difracción por una red periódica. Midiendo la posición de uno sólo de sus átomos no nos da información alguna sobre el espaciado de la red. Pero difractando con ella un sólo fotón y midiendo su dirección de salida, que sabemos que preferentemente va a ser una dirección de máximo (Bragg), se puede extraer información sobre el período de la red.) Calcula en tiempo $\mathrm{pol}(n)$ el período r de cualquier función $f : \{0,1\}^n \to \{0,1\}^m$ cuya evaluación sea también de complejidad polinómica. Es el caso del orden r de un número entero a mod N: ahora $m = n$, y n es el número de bits de N.

Los algoritmos clásicos del cálculo del orden r mod N de un entero a coprimo con N son, como acabamos de decir, muy lentos. Para hallar el orden de a cuando N tiene unos 200 dígitos decimales pueden hacer falta del orden de 10^{150} multiplicaciones. Aunque

[108] El algoritmo de Shor para el cálculo del orden r de un entero a módulo N es un caso particular de un problema más general que admite una resolución similar, y que contiene como otros casos particulares el cálculo de logaritmos discretos, de períodos, de estabilizadores abelianos, el problema de Simon, etc. Es el problema de búsqueda de subgrupos ocultos.

un ordenador realizase 10^{12} multiplicaciones por segundo, se tardaría unos 10^{80} años. Se sabe que r es un divisor de $\phi(N)$ (el orden del grupo $(\mathbb{Z}/N\mathbb{Z})^*$) [216]. Pero no se conoce método rápido de conocer $\phi(N)$ a no ser que se conozca la factorización de N. También se sabe que el mayor valor de r es $\lambda(N)$, la función de Carmichael (mcm $(\lambda(p_1^{n_1}), \lambda(p_2^{n_2}), \ldots, \lambda(p_k^{n_k}))$, donde $p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ es la descomposición en primos de N; $(\lambda(p) = p-1$, $\lambda(p^n) = \phi(p^n)$ si el primo p es > 2, $\lambda(2^n) = \phi(2^n)$ si $n = 0, 1, 2$, y $\lambda(2^n) = (1/2)\phi(2^n)$ si $n > 2)$. Y se sabe que todo orden es divisor de $\lambda(N)$, que es generalmente mucho menor que $\phi(N)$. Pero tampoco se conoce un método eficiente para calcular $\lambda(N)$, a no ser que se conozca la factorización de N.

Para el algoritmo de Shor necesitamos, como ya es usual, dos registros cuánticos; ahora uno con $K_1 := \log_2 Q$ qubits, donde $Q = 2^{K_1} \in (N^2, 2N^2)$, y otro con $K_2 := \lceil \log_2 N \rceil$ qubits. En cada uno de esos registros los estados cuánticos pueden representarse en la llamada base computacional asociada $|x\rangle := |x_{K-1}\rangle \otimes \ldots \otimes x_0$, con $x = 0, \ldots, 2^K - 1$ y $x := x_{K-1} 2^{K-1} + \ldots + x_0$ la expresión de x en base 2. Así, para $K = 4$, $|6\rangle = |0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |0\rangle$. Los pasos a seguir son éstos:

1/ Iniciamos los registros en el estado global $\psi_1 := |0\rangle \otimes |0\rangle$.

2/ A continuación se aplica al primer registro la transformación de Fourier discreta cuántica (QFT) F_Q en $\mathbb{Z}_Q := \mathbb{Z}/Q\mathbb{Z}$. El estado inicial ψ_1 pasa a ser $\psi_2 := Q^{-1/2} \sum_{q=0}^{Q-1} |q\rangle \otimes |0\rangle$.

3/ A continuación, actuamos sobre este último estado con la puerta $U_f : |q\rangle \otimes |0\rangle \mapsto |q\rangle \otimes |f(q)\rangle$, donde $f(q) := a^q \bmod N$.

De una sola tacada, esta operación calcula $f(q)$ ¡para todos los q a la vez! (paralelismo cuántico masivo), produciendo el estado $\psi_3 := Q^{-1/2} \sum_{q=0}^{Q-1} |q\rangle \otimes |f(q)\rangle$.

4/ La periodicidad de $f(q)$ (periodo r) hace que la medición (ideal) ahora del estado del segundo registro, con el resultado $|b\rangle$, proyecte al sistema total en una superposición $\psi_4 := B^{-1/2} \sum_{q \in f^{-1}(b)} |q\rangle \otimes |b\rangle = B^{-1/2} \sum_{k=0}^{B-1} |d_b + kr\rangle \otimes |b\rangle$, donde $d_b < N$ es el mínimo entero no negativo tal que $f(d_b) = b$, y $B := 1 + \lfloor (Q - 1 - d_b)/r \rfloor$ ($\sim Q/r$ para $N \gg 1$) la longitud de la serie.

El primer registro se halla ahora en un estado que es superposición periódica de estados base. Si decidiéramos medir sobre él, no obtendríamos información acerca del período r, pues esa medición se limitaría a proyectar sobre uno de los estados $|d_b + kr\rangle$. Una nueva aplicación de la QFT va a realizar el milagro de permitirnos "destapar" r.

5/ Aplicando F_Q al primer registro, y midiendo este a continuación, la probabilidad de encontrarlo con estado $|q\rangle$ resulta

$$\mathrm{prob}(q) = \frac{1}{QB} \left| \sum_{k=0}^{B-1} \left(\mathrm{e}^{2\pi i q r/Q} \right)^k \right|^2 .$$

Veamos cómo del estudio de esta probabilidad podemos extraer el periodo r. El análisis de la serie geométrica en $\mathrm{prob}(q)$ revela que esta probabilidad está concentrada alrededor de aquellos q para los que todos los complejos del sumatorio caen en un mismo semiplano de $\mathbb{C}$, y por tanto se refuerzan constructivamente. Tales q se caracterizan por satisfacer $|(qr \bmod Q)| \leq \frac{1}{2} r$, y para ellos, que son en número de r, se prueba que $\mathrm{prob}(q) \geq (2/\pi)^2 r^{-1}$, por lo que la probabilidad de dar con alguno de ellos es $\geq (2/\pi)^2 = 0.405\ldots$ Los picos o "máximos de difracción" de $\mathrm{prob}(q)$ están en las vecindades de $\lfloor sQ/r \rfloor$, $s \in \mathbb{Z}$.

La condición de interferencia constructiva para q equivale a la existencia de un $0 \leq q' < r$ tal que $|(q/Q) - (q'/r)| \leq \frac{1}{2} Q^{-1}$. Como hemos elegido $Q > N^2$, y $r < N$, existe a lo sumo una fracción q'/r, que satisface esa desigualdad y tiene un denominador

$r < N$.[109] En ese caso, este número racional q'/r puede hallarse fácilmente a través de los aproximantes o convergentes del desarrollo de q/Q en fracción continua. Si este aproximante es la fracción irreductible q_1/r_1, puede ocurrir que $a^{r_1} \equiv 1 \bmod N$, en cuyo caso $r = r_1$, y habremos concluido. De lo contrario, sólo sabemos que r_1 es divisor de r, y tendremos que continuar, eligiendo otro q de interferencia constructiva, a ver si esta vez hay más suerte. Se demuestra que la probabilidad de dar con un q adecuado es del orden $O(1/\log\log r)$, y por tanto con un número $O(\log\log r)$ de ensayos es sumamente probable que obtengamos r.

Ejemplo ficticio: Sea $N = 16163174827$, y $a = 15436641538$. Debemos entonces tomar $Q = 2^{68}$. Supongamos que tras implementar experimentalmente el algoritmo de Shor y medir el estado del primer registro, obtenemos $q = 34590527603422562$.[110] El desarrollo en fracción continua de q/Q es $[0, 8532, 1, 1, 1, 1, 1, 5, 25, 4, 7, 6, 1, 186, 1, 2, 3, 2, 1, 2, 1, 18, 5, 3, 8, 1, 3, 10, 1, 1, 13]$, y tiene un convergente q_1/r_1 que satisface $|(q/Q) - (q_1/r_1)| \leq \frac{1}{2}Q^{-1}$, a saber, $q_1/r_1 = 236781/2020362827$. Luego el período r buscado es múltiplo de r_1. Probando, se ve inmediatamente que $a^{r_1} \bmod N \neq 1$, $a^{2r_1} \bmod N = 1$, por lo que $r = 4040725654$.

De este modo se calcula un presunto r. Repitiendo el proceso un número $O(\log\log N)$ de veces obtendremos un valor r' tal que $a^{r'} = 1 \bmod N$, y por tanto $r = r'$.

Todo esto está muy bien. Pero, ¿cuánto "cuesta"? En primer lugar, tenemos una Hadamard (primera QFT), con coste lineal en $\log_2 N$, pues actúa bit a bit. Luego tenemos el cálculo de la función $a^x \bmod N$ para todo x. Se demuestra [216] que su coste en tiempo es $O(\log_2^2 N \log_2\log_2 N \log_2\log_2\log_2 N)$. Y finalmente una segunda QFT. Debido a que F_Q transforma la base computacional en otra base sin enredo, esto es, con vectores factorizables, es posible una implementación sumamente eficiente de la QFT, con $O(\log_2^2 N)$ puertas [88].[111] De aqui el coste total $O(\log_2^{2+\varepsilon} N)$ para hallar el orden r de $a \bmod N$, con una probabilidad $O(1)$ de éxito. Si ahora tenemos en cuenta que hay que calcular m.c.d.$(a^{r/2} \pm 1, N)$ para lograr finalmente algún factor de N, y que el m.c.d. de dos números del orden de N cuesta $O(\log_2^3 N)$ (con el algoritmo clásico de Euclides), éste será el coste total de la factorización (fijada una probabilidad de fracaso tan pequeña, pero no nula, como se desee).[112]

La Tabla 3 contiene estimaciones del tiempo de factorización mediante el algoritmo de Shor, así como de los números de qubits y puertas necesarios [107].

$l(N)$	512	1024	2048	4096
# qubits $(5l(N)+4)$	2564	5124	10244	20484
# puertas $(\sim 25l^3(N))$	10^9	10^{10}	10^{11}	10^{12}
t_{fact}	34 s	4.5 min	36 min	4.8 horas

Tabla 3: Tiempos de factorización, con el algoritmo de Shor, de enteros N de $l(N)$ bits, mediante un computador cuántico de 100 MHz de frecuencia nominal de reloj.

[109] Pero puede que no exista. Por ejemplo, si $N = 16163174827$, $Q = 2^{68}$, y $q = 34590527603422561$, no existe ninguna fracción q'/r, con $r < N$, que satisfaga $|(q/Q) - (q'/r)| \leq \frac{1}{2}Q^{-1}$. Pues de existir, debería ser un convergente a q/Q con denominador $< N$, y explícitamente se comprueba en este caso que tal convergente no existe.

[110] La probabilidad de que esto ocurra es $O(1/r)$, concretamente 1.5×10^{-10}; es muy baja, pero el resultado final no cambia para los r valores de q que pueden obtenerse con probabilidades similares.

[111] Exits un algoritmo debido a Kitaev [122] para evaluar en tiempo polinómico el orden r de un entero a módulo un entero N con el que es coprimo, y que no utiliza la transformación cuántica de Fourier.

[112] En realidad, el coste del cálculo del mcd puede rebajarse a $O(\log_2^2 N)$, incluso a $O(\log_2 N(\log_2\log_2 N)^2 \log_2\log_2\log_2 N)$, por lo que $O(\log_2^2 N \log_2\log_2 N \log_2\log_2\log_2 N)$ representa, por tanto, el coste total de la factorización. (Ver [128], p 339, problema 32, y solución en p 598).

Conviene observar que aunque el algoritmo de Shor permite factorizar en tiempo polinómico no es razonable esperar por ello que cualquier problema NP admita solución en tiempo polinómico con un ordenador cuántico, pues, como ya se dijo, muy probablemente COMP $\not\subseteq$ NPC.

No quantum computer can ever be built that can outperform a classical computer if the latter would have its components and processing speed scaled to Planck units, dice Gerardus 't Hooft [204]. Sostiene este galardonado físico que ningún ordenador cuántico podrá factorizar enteros de más de unos pocos miles de dígitos decimales. Arguye que siendo del orden de $10^{\sqrt{N \log_{10} N}}$ la memoria requerida y el número de operaciones a ejecutar para factorizar un entero N, y dado que un ordenador razonable podría tal vez ocupar unos 10^{120} volúmenes Planck, sólo tendría capacidad para poder factorizar clásicamente un entero del orden de 10^{4000}. Luego 't Hooft pronostica que ningún ordenador cuántico podrá superar este récord. El tiempo lo dirá.

3.9.7 Cálculo contrafactual

Llámase efecto *contrafactual* a un efecto físico cuyo resultado depende de una cierta eventualidad que pudiera ocurrir pero que de hecho no ha sucedido, es decir, de una cierta alternativa potencial que no ha ocurrido [115, 214].

Supongamos un interferómetro Mach-Zehnder, con un par de divisores de haz $\mathrm{DH}_{1,2}$, dos espejos $\mathrm{E}_{1,2}$, y dos detectores $\mathrm{D}_{1,2}$ tras el último DH. Imaginemos una disposición esquemática en que DH_1 y E_1 son vértices izquierdo y derecho de la base de un rectángulo, y E_2, DH_2 los extremos (izquierdo y derecho) del lado opuesto. El detector D_1 está en la línea E_2, DH_2, a la derecha del divisor, y el detector D_2 está en la línea E_1, DH_2, por encima del divisor. En las reflexiones especulares la fase de los fotones cambia en π; en un divisor de haz, el haz reflejado desplaza su fase en $\frac{1}{2}\pi$. Por eso, si los dos caminos ópticos, (DH_1, E_1, DH_2) y (DH_1, E_2, DH_2), son exactamente iguales, la luz que incide por la izquierda sobre DH_1 no llega al detector D_2 y sólo dispara el D_1.

Si al interferómetro de Mach-Zehnder le intercalamos unos desfasadores $-\pi/2$, los divisores de haz se comportarán como puertas de Hadamard.

Supongamos un ordenador interpuesto en el brazo (E_1, DH_2) del interferómetro, que decide si un número es primo o no, poniendo un registro R en los valores $r = 1, 0$, respectivamente. Suponemos que ese registro está inicializado a 0, antes de realizar el cálculo. El estado $|\mathrm{qc}\rangle$ indica el ordenador en estado inicial, con un dato inicial X cuya primalidad ha de averiguar. Al terminar un cálculo, vuelve a este estado inicial. Con $|\mathrm{N}\rangle$ ($|\mathrm{S}\rangle$) indicamos un estado de fotón en el interior del interferómetro que no (sí) dispara el qomputador. Mandamos un fotón $|\mathrm{H}_1\rangle$ al divisor DH_1 desde la izquierda, y así formamos el estado conjunto $|\mathrm{H}_1, \mathrm{qc}, 0\rangle$.

Tras atravesar DH_1 y su desfasador, el estado inicial $|\mathrm{H}_1, \mathrm{qc}, 0\rangle$ cambia así:

$$|\mathrm{H}_1\rangle|\mathrm{qc}\rangle|0\rangle \mapsto 2^{-1/2}(|\mathrm{N}\rangle + |\mathrm{S}\rangle)|\mathrm{qc}\rangle|0\rangle.$$

Dejamos pasar el tiempo preciso para que el ordenador realice el cálculo en el caso de que le llegue el fotón S, y el estado anterior cambia como sigue:

$$2^{-1/2}(|\mathrm{N}\rangle + |\mathrm{S}\rangle)|\mathrm{qc}\rangle|0\rangle \mapsto -2^{-1/2}(|\mathrm{N}\rangle|\mathrm{qc}\rangle|0\rangle + |\mathrm{S}\rangle|\mathrm{qc}\rangle|r\rangle).$$

Finalmente, el fotón atraviesa DH_2 y sus desfasadores, con lo que

$$-2^{-1/2}(|N\rangle|qc\rangle|0\rangle+|S\rangle|qc\rangle|r\rangle)\mapsto$$
$$-2^{-1/2}(2^{-1/2}(|H_2\rangle+|V_2\rangle)|qc\rangle|0\rangle+(2^{-1/2}(|H_2\rangle-|V_2\rangle)|qc\rangle|r\rangle)=$$
$$-2^{-1/2}(|H_2\rangle|qc\rangle 2^{-1/2}(|0\rangle+|r\rangle)+|V_2\rangle|qc\rangle 2^{-1/2}(|0\rangle-|r\rangle)),$$

donde $|H_2\rangle$ ($|V_2\rangle$) es un estado de un fotón que va de DH_2 a D_1 (D_2).

Supongamos que X no sea primo. Tanto si el qomputador realiza el cálculo como si no, $r=0$ y el fotón final será de tipo H_2, disparando por tanto el detector D_1 como era de esperar (pues al no ser primo el número, no hay forma de saber por el resultado r por qué camino ha ido el fotón, y su autointerferencia se mantendrá como si el qomputador no estuviera).

Si X es primo, r pasará a 1 si el qomputador se pone en marcha, y se mantendrá en 0 en caso contrario. Tenemos 4 posibilidades de igual probabilidad: (H_2, qc, 0), (H_2, qc, 1), (V_2, qc, 1), y (V_2, qc, 0). La posibilidad (H_2, qc, 0) indica que el ordenador no se ha puesto en marcha, pues de lo contrario el registro marcaría 1 (estamos suponiendo que X es primo).

Las posibilidades (H_2, qc, 1) y (V_2, qc, 1) señalan que X es primo. Puede parecer extraña la primera, pues indica primalidad aunque aparentemente no ha funcionado el computador. Pero el que el fotón al final sea H_2 no quiere decir que fuera N en el interior del interferómetro. De hecho, ese fotón tuvo que disparar el qomputador, por lo que fue un S en el interior, y como disparó el qomputador, nos reveló a través de $r=1$ qué camino siguió, desapareciendo así la autointerferencia, y pudiendo salir con igual probabilidad hacia cualquiera de los dos detectores finales.

Finalmente, la posibilidad (V_2, qc, 0) es sorprendente: parece indicar que ha funcionado el qomputador, pero con un resultado erróneo, porque X es primo, y sin embargo da $r=0$. Así que el qomputador no ha podido funcionar. Pero vimos antes que si X no fuera primo, el estado final sería siempre (H_2, qc, 0). Como vemos un (V_2, qc, 0), X debe ser primo. Inferencia "gratuita" obtenida contrafácticamente, aunque el qomputador no se haya activado. Del mero hecho de que si hubiera actuado nos daría la respuesta correcta inferimos esta respuesta sin necesidad de que actúe. ¡Así que en el 25% de los casos, podemos saber el resultado de la computación sin que el qomputador se haya puesto en marcha!

3.9.8 Clases de "qomplejidad"

Cuando se admiten máquinas de Turing cuánticas (MQTs) aparecen nuevas clases de complejidad:

1. $\mathsf{QP} := \cup_{k>0}\mathsf{QTIME}[n^k]$, con notación obvia. Esta clase consta de los problemas (de decisión) solubles en tiempo polinómico con una MQT.

2. BQP. Contiene los problemas solubles con error $\leq 1/4$ en tiempo polinómico con una MQT.

3. ZQP. Clase de problemas solubles con error nulo en tiempo (esperado) polinómico con una MQT.

Guardan las siguientes relaciones con las complejidades clásicas:

$\mathsf{P} \subsetneqq \mathsf{QP}$ (Berthiaume-Brassard 1992 [34])

$\mathsf{BPP} \subseteq \mathsf{BQP} \subseteq \mathsf{PSPACE}$ (Bernstein-Vazirani 1993 [32])

$\exists$ un oráculo A tal que $\mathsf{ZPP}^A \subsetneqq \mathsf{QP}^A$ (Berthiaume-Brassard 1994 [35])

$\exists$ un oráculo A tal que $\mathsf{ZPEXP}^A \subsetneqq \mathsf{QP}^A$ (Brassard-Hyer 1997 [47]).

La inclusión propia de P en QP es notable. Indica que los computadores cuánticos pueden resolver con eficacia más problemas que los ordenadores clásicos. Es la primera victoria clara en la separación estricta de clases de complejidad clásica y cuántica.

Vemos también que existen problemas de decisión en tiempo polinómico con un ordenador cuántico ayudado de un oráculo, que no están en ZPP ni en ZPEXP.

Sigue abierta la cuestión crucial de si BPP $\subsetneq$ BQP o no. Es decir, ¿$\exists$ problemas "tratables" cuánticamente que no lo sean clásicamente? El algoritmo de Simon (1994) es un indicio positivo, pues muestra que así es en presencia de algún oráculo: $\mathsf{BPP}^A \subsetneq \mathsf{BQP}^A$. Otro apoyo viene del algoritmo de Shor (1994), que inspirado en el resultado de Simon, prueba que FACT y DLOG están en BQP, y el estado actual del arte de la computación no nos permite afirmar que estén en BPP. La inclusión de BQP en PSPACE implica que es posible simular clásicamente, y con tan buena aproximación como se desee, problemas cuánticos con recursos de memoria que no se "desmadren", aunque eso sí, la simulación será muy, muy lenta, de tipo exponencial en tiempo. Por eso no hay problemas solubles mediante una MTQ que escapen al dominio de una MTD. Dicho de otro modo, la computación cuántica no contradice la tesis de Church-Turing. Sólo al invocar la eficiencia pueden quedarse descolgadas las MT clásicas y poner en entredicho la versión fuerte de dicha tesis.

Si bien no sabemos si BPP es subconjunto propio de BQP, sí conocemos casos particulares de algoritmos (ya que no clases de complejidad completas) que pueden acelerarse cuánticamente con respecto a su funcionamiento clásico. El de Simon muestra una ganancia exponencial ($O(2^n) \to O(n)$). El de Grover (1996) supone una mejora cuadrática, óptima ($O(N) \to O(N^{1/2})$). Pero no siempre se consigue acelerar el algoritmo de modo substancial. Existen problemas de consulta a oráculos que no admiten aceleración cuántica esencial. Lo más que se consigue es pasar de N consultas clásicas a $N/2$ consultas cuánticas. Un ejemplo lo da el problema PARIDAD (averiguar la paridad del número de bits no nulos en una ristra de $\{0,1\}^n$) [78].

3.9.9 El enredo en la qomputación

Algunos algoritmos cuánticos (Simon, Shor) presentan una mejora exponencial respecto de los algoritmos cuánticos. ¿A qué se debe ésta?

En todos los algoritmos cuánticos conocidos interviene el paralelismo masivo, consecuencia del principio de superposición lineal. Pero este no es exclusivo de la física cuántica; también se da en la física de ondas clásicas.

Por contra, el enredo es típicamente cuántico, e interviene en operaciones tan centrales en los algoritmos como la implementación de funciones $f \mapsto U_f$:

$$U_f : (U_{\mathrm{H}}^{\otimes n} \otimes 1)|0^n\rangle|0\rangle = 2^{-n/2} \sum_x |x\rangle|0\rangle \mapsto 2^{-n/2} \sum_x |x\rangle|f(x)\rangle.$$

Ningún proceso clásico es capaz de producir este efecto, en el que un estado separable pasa a estar enredado. Los estados clásicos multipartitos siempre son separables, el espacio de estados de dos sistemas clásicos es el producto cartesiano de los espacios individuales, y la información necesaria para describir un sistema de n subsistemas iguales es n veces la que se precisa para uno de éstos y por tanto crece linealmente con n. Por contra, para sistemas cuánticos hay que tomar el producto tensorial, y ahora la información necesaria para describir un sistema de n subsistemas iguales crece exponencialmente con n, pues así lo hace el número de amplitudes de una superposición arbitraria de los vectores de la base tensorial. Podemos decir que en un sistema de n qubits podemos almacenar una información que es exponencial en n. Otra cosa es su

extracción: del teorema de Holevo se desprende que a lo sumo pueden extraerse n bits informativos de un estado cualquiera de n qubits. La evolución cuántica logra procesar esa ingente información cuántica escondida en el sistema de modo supereficiente, y aunque no toda se deje leer, los algoritmos cuánticos consiguen, como hemos visto, destapar retazos de esa información que clásicamente serían inaccesibles en tiempos de cálculo equivalentes [114, 115].

Un ejemplo pertinente lo da la transformación de Fourier cuántica (QFT). El cálculo ordinario de la transformada de Fourier discreta en $\mathbb{Z}_N$ exige $O(N^2)$ operaciones. Cuando $N = 2^n$, la complejidad en tiempo de la transformada rápida de Fourier baja a $O(N \log_2 N)$. El hecho de que la QFT sobre n qubits pueda hacerse con sólo $O(n^2)$ operaciones (mejora esencial para los algoritmos cuánticos que la usan, como los de Simon, Shor, Grover, y Deutsch) es fruto del enredo.

Algunos afirman que el enredo no es tan importante como se dice, y atribuyen por contra al paralelismo masivo y a la interferencia de amplitudes la razón del éxito de la computación cuántica frente a la clásica [124, 82].

3.9.10 Límites físicos a la computación

Terminaremos comentando cómo la física no sólo potencia nuevos y mejores procesadores de información. También pone límites a la capacidad de almacenamiento y al ritmo de procesado de la información [142].

Se sabe, por aplicación del principio de indeterminación energía-tiempo, que si la energía media de un sistema por encima de su energía fundamental es E, el tiempo t que tarda un estado en hacerse ortogonal y por tanto distinguible del de partida satisface $t \gtrsim \pi\hbar/2E$. Luego $\nu \lesssim m$ (unidades geométricas), siendo m la masa del ordenador, y $\nu := 1/t$ el número de operaciones por unidad de tiempo.

Por otra parte, la memoria I (número de bits de memoria) de un sistema será a lo sumo del orden del número de grados de libertad que tiene, y por ende, de la entropía que tendría si estuviera en equilibrio termodinámico con energía media E. Es decir $I \lesssim S$.

Por tanto:

1/ La energía E limita el ritmo de operación: $\nu \lesssim E$.

2/ La entropía S limita la capacidad de memoria: $I \lesssim S$.

3/ La temperatura equivalente $T \sim E/S$ indica el número de operaciones por bit y por unidad de tiempo cuando tanto el ritmo de operación como la capacidad de memoria son máximos.

Finalmente, el tamaño limita el nivel de paralelismo con el que puede funcionar el ordenador. Cuanto más grande es el tamaño, mayor paralelismo manifiesta, pues mayor es el tiempo que tarda una señal en ir de un bit de memoria a otro alejado. Cuando el ordenador está comprimido a su radio de Schwarzschild, el tiempo en recorrer la luz éste y el tiempo I/E en invertirse un bit son del mismo orden, y el funcionamiento del ordenador en sumamente secuencial.

Un portátil actual tiene una memoria rápida $I \sim 10^{10}$ bits (pensar en 1 GB de RAM), y realiza unas 10^{10} operaciones por segundo (tomar una frecuencia de reloj de 1 GHz, y pensar que en cada ciclo pueden llegar a realizarse 3-5 operaciones enteras). Estos valores son muy inferiores a los máximos de un portátil de 1 kg de peso y volumen 1 litro. (La entropía máxima de este se obtiene cuando toda su energía está en forma de partículas relativistas, digamos fotones, y por tanto a la temperatura de 1 GK. Hay que tener en cuenta, sin embargo, que la entropía de la máquina computacional es nula, pues en cada momento es preciso conocer su estado si queremos que calcule

algorítmicamente y no a lo loco. Esos máximos, para dicho portátil de $m = 1$ kg, $V = 1$ litro, $T = 1$ GK, son $I \sim 10^{31}$ bits, y $\nu = 10^{51}$ IPS.) La razón es que en los portátiles convencionales las mayoría de grados de libertad están inmovilizados en la masa inerte. Por otro lado, los convencionales usan miles de millones de grados de libertad para representar un solo bit. Esta redundancia es aconsejable para su robustez, pero no es absolutamente necesaria. De hecho, los microordenadores cuánticos usan un solo grado de libertad para representar un bit, e invierten este en un tiempo del orden de $\pi/2E$.

Un ordenador de 1 kg (y por tanto con $\nu \lesssim 10^{31}$ IPS) y memoria máxima tiene estas características:

1/ A temperatura de 3 K, ocuparía un volumen de $(0.1\ \mathrm{UA})^3$ (para que la energía total de un baño de fotones con ese volumen y a esta temperatura equivaliera a la masa de 1 kg), y una memoria máxima de unos 10^{40} bits. Sería altamente paralelo.

2/ Si su volumen fuera de 1 litro, su temperatura habría de ser de 1 GK, por igual razón que antes, y tendría una memoria máxima de 10^{31} bits. Sería bastante paralelo.

3/ Con independencia de su constitución, si su tamaño fuera R_S, entonces la temperatura sería la de Hawking, a saber 10^{23} K, y tendría una memoria máxima de 10^{16} bits (correspondiente a la entropía de Bekenstein-Hawking). Sería altamente secuencial.

¿Podrá algún día alcanzar la potencia de los ordenadores estas cotas físicas? No se sabe. Si la ley de Moore fuese aplicable sin límite (sabemos que muy probablemente no lo es), se tardarían unos 250 años en alcanzarse los ritmos máximos de procesado de información, pasando de las 10^{10} IPS actuales al tope de 10^{51} para portátiles de 1 kg.

Las consideraciones anteriores de Lloyd, aunque en un principio cuestionadas por Ng [160], han sido luego corroboradas por éste [161]. Sostiene Ng, apoyándose en los argumentos de Wigner sobre relojes cuánticos, y en propiedades de los ANs, que si un reloj de masa m tiene precisión τ estable durante un tiempo T, necesariamente $mc^2/\hbar \gtrsim (1/\tau)(T/\tau)$, $\tau \gtrsim G_N m/c^3$, y por tanto, $T/\tau \lesssim (\tau/t_P)^2$. La memoria I de un ordenador es estimable como el número máximo T/τ de pasos en el procesado de información, y $\bar{\nu} := 1/\tau$ viene a ser el número de operaciones por bit y por unidad de tiempo; luego $I\bar{\nu} \lesssim mc^2/\hbar$, $\bar{\nu} \lesssim \hbar/(mc^2 t_P^2)$, e $I\bar{\nu}^2 \lesssim t_P^{-2}$. Como el número de operaciones por unidad de tiempo es $\nu := I\bar{\nu}$, queda $I^{-1}\nu^2 \lesssim t_P^{-2} \sim 10^{86}\ \mathrm{s}^{-2}$. Finalmente, para un portátil de 1 kg, se tiene que, en unidades geométricas, $\bar{\nu} \lesssim 1/m \sim 10^{35}\ \mathrm{s}^{-1}\mathrm{bit}^{-1}$, y, en coincidencia con Lloyd, $\nu \lesssim m \sim 10^{51}$ IPS.

Referencias

[1] Adleman, L., Pomerance, C., and Rumely, R., "On distinguishing prime numbers from composite numbers", Ann. of Math. **117**, 173-206 (1983).

[2] Adleman, L.M., "Molecular computation of solutions to combinatorial problems", Science **266**, 1021 (1994).

[3] Adleman, L.M., "Computing with DNA", Sci. Am. **279**, (2) Aug, 34-41 (1998).

[4] Aharonov, D., "Quantum computation", e-print quant-ph/9812037.

[5] Arkani-Hamed, N., Cohen, A.G., Georgi, H., "(De)Constructing dimensions", Phys. Rev. Lett. **86**, 4757-4761 (2001).

[6] Arkani-Hamed, N., Dimopoulos, S., Dvali, G., "Phenomenology, astrophysics, and cosmology of theories with submillimeter dimensions and TeV scale quantum gravity", Phys. Rev. D **59**, 086004 (1999).

[7] Arndt, M., Nairz, O., Vos-Andreae, J., Keller, C., van der Zouvw, G., Zeilinger, A., "Wave-particle duality of C_{60} molecules", Nature **401**, 680-682 (1999).

[8] Arvind, "Quantum entanglement and quantum computational algorithms", e-print quant-ph/0012116.

[9] Atkins, D., Graff, M., Lenstra, A.K., Leyland, P.C., "THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE", Proceedings Asiacrypt'94, Lecture Notes in Comput. Sci. 917, 263-277 (1995).

[10] Barenco, A., Bennett, C.H., Cleve, R., DiVincenzo, D.P., Margolus, N., Shor, P., Sleator, T., Smolin, J.A.,Weinfurter, H., "Elementary gates for quantum computation", Phys. Rev. A **52**, 3457-3467 (1995).

[11] Bell, J.S., "On the Einstein-Podolsky-Rosen paradox", Physics **1**, 195-200 (1964).

[12] Bell, J.S., "On the problem of hidden variables in quantum theory", Rev. Mod. Phys. **38**, 447-52 (1966).

[13] Bell, J.S., "Speakable and unspeakable in quantum mechanics", Cambridge Univ. Press 1987.

[14] Benioff, P.A., "The computer as a physical system: a microscopic Hamiltonian model of computers as represented by Turing machines", J. of Stat. Phys. **22**, 563-591 (1980).

[15] Benioff, P.A., "Quantum mechanical Hamiltonian models of discrete processes", J. of Math. Phys. **22**, 495 (1981).

[16] Benioff, P.A., "Quantum mechanical models of Turing machines that dissipate no energy", Phy. Rev. Lett. **48**, 1581-1585 (1982).

[17] Bennett, C.H., "Quantum cryptography using any two nonorthogonal states", Phys. Rev. Lett. **68**, 3121-3124 (1992).

[18] Bennett, C.H., "Quantum cryptography: uncertainty in the service of privacy", Science **257**, 752-753 (1992).

[19] Bennett, C.H., "Demons, engines and the second law", Sci. Am. **295**, (5) Nov, 88-96 (1987).

[20] Bennett, C.H., "Quantum information and computation", Physics Today, October 1995, pp 24-30.

[21] Bennett, C.H., Bernstein, E., Brassard, G., Vazirani, U., "Strengths and weaknesses of quantum computing", SIAM J. Comput. **26**, 1510-1523 (1997).

[22] Bennett, C.H., Bessette, F., Brassard, G., Savail, L., Smolin, J., "Experimental quantum cryptography", J. Cryptol. **5**, 3-28 (1992).

[23] Bennett, C.H., Brassard, G., “Quantum cryptography: Public key distribution and coin tossing”, International Conference on Computers, Systems & Signal Processing, Bagalore, India, pp 175-179 (1984).

[24] Bennett, C.H., Brassard, G., Ekert, A., “Quantum cryptography”, Sci. Am. **267**, (4) Oct, 26-33 (1992).

[25] Bennett, C.H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A., Wootters, W.K., “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels”, Phys. Rev. Lett. **70**, 1895-1898 (1993).

[26] Bennett, C.H., DiVincenzo, D.P., Gershenfeld, N., Gibbs, H.M., Kimble, H.J., Preskill, J., Vazirani, U.V., Wineland, D.J., Yao, C., “Quantum information science. An emerging field of interdisciplinary research and education in science and engineering”, Report of the NSF Workshop, Arlington, Virginia, Oct 1999.

[27] Bennett, C.H., DiVincenzo, D.P., Smolin, J., “Capacities of quantum erasure channels”, Phys. Rev. Lett. **78**, 3217-3220 (1997).

[28] Bennett, C.H., DiVincenzo, D.P., Smolin, J., Wootters, W.K., “Mixed state entanglement and quantum error correction”, Phys. Rev. A **54**, 3824-3851 (1996).

[29] Bennett, C.H., Shor, P.W., “Quantum information theory”, IEEE Trans. Inform. Theory **44**, 2724-2742 (1998).

[30] Bennett, C.H., Shor, P.W., Smolin, J.A., Thapliyal, A.V., “Entangled assisted classical capacity of noisy quantum channels”, e-print quant-ph/9904025 v5.

[31] Bennett, C.H., Wiesner, S.J., “Communication via one- and two-particle operations on Einstein-Podolsky-Rosen states”, Phys. Rev. Lett. **69**, 2881-2884 (1992).

[32] Bernstein, E., Vazirani, U., “Quantum complexity theory”, Proceedings of the 25th Annual ACM Symposium on the Theory of Computing, 11-20 (1993).

[33] Bernstein, E., Vazirani, U., “Quantum computability”, SIAM J. Comput. **26**, 1411-1473 (1997).

[34] Berthiaume, A., Brassard, G., “The quantum challenge to structural complexity theory”, Proc. 7th IEEE Conference on Structure in Complexity Theory, Boston, MA, 132-137 (1992).

[35] Berthiaume, A., Brassard, G., “Oracle quantum computing”, J. Modern Opt. **41**, 2521-2535 (1994).

[36] Blake, I., Heegard, C., Høholdt, T., Wei, V., “Algebraic-geometric codes”, IEEE Transactions on Information Theory **44**, 2596-2618 (1998).

[37] Bohm, D., “Quantum theory”, Prentice-Hall, 1951.

[38] Boschi, D., Branca, S., De Martini, F., Hardy, L., Popescu, S., “Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels”, Phys. Rev. Lett. **80**, 1121-1125 (1998).

[39] Bouwmeester, D., Ekert, A., Zeilinger, A., (eds.) “The physics of quantum information”, Springer-Verlag 2000.

[40] Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A., "Experimental quantum teleportation", Nature **390**, 575-579 (1997).

[41] Bouwmeester, D., Pan, J.-W., Daniell, M., Weinfurter, H., Zukowski, M., Zeilinger, A., "Reply to comment "*A posteriori* teleportation"", Nature **394**, 841 (1998).

[42] Bouwmeester, D., Pan, J.-W., Weinfurter, H., Zeilinger, A., "High fidelity teleportation of independent qubits", e-print quant-ph/9910043.

[43] Boyer, M, G. Brassard, P. Hoyer, A. Tapp, 1998, "Tight bounds on quantum searching", Fortsch.Phys. **46**, 493-506; e-print quant-ph/9605034.

[44] Boykin, P.O., Mor, T., Pulver, M., Roychowdhury, V., Vatan, F., "On universal and fault-tolerant quantum computing", e-print quant-ph/9906054.

[45] Brassard, G., "The dawn of a new era for quantum cryptography: The experimental prototype is working!", SIGACT News **20**(4), 78-82 (1989).

[46] Brassard, G., Crépeau, C., Mayers, D., Salvail, L., "A brief review on the impossibility of quantum bit commitment", e-print quant-ph/9712023.

[47] Brassard, G., P. Hyer, "An exact quantum polynomial-time algorithm for Simon's problem", e-print quant-ph/9704027.

[48] Brassard, G., P. Hyer, A. Tapp, "Quantum counting", Proc. 25th ICALP vol. 1443, Lectures Notes in Computer Science **80**, Springer-Verlag 1998; e-print quant-ph/9805082.

[49] Braunstein, S.L., Fuchs, C.A., Kimble, H.J., "Criteria for continuous-variable quantum teleportation", e-print quant-ph/9910030.

[50] Braunstein, S.L., Kimble, H.J., "*A posteriori* teleportation", Nature **394**, 840-841 (1998).

[51] Calderbank, A.R., Shor, P.W., "Good quantum error-correcting codes exist", Phys. Rev. A **54**, 1098-1105 (1996).

[52] Calderbank, A.R., Sloane, N.J.A., "Claude Shannon (1916-2001)", Nature **410**, 768 (2001).

[53] Cerf, N.J., Gisin, N., Massar, S., "Classical teleportation of a quantum bit", e-print quant-ph/9906105.

[54] Chuang, I.L., "Quantum algorithm for distributed clock synchronization", Phys. Rev. Lett. **85**, 2006-2009 (2000); e-print quant-ph/0005092.

[55] Church, A., "A note on the Entscheidungsproblem", J. Symb. Log. **1**, 40-41 (1936).

[56] Cirac, J.I., Zoller, P., "Quantum computations with cold trapped ions", Phys. Rev. Lett. **74**, 4091-4094 (1995).

[57] Cleve, R., "An introduction to quantum complexity theory", e-print quant-ph/9906111.

[58] Cleve, R., A. Ekert, C. Macchiavello, M. Mosca, 1998, "Quantum algorithms revisited", Proc. R. Soc. London, Ser. A **454**, 339.

[59] Cohen, H., Lenstra, H.W., "Primality testing and Jacobi sums", Math. Comp. **42**, 297-330 (1984).

[60] Cohen, H., "A course in computational algebraic number theory", Graduate texts in mathematics, Vol 138, Springer-Verlag 1993.

[61] Collins, G.P., "Quantum cryptography defies eavesdropping", Physics Today, November 1992, pp 21-23.

[62] Conway, J.H., Sloane, N.J.A., "Sphere packings, lattices and groups", third edition, Grundlehren der mathematischen Wissenschaften, Vol 290, Springer-Verlag 1999.

[63] Davis, M., "The universal computer", W.W. Norton & Company 2000.

[64] Deutsch, D., "Quantum theory, the Church-Turing principle and the universal quantum computer", Proc. Roy. Soc. Lond. A **400**, 97-117 (1985).

[65] Deutsch, D., "Quantum computational networks", Proc. Roy. Soc. Lond. A **425**, 73-90 (1989).

[66] Deutsch, D., Jozsa, R., "Rapid solution of problems by quantum computation", Proc. Roy. Soc. Lond. A **439**, 553-558 (1992).

[67] Dieks, D., "Communication by EPR devices", Phys. Lett. A **92**, 271-272 (1982).

[68] Diffie, W., Hellman, M.E., "New directions in cryptography", IEEE Transactions on Information Theory **22**, 644-654 (1976).

[69] Diffie, W., "The first ten years in public-key cryptography", in "Contemporary cryptology: The science of information integrity," pp 135-175, IEEE Press 1992.

[70] DiVincenzo, D.P., "Two-bit gates are universal for quantum computation", Phys. Rev. A **51** 1015-1022 (1995).

[71] Durr, Ch., P. Hoyer, "A quantum algorithm for finding the minimum", e-print quant-ph/9607014.

[72] EFF Electronic Frontier Foundation, "Cracking DES. Secrets of encryption research, wiretap politics & chip design. How federal agencies subvert privacy", foreword by W. Diffie, O'Reilly and Associates 1998.

[73] Eintein, A., Podolsky, B., Rosen, N., "Can quantum-mechanical description of physical reality be considered complete?", Phys. Rev. **47**, 777-780 (1935).

[74] Ekert, A., "Quantum cryptography based on Bell's theorem", Phys. Rev. Lett. **67**, 661-663 (1991).

[75] Ekert, A., Jozsa, R., "Quantum computation and Shor's factoring algorithm", Rev. Mod. Phys. **68**, 733 (1996).

[76] Ekert, A., Macchiavello, C., "Quantum error correction for communication", e-print quant-ph/9602022.

[77] Fang, X., Zhu, X., Feng, M., Mao, X., Du, F., "Experimental implementaton of dense coding using nuclear magnetic resonance", e-print quant-ph/9906041.

[78] Farhi, E., Goldstone, J., Gutmann, S., Sipser, M., "A limit on the speed of quantum computation in determining parity", e-print quant-ph/9802045.

[79] Feynman, R.P., "Simulating physics with computers", Int. J. Theor. Phys. **21**, 467-488 (1982).

[80] Feynman, R.P., 1985, "Quantum mechanical computers", Opt. News **11**, 11-20 (1985).

[81] Feynman, R.P., "Feynman lectures on computation", eds. Hey, A., Allen, R., Addison-Wesley 1996.

[82] Fortnow, L., "One complexity theorist's view of quantum computing", e-print quant-ph/0003035.

[83] Freedman, M.H., "P/NP, and the quantum field computer", Proc. Natl. Acad. Sci. USA **95**, 98-101 (1998).

[84] Furuzawa, A., Sørensen, J.L., Braunstein, S.L., Fuchs, C.A., Kimble, H.J., Polzik, E.S., "Unconditional quantum teleportation", Science **282**, 706 (1998).

[85] Galindo, A., "Cien años de quanta", Revista Española de Física **14** (Número especial: Cien años de quanta), 1-3 (2000).

[86] Galindo, A., "Quanta e información", Revista Española de Física **14** (Número especial: Cien años de quanta), 30-48 (2000).

[87] Galindo, A., Martín-Delgado, M.A., "A family of Grover's quantum searching algorithms", e-preprint quant-ph/0009086, Phys. Rev. A **62**, 62303 (2000).

[88] Galindo, A., Martín-Delgado, M.A., "Information and computation: classical and quantum aspects", preprint 2001, aceptado para su publicación en Rev. Mod. Phys.

[89] Galindo, A., Moreno, A., Benedí, A., Varela, P., Capítulo sobre "Física cuántica" en el libro "Física 2", McGraw-Hill 1998.

[90] Galindo, A., Pascual, P., "Problemas de mecánica cuántica", Eudema 1989.

[91] Galindo, A., Pascual, P., "Quantum mechanics I, II", Springer-Verlag 1990-91.

[92] García Alcaine, G., "Enredo cuántico", Revista Española de Física **14** (Número especial: Cien años de quanta), 17-29 (2000).

[93] García Alcaine, G., Álvarez Galindo, G., "Adversus collapsum", Revista Española de Física **15**, no. 2, 29-34 (2000).

[94] Gardner, M., "Mathematical games", Sci. Am. **237**, (2) Aug, 120-124 (1977).

[95] Garey, M R., Johnson, D. S., "Computers and intractability. A guide to the theory of NP-completeness," Freeman and Co. 1979.

[96] Gerber, J., "Factoring large numbers with a quadratic sieve", Math. Comp. **41**, 287-294 (1983).

[97] Gödel, K., "Über formal unentscheidbare Sätze der *Principia mathematica* und verwandter Systeme I", Monatshefte für Mathematik und Physik **38**, 173-198 (1931).

[98] Grisenti, R.E., Schöllkopf, W., Toennies, J.P., Hegerfeldt, G.C., Köhler, T., Stoll, M., "Determination of the bond length and binding energy of the Helium dimer by diffraction from a transmission grating", Phys. Rev. Lett. **85**, 2284-2287 (2000).

[99] Grover, L.K., 1996, "A fast quantum mechanical algorithm for database search", Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, pp 212-219.

[100] Grover, L.K., 1997, "Quantum mechanics helps in searching for a needle in a haystack", Phys. Rev. Lett. **79**, 325-328.

[101] Gruska, J., "Quantum computing", McGraw-Hill 1999.

[102] Haroche, S., Raimond, J.-M., "L'ordinateur quantique: rêve ou cachemar?", La Recherche **292**, 58-60 (1996).

[103] Hellman, M.E., "The mathematics of public key cryptography", Sci. Am. **241**, (2) Aug, 130-139 (1979).

[104] Holevo, A.S., "Some estimates of the information transmitted by a quantum communication channel", Probl. Peredachi Inform. **9**, 3-11 (1973), in Russian; translated in Probl. Inform. Transm. **9**, 177-183 (1973).

[105] Hoyle, C.D., Schmidt, U., Heckel, B.R., Adelberger, E.G., Gundlach, J.H., Kapner, D.J., Swanson, H.E., "Submillimeter test of the gravitational inverse-square law: a search for "large" extra dimensions", Phys. Rev. Lett. **86**, 1418-1421 (2001).

[106] Hughes, R.J., Alde, D.M., Dyer, P., Luther, G.G., Morgan, G.L., Schauer, M., "Quantum cryptography", Contemp. Phys. **36**, 149-163 (1995).

[107] Hughes, R.J., "Cryptography, quantum computation and trapped ions", preprint LA-UR-97-4986.

[108] Hughes, R.J., Buttler, W.T., Kwiat, P.G., Lamoreaux, S.K., Morgan, G.L., Nordholt, J.E., Peterson C.G., "Practical quantum cryptography for secure free-space communications", e-print quant-ph/9905009.

[109] Hughes, R.J., Luther, G., Morgan, G., Peterson, G., Simmons, C., "Quantum cryptography over underground optical fibers", in Lecture Notes in Computer Science, vol 1109, pp 329-342 (1996).

[110] Hughes, R.J., Morgan, G.L., Peterson, C.G., "Practical quantum key distribution over a 48-km optical fiber network", Los Alamos report LA-UR-99-1593; e-print quant-ph/9904038.

[111] Hughes, R.J., Nordholt, J.E., "Quantum cryptography takes to the air", Physics World **12**, 31-35 (1999).

[112] Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., Zeilinger, A., "Quantum cryptography with entangled photons", e-print quant-ph/9912117.

[113] Jozsa, R., "Fidelity for mixed quantum states", J. Modern Opt. **41**, 2315-2323 (1994).

[114] Jozsa, R., "Entanglement and quantum computation", e-print quant-ph/9707034.

[115] Jozsa, R., "Quantum effects in algorithms", Chaos, Solitons and Fractals **10**, 1657-1664 (1999); e-print quant-ph/9805086.

[116] Jozsa, R., Abrams, D.S., Dowling, J.P., Williams, C.P., "Quantum clock synchronization based on shared prior entanglement", Phys. Rev. Lett. **85**, 2010-2013 (2000); e-print quant-ph/0004105.

[117] Jozsa, R., Schumacher, B., "A new proof of the quantum noiseless coding theorem", J. Modern Opt. **41**, 2343-2349 (1994).

[118] Kahn, D., "The codebreakers, the story of secret writing", Macmillan 1967.

[119] Kane, B.E., "A silicon-based nuclear spin quantum computer", Nature **393**, 133 (1998).

[120] Kane, B.E., "Silicon-based quantum computation", e-print quant-ph/0003031.

[121] Kim, E.E., Toole, B.A., "Ada and the first computer", Sci. Am. **280**, (5) May, 66-71 (1999).

[122] Kitaev, A. Y., "Quantum measurements and the Abelian stabilizer problem", e-print quant-ph/9511026.

[123] Kitaev, A. Y., "Quantum computations: algorithms and error correction", Russian Math. Surveys **52**, 1191-1249 (1997).

[124] Knight, P., "Quantum information processing without entanglement", Science **287**, 441-442 (2000).

[125] Knill, E., "Approximation by quantum circuits", e-print quant-ph/9508006.

[126] Knill, E., Laflamme, R., Martínez, R., Negrevergne, C., "Benchmarking quantum computers: the five-qubit error correcting code", Phys. Rev. Lett. **86**, 5811-5814 (2001).

[127] Knuth, D.E., "Selected papers on computer science", CSLI Lecture Notes **49**, CSLI Publications and Cambridge Univ. Press 1996.

[128] Knuth, D.E., "The art of computer programming. Vol. 2: Seminumerical algorithms", Addison-Wesley 1981.

[129] Koblitz, N., "A course in number theory and cryptography". second edition, Springer-Verlag 1994.

[130] Landauer, R., "Irreversibility and heat generation in the computing process", IBM J. Res. Dev. **5**, 183 (1961).

[131] Landauer, R., "Information is physical", Physics Today, May 1991, pp 23-29.

[132] Landauer, R., "The physical nature of information", Phys. Lett. A **217**, 188-193 (1996).

[133] Landauer, R., "Is quantum mechanically coherent computation useful?", Proceedings Drexel-4 Symposium on Quantum Nonintegrability-Quantum-Classical Correspondence, Philadelphia, PA, 8 September 1994, ed. D. H. Feng and B.-L. Hu (Boston, International Press, 1997).

[134] Lenstra, H.W., "Factoring integers with elliptic curves", Annals of Math. (2) **126**, 649-673 (1987).

[135] Lenstra, A., Lenstra, H.W., eds, "The development of the number field sieve", Lecture Notes in Math. 1554, Springer-Verlag, 1993.

[136] Levitin, L.B., "On quantum measure of information", Proceedings 4th All-Union Conf. Information and Coding Theory, pp 111-115, Tashkent 1969, in Russian.

[137] Li, M., Vitányi, P., "An introduction to Kolmogorov complexity and its applications", Second edition, Springer-Verlag 1997.

[138] Lipton, R.J., "DNA solution of hard computational problems", Science **268**, 542-545 (1995).

[139] Lloyd, S., "Almost any quantum logic gate is universal", Phys. Rev. Lett. **75**, 346-349 (1995).

[140] Lloyd, S., "Universal quantum simulators", Science **273**, 1073-1078 (1996).

[141] Lloyd, S., "Quantum search without entanglement", e-print quant-ph/9903057.

[142] Lloyd, S., "Ultimate physical limits to computation", Nature **406**, 1047-1054 (2000).

[143] Lo, H-K, Chau, H.F., "Unconditional security of quantum key distribution over arbitrarily long distances", Science **283**, 2050-2056 (1999).

[144] van der Lubbe, J.C.A., "Basic methods of cryptography", Cambridge Univ. Press 1998.

[145] Macwilliams, F.J., Sloane, N.J.A., "The theory of error-correcting codes", North Holland 1977.

[146] Manin, Y.I., "Computable e incomputable", en ruso. Sovetskoye Radio, Moscú, 1980.

[147] Manin, Y.I., "Classical computing, quantum computing and Shor's factoring algorithm', e-print quant-ph/9903008.

[148] Marand, Ch., Townsend, P.D., "Quantum key distribution over distances as long as 30 km", Opt. Lett. **20**, 1695-1697 (1995).

[149] Mattle, K., Weinfurter, H., Kwiat, P.G., Zeilinger, A., "Dense coding in experimental quantum communication", Phys. Rev. Lett. **76**, 4656-4659 (1996).

[150] Mayers, D., "Unconditionally secure quantum bit commitment is impossible", Fourth workshop on physics and computation – PhysCom '96, Boston, November 1996.

[151] Mayers, D., "Unconditionally secure quantum bit commitment is impossible", Phys. Rev. Lett. **78**, 3414-3417 (1997).

[152] Mayers, D., "Unconditional security in quantum cryptography", e-print quant-ph/9802025.

[153] Mertens, S., "Computational complexity for physicists", e-print cond-mat/0012185.

[154] Meyer, D.A., "Quantum games and quantum algorithms", e-print quant-ph/0004092.

[155] Miller, G.L., "Riemann's hypothesis and tests for primality", Journal of Computer and Systems Science **13**, 300-317 (1976).

[156] Mitchison, G., Jozsa, R., "Counterfactual computation", e-print quant-ph/9907007.

[157] Muller, A., Breguet, J., Gisin, N., "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km", Europhys. Lett. **23**, 383-388 (1993).

[158] Muller, A., Zbinden, H., Gisin, N., "Quantum cryptography over 23 km of installed under-lake Telecom fiber", Europhys. Lett. **33**, 335-339 (1996).

[159] Naughton, J., "Slaves to logic", Nature **410**, 870-871 (2001).

[160] Ng, Y.J., "From computation to black holes and space-time foam", Phys. Rev. Lett. **86**, 2946-2949 (2001).

[161] Ng, Y.J., "From computation to black holes and space-time foam", e-print gr-qc/0006105 v5 (30 Mar 2001).

[162] Nielsen, M.A., "On the units of bipartite entanglement: Is sixteen ounces of entanglement always equal to one pound?", e-print quant-ph/0011063.

[163] Nielsen, M.A., "Introduction to quantum information theory", e-print quant-ph/0011064.

[164] Nielsen, M.A., Chuang, I.L., "Quantum computation and quantum information", Cambridge Univ. Press 2000.

[165] Ogburn, R.W., Preskill, J., "Topological quantum computation', en "Quantum computing and quantum communications", Lecture Notes in Computer Sciences 1509, Ed. C.P. Williams, Springer-Verlag 1999, pp 341-356.

[166] Pan, J-W., Bouwmeester, D., Weinfurter, H., Zeilinger, A., "Experimental entanglement swapping: entangling photons that never interacted", Phys. Rev. Lett. **89**, 3891 (1998).

[167] Papadimitriou, Ch.H., "Computational complexity", Addison-Wesley 1994.

[168] Pati, A.K., "Minimum cbits required to transmit a qubit", e-print quant-ph/9907022.

[169] Petri, C.A., "Grundsätzliches zur Berschreibung diskreter Prozesse", Proceedings 3. Colloquium über Automatentheorie (Hannover, 1965), pp 121-140, 1967.

[170] Pomerance, C., "Analysis and comparison of some integer factoring algorithms", in "Computational Methods in Number Theory", Eds. H.W. Lenstra, Jr. and R. Tidjeman, Mathematisch Centrum, Amsterdam 1982, pp 89-139.

[171] Pomerance, C., "A tale of two sieves", Notices of the AMS **43**, 1473-1485 (1996).

[172] Preskill, J., "Quantum information and quantum computation", Talk, 15 January 1997, www.theory.caltech.edu/∼preskill.

[173] Preskill, J., "Lecture notes", www.theory.caltech.edu/∼preskill/ ph229 (1998).

[174] Preskill, J., "Quantum information: its future impact on physics", Talk, 18 December 1998, www.theory.caltech.edu/∼preskill.

[175] Preskill, J., "Reliable quantum computers", Proc. R. Soc. Lond. A **454**, 386 (1998).

[176] Preskill, J., "Quantum information and physics: some future directions", 8 April 1999, www.theory.caltech.edu/∼preskill.

[177] Rabin, M.O., "Probabilistic algorithms for testing primality", J. Number Theory **12**, 128-138 (1980).

[178] Reck, M., Zeilinger, A., Berstein, H.J., Bertani, P., "Experimental realization of any discrete unitary operator", Phys. Rev. Lett. **73**, 58-61 (1994).

[179] Rieffel, E., Polack, W., "An introduction to quantum computing for non-physicists", e-print quant-ph/9809016.

[180] Rivest, R.L., Shamir, A., Adleman, L., "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM **21**, 120-126 (1978).

[181] Roman, S., "Coding and information theory", Springer-Verlag 1992.

[182] Rowe, M.A., Kleipinski, D., Meyer, V., Sackett, C.A., Itano, W.M., Monroe, C., Wineland, D.J., "Experimental violation of a Bell's inequality with efficient detection", Nature **409**, 791-794 (2001).

[183] Saitoh, E., Okamoto, S., Takahashi, K.T., Tobe, K., Yamamoto, K., Kimura, T., Ishihara, S., Maekawa, S., Tokura, Y., "Observation of orbital waves as elementary excitations in a solid", Nature **410**, 180-183 (2001).

[184] Sakamoto, K., Gouzu, H., Komiya, K., Kiga, D., Yokoyama, S., Yokomori, T., Hagiya, M., "Molecular computation by DNA hairpin formation", Science **288**, 1223-1226 (2000).

[185] Salomaa, A., "Computation and automata", Encyclopedia of mathematics and its applications, Vol. 25, Ed. G.-C. Rota, Cambridge Univ. Press 1985.

[186] Salomaa, A., "Public-key cryptography", second, enlarged edition, Springer-Verlag 1996.

[187] Schumacher, B., "Quantum coding", Phys. Rev. A **51**, 2738-2747 (1995).

[188] Shannon, C.E., "A mathematical theory of communication", Bell Systems Technical Journal **27**, 379-423, 623-656 (1948).

[189] Shannon, C.E., "Communication theory of secrecy systems", Bell Systems Technical Journal **28**, 656-715 (1949).

[190] Shimony, A., "Conceptual foundations of quantum mechanics", in "The new physics", Ed. P. Davies, Cambridge Univ. Press 1989, pp 373-395.

[191] Shor, P.W., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, p. 124 (IEEE Computer Society Press, Los Alamitos, CA, 1994); e-print quant-ph/9508027.

[192] Shor, P.W., "Scheme for reducing decoherence in quantum computer memory", Phys. Rev. A **52**, 2493-2496 (1995).

[193] Shor, P.W., Sloane, J.A., "A family of optimal packings in Grassmannian manifolds", J. of Algebraic Combinatorics **7**, 157-163 (1998).

[194] Shor, P.W., "Introduction to quantum algorithms", e-print quant-ph/0005003.

[195] Simon, D.R., "On the power of quantum computation", Proceedings of the 35th Annual IEEE Symp. on the Found. of Comp. Sci. (IEEE Computer Society, Los Alamitos), 1994. Extended Abstract on pages 116-123. Full Version of the paper in S.I.A.M. Jour. on Computing, **26**, Oct 97.

[196] Sleator, T., Weinfurter, H., "Realizable universal quantum logic gates", Phys. Rev. Lett. **74**, 4087-4090 (1995).

[197] Steane, A.M., "Error correcting codes in quantum theory", Phys. Rev. Lett. **77**, 793 (1996).

[198] Steane, A.M., "Multiple particle interference and quantum error correction", Proc. Roy. Soc. Lond. A **452**, 2551 (1996).

[199] Steane, A.M., "Quantum computing", e-print quant-ph/9708022.

[200] Stichtenoth, H., "Algebraic function fields and codes", Springer-Verlag 1993.

[201] Stinson, D.R., "Cryptography: Theory and practice", CRC Press, Boca Raton, Florida 1995.

[202] Tegmark, M., "The quantum brain", e-print quant-ph/9907009.

[203] Thirring, W., "A course in mathematical physics, 4: Quantum mechanics of large systems", Springer-Verlag 1983.

[204] 't Hooft, G., "Determination and dissipation in quantum gravity", e-print hep-th/0003005.

[205] Turing, A., "On computable numbers, with an application to the Entscheidungsproblem", Proc. Lond. Math. Soc. (2) **42** 230-265 (1936); correction ibid. **43**, pp 544-546 (1937).

[206] Uhlmann, A., "The "transition probability" in the state space of a *-algebra", Rep. Math. Phys. **9**, 273-279 (1976).

[207] Unruh, W.G., "Maintaining coherence in quantum computers", Phys. Rev. A **51**, 992-997 (1995).

[208] Vaidman, L., "Teleportation: dream or reality?", Proceedings of the Conference: Misteries, puzzles and paradoxes in quantum mechanics, Gargano, Italy, 1998; e-print quant-ph/9810089.

[209] Vedral, V., Plenio, M.B., "Basics of quantum computation", e-print quant-ph/9802065.

[210] Vernam, G.S., "Cipher printing telegraph systems for secret wire and radio telegraphic communications", J. Am. Inst. Elect. Engrs., XLV, 109-115 (1926).

[211] Welsh, D., "Codes and cryptography", Oxford Univ. Press 1995.

[212] Wiesner, S., "Conjugate coding", SIGACT News **15:1**, 78-88 (1983). (Manuscript *circa* 1970.)

[213] Williams, C.P., Clearwater, S.H., "Explorations in quantum computing", TELOS, Springer-Verlag 1998.

[214] Williams, C.P., Clearwater, S.H., "Ultimate zero and one", Copernicus, Springer-Verlag 2000.

[215] Wootters, W.K., Zurek, W.H., "A single quantum cannot be cloned", Nature **299**, 802-803 (1982).

[216] Yan, S.Y., "Number theory for computing", Springer-Verlag 2000.

[217] Yao, A., "Quantum circuit complexity", Proceedings of the 34th IEEE Symposium on Foundations of Computer Science, 352-361 (1993).

[218] Ynduráin, F.J., "Quantum chromodynamics", Springer-Verlag 1983.

[219] Ynduráin, F.J., "Mecánica cuántica y física de partículas elementales", Revista Española de Física **14** (Número especial: Cien años de quanta), 54-64 (2000).

[220] Zalka, Ch., "Grover's quantum searching algorithm is optimal", Phys. Rev. A **60**, 2746-2751 (1999).