

Computación Cuántica: un reto tecnológico

Quantum Computing: a technological challenge

MANUEL CALIXTO

*Departamento de Matemática Aplicada y Estadística, Campus Universitario Alfonso XIII,
Paseo Alfonso XIII, 52, 30203 Cartagena.*

*Instituto Carlos I de Física Teórica y Computacional, Facultad de Ciencias, Universidad de
Granada, Campus de Fuentenueva, 18002 Granada.*

E-mail: calixto@ugr.es

Resumen: La nueva Teoría de la Información Cuántica augura poderosas máquinas que obedecen a la “enredada” lógica del mundo submicroscópico. Paralelismo, enredo, teleportación, no-clonación y criptografía cuántica son peculiaridades típicas de este nuevo modo de entender la computación.

Abstract: The new Quantum Information Theory augurs powerful machines that obey the “entangled” logic of the subatomic world. Parallelism, entanglement, teleportation, no-cloning and quantum cryptography are typical peculiarities of this novel way of understanding computation.

1 Introducción

La mera unión de las palabras “Computación” y “Cuántica” sugiere algo extraño, revolucionario y potente; quizás porque se combinan dos de los principales logros científicos del siglo ya pasado: la *Teoría de la Información* (TI) y la *Mecánica Cuántica* (MC). Su carácter interdisciplinario es uno de los aspectos más estimulantes y llamativos.

La invención del ordenador ha hecho posible el procesamiento complejo de la información fuera del cerebro humano. Es más, la robótica, traductores de lenguajes, programas de ajedrez (Garry Kasparov tiene algo que contar al respecto...) y programas de reconocimiento de voz (por mencionar algunos) nos hacen ver que los ordenadores son capaces de *simular* ciertos aspectos antes considerados (casi) exclusivamente “humanos”. Pero todavía podemos ir más lejos. Quién nos dice que, algún día, tras conocer cómo se traducen los estímulos visuales, auditivos, etc en impulsos eléctricos, no podamos simular también la “realidad” por medio de un ordenador suficientemente potente conectado a nuestro cerebro?. Por lo pronto, la “realidad virtual” nos proporciona un sucedáneo.

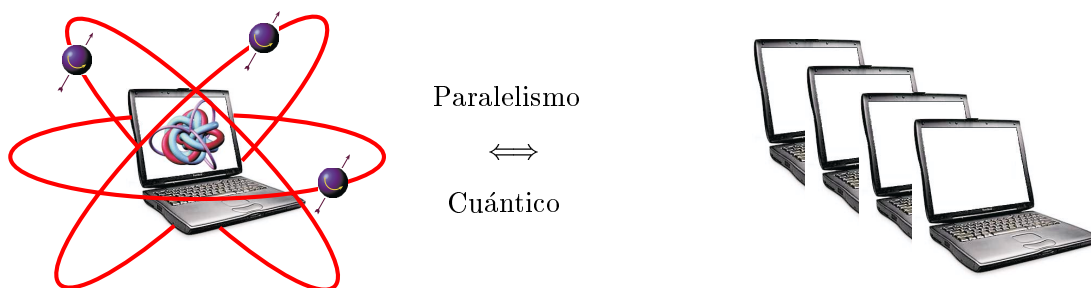
Todos estos logros en las ciencias de la computación e inteligencia artificial se deben al ritmo vertiginoso en el progreso tecnológico en las últimas décadas. Esencialmente, la potencia de los ordenadores se viene doblando cada dos años desde 1970, de acuerdo con la Ley de Moores, cofundador de Intel, el cual predijo esta tendencia durante un discurso visionario en 1965 [1]. Extrapolando a un futuro cercano, este continuo crecimiento exponencial en la miniaturización del componente más elemental (el transistor) alcanzará su límite (nanotecnología) para el año 2017, cuando un “bit” de información (digamos, la respuesta “sí” o “no” a una pregunta) pueda codificarse en un solo átomo (!). Para entonces, deberemos empezar a preocuparnos de los nuevos y sorprendentes efectos mecano-cuánticos que surgen a escalas submicroscópicas. Estos efectos pueden presentarse como perniciosos (por ejemplo, la aparición de efecto túnel) si no se rediseñan los transistores. Aunque quizás, mejor que luchar contra los efectos cuánticos, sería conveniente aliarse con ellos y pensar en otras alternativas a la tecnología del transistor, es decir, una nueva arquitectura más apropiada a la escala nanométrica: “un ordenador cuántico...”

Resulta que las leyes de la MC implican una forma de procesar la información diferente a la tradicional basada en leyes de la física clásica. El tratamiento de la información contenida en la función de onda de un sistema físico cuántico es el cometido de la nueva *Teoría Cuántica de la*

Información [2]: un matrimonio perfecto entre la TI y la MC, comparable a la simbiosis entre Física y Geometría que da lugar a la Relatividad General.

A efectos prácticos, la manipulación cuántica de la información ofrece aplicaciones *reales*, especialmente en la transmisión segura de información (*Criptografía Cuántica*), y *potenciales*, como el diseño de algoritmos varios órdenes de magnitud más rápidos que cualquier algoritmo clásico imaginable; por ejemplo: algoritmos de factorización que podrían amenazar la privacidad de muchas operaciones financieras, o algoritmos de búsqueda extremadamente eficientes, tanto que (pongamos por caso) marcarían barreras insalvables entre ajedrecistas “cibernéticos” y nuestros mejores maestros (véase más adelante).

Las ventajas de la computación cuántica sobre la clásica recaen sobre dos propiedades mecano-cuánticas por excelencia: la *superposición* (interferencia o paralelismo) y el *enredo* cuánticos. La superposición cuántica proporciona la posibilidad de efectuar múltiples operaciones matemáticas simultáneas (equivalente a múltiples ordenadores clásicos trabajando en paralelo); mientras que el enredo cuántico (el cual definiremos más tarde) proporciona una correlación entre las respuestas mayor que cualquier correlación clásica imaginable.



Desafortunadamente, lo que se gana en potencia se pierde en estabilidad. Un ordenador cuántico resulta ser extremadamente vulnerable, frágil, sensible a toda clase de ruido ambiente; tanto más cuanto mayor es. Por ejemplo, mantener la coherencia entre dos o tres átomos (el ordenador cuántico más grande hasta el momento...) resulta ya extremadamente difícil con la tecnología actual. Otra desventaja es que no se puede amplificar una señal cuántica, debido al teorema de *no-clonación* (no existen “fotocopiadoras cuánticas” perfectas), limitando así el alcance de la comunicación cuántica (hasta ahora de unas decenas de kilómetros, usando fibra óptica); aunque sí es posible la *teleportación* (véase más adelante). No obstante, la imposibilidad

de copiar (clonar) estados cuánticos tiene otra vertiente positiva: la detección de “fisgones” y el establecimiento de comunicaciones seguras.

No pensemos pues en esperar a la nueva generación de computadores cuánticos para comprar un ordenador, por la misma razón que no llevamos nuestro coche a reparar al “taller mecánico-cuántico”... No obstante, a pesar de lo extremadamente sensible al ruido de un ordenador cuántico, una cierta tolerancia al fallo y algoritmos de corrección de errores, junto con un esfuerzo en mejora tecnológica, podrían hacer factible la computación cuántica algún día.

Por lo pronto, merece la pena analizar lo que significa la información cuántica y el procesamiento abstracto de la misma, olvidándonos del posible soporte físico o “hardware” (trampa de iones, resonancia magnética nuclear, láser, o lo que sea) que pueda realizar de forma eficiente nuestro hipotético ordenador en un futuro.

2 Clásico versus Cuántico: “bit” versus “qubit”

El procesamiento de la información fuera del cerebro humano pasa por convertir un mensaje (información) en una secuencia de símbolos, llámese alfabeto o, más básico aún, el lenguaje Morse o sistema de numeración binario: es decir, una secuencia finita de puntos y rayas o dígitos binarios (“bits”) 0 y 1 (“sí” y “no” en la lógica Booleana ordinaria). Un dispositivo con dos posiciones estables puede almacenar un bit de información. N dispositivos almacenan pues N bits, con un número total de estados 2^N . Por ejemplo, la representación de todas las letras del abecedario requiere, como mínimo, $N = 5$ bits. Asignando a cada letra un número l del 0 al 26

$$\begin{array}{cccccc} \text{A} & \text{B} & \text{C} & \dots & \text{X} & \text{Y} & \text{Z} \\ 00 & 01 & 02 & \dots & 24 & 25 & 26 \end{array}, \quad (1)$$

la correspondiente representación en binario viene dada por $(b_{N-1}b_{N-2}\dots b_0)$, donde $b_j = 0, 1$ y

$$l = b_{N-1}2^{N-1} + b_{N-2}2^{N-2} + \dots + b_02^0. \quad (2)$$

El procesamiento y manipulación de la información se reduce pues, en términos generales, a “cambiar ceros por unos” y viceversa. Un dispositivo que almacena un bit de información puede ser un cable por el que pasa (1) o no pasa (0) corriente, y una acción no trivial (*puerta lógica*) sobre el estado del cable la efectúa el componente electrónico por excelencia: el *transistor*. La acción básica del transistor sobre un cable es *negar* (NOT) la entrada, o sea: si entra corriente no

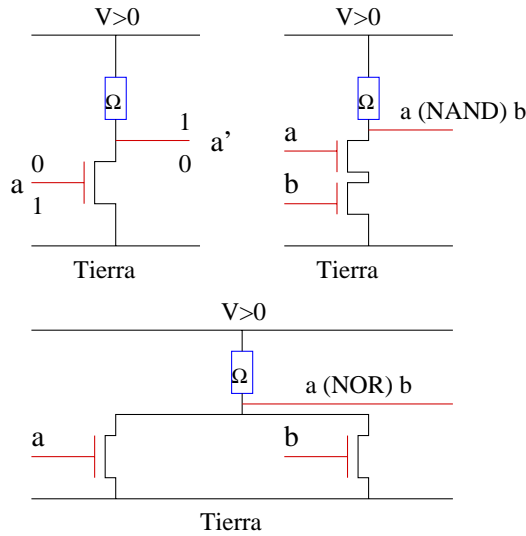


Figura 1: Representación esquemática de las puertas lógicas NOT, NAND, NOR por acción del transistor sobre la corriente. Ω denota una resistencia.

sale y viceversa. La acción de dos transistores sobre dos cables puede corresponderse bien con la operación lógica NAND o con NOR, dependiendo de la geometría (véase Figura 1). Con una combinación de estas tres *puertas lógicas* podemos implementar la suma binaria XOR = \oplus , donde AND almacena el “acarreo” y, de ahí, saltar a la multiplicación y a la resolución de ecuaciones diferenciales!

Nótese que las operaciones como NAND (Figura 1) en un ordenador son *irreversibles*. Es decir, conocido el resultado r de la suma $r = a \oplus b$, es imposible reobtener los sumandos a, b . Esta es la causa de que los ordenadores disipen calor (véase Figura 2). No obstante, siempre se puede hacer el cálculo *reversible* añadiendo en la salida uno de los sumandos (Figura 4), con lo cual no se pierde información acerca de la entrada. Esto supone acarrear “basura” en los cálculos, pero es el precio que hay que pagar por la reversibilidad, esencial ésta en la computación cuántica por medio de *transformaciones unitarias* (como la puerta lógica CNOT de la Figura 4).

Permítaseme usar la siguiente analogía, con el objetivo de introducir el concepto de “qubit”. Supongamos que disminuimos la corriente en el cable hasta el punto en que no somos capaces de distinguir si circula (1) o no circula (0), es decir, el flujo de electrones es tan bajo (posiblemente un solo electrón) que no podemos detectar la diferencia. Podríamos decir entonces que el estado de circulación de la corriente es una “mezcla estadística” $(\psi) = p_0(0) + p_1(1)$ de ambas posibili-

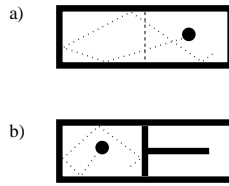


Figura 2: Analogía mecánica de la disipación de calor ($kT \ln 2$) al restringir los posibles valores de un bit: “partícula en la parte derecha (0) o izquierda (1) de la caja”, al valor (1) por acción de un pistón.

dades con probabilidades p_0, p_1 . No obstante, aunque parezca que ganamos en posibilidades, lo único que hacemos es introducir *errores* e incertidumbre. La computación cuántica no tendría pues ningún atractivo si no fuese porque el estado cuántico descrito por una función de onda

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \quad (3)$$

(c_0 y c_1 son números *complejos*) *no* es una mera mezcla estadística con probabilidades $p_0 = |c_0|^2$ y $p_1 = |c_1|^2$, sino que además incorpora *interferencia y enredo* (para este último se necesitan dos o más bits). El punto en común entre esta analogía clásica y el mundo cuántico es que la descripción de los fenómenos físicos empieza a necesitar de la teoría cuántica conforme las diferencias de energía —o, más precisamente, de *acción*— entre posibilidades alternativas (digamos, cero o uno) empieza a ser muy pequeña. Esto ocurre con más frecuencia en el mundo submicroscópico (a escala nanométrica) que en el macroscópico (clásico). Todas las alternativas $\psi_j \sim e^{\frac{i}{\hbar}S_j}$ que difieren poco $S_j - S_k \sim \hbar$ (la constante de Planck) en acción S , coexisten en una especie de superposición cuántica con pesos complejos —como en Eq. (3). Estas alternativas son indistinguibles para un observador (clásico), el cual no tiene acceso a dicha particular superposición. Para *observar* la superposición, lo único que puede hacer es “amplificar” las diferencias entre las posibles alternativas cuánticas hasta el nivel clásico, es decir, hasta que éstas son distinguibles por él. En este proceso de “amplificación” o de “medida”, la superposición se destruye y sólo una de las alternativas (digamos, cero ó uno) sobrevive a la experiencia. Éste es el tan controvertido proceso de medición o *colapso de la función de onda*, que ha creado (y sigue creando) tantos problemas filosóficos y de interpretación de la MC.*

*Como ancdota, está aquella interpretación (sostenida por algunos físicos célebres [3]) según la cual todas las potenciales alternativas cuánticas se realizan de forma real en diversos *universos paralelos*, los cuales interactúan mediante interferencia. Éste es el ingrediente básico de muchas películas y libros de ciencia ficción. O aquella otra

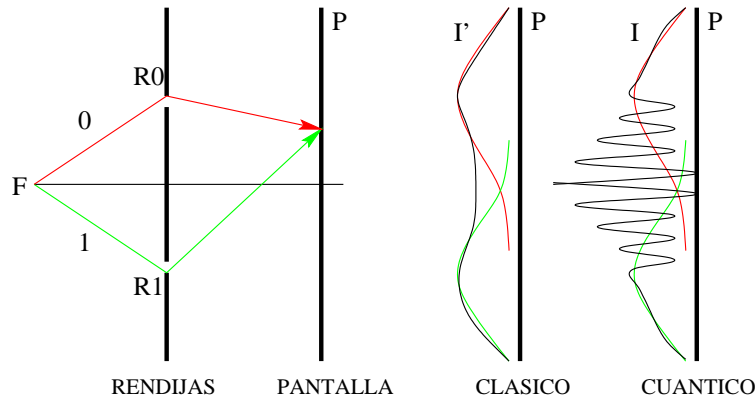


Figura 3: La interferencia entre los dos posibles caminos a seguir por un fotón (digamos, cero y uno) da lugar a una intensidad resultante (caso cuántico) $I \propto |c_0 + c_1|^2 \neq |c_0|^2 + |c_1|^2 \propto I'$, en cada punto de la pantalla P, diferente de la suma de intensidades a través de cada una de las rendijas (caso clásico). En particular, existen zonas en la pantalla donde el fotón “rehsa” llegar cuando se le abren más posibilidades (más rendijas); y al revés, existen otras zonas en la pantalla donde el fotón tiene más “querencia” (en lenguaje “taurino”) con las dos rendijas abiertas de la que tendría si se le obligase a entrar por una o por otra rendija. De hecho, cuando se amplifican las diferencias entre los caminos alternativos (es decir, cuando se mide la posición del fotón), sólo una alternativa sobrevive (el fotón sigue un cierto camino, 0 ó 1, cuando lo “miramos”) y el patrón de interferencia se destruye.

La coexistencia de alternativas cuánticas da lugar a efectos de interferencia que desafían el sentido común. Por ejemplo, el archiconocido experimento de Young de la doble rendija (véase Figura 3).

As pues, la función de onda (3) acarrea una información distinta de la clásica, la cual denominaremos *qubit* (“quantum bit”) [†]. Además de los *estados puros* $|0\rangle$ y $|1\rangle$ (tipo clásico), un qubit admite muchas más representaciones, como en (3). Dispositivos que pueden almacenar un qubit de información (es decir, “la contrapartida cuántica del cable”) son sistemas de dos niveles como: estados $|\uparrow\rangle$ y $|\downarrow\rangle$ de cualquier partícula subatómica de espín $\frac{1}{2}$; polarización horizontal $|\leftrightarrow\rangle$ y vertical $|\updownarrow\rangle$ de un fotón; estado fundamental $|0\rangle$ y excitado $|1\rangle$ de ciertos iones, etc. Por ejemplo, es posible preparar un estado como (3) haciendo incidir un haz de luz láser (la que sugiere la posibilidad de que la falta de determinismo en MC esté relacionada (compensada) con la pérdida de información en agujeros negros [4].

[†]léase “cúbit” ó “kiúbit”, a la inglesa...

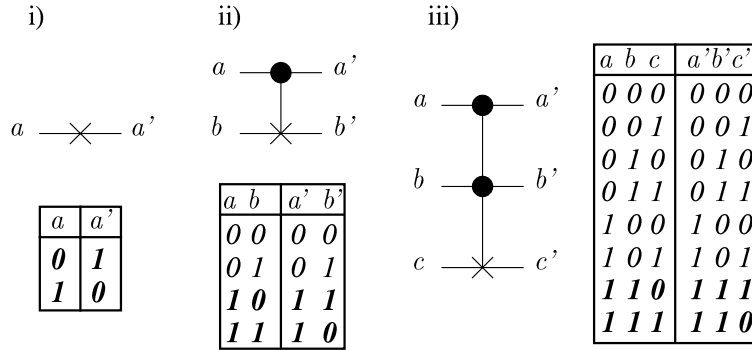


Figura 4: Representación esquemática de las puertas reversibles: NOT, CNOT y CCNOT o puerta de Toffoli. La concatenación de la puerta CNOT con la CCNOT da como resultado un “sumador cuántico”, donde c' almacena el acarreo.

contrapartida cuántica del transistor) de frecuencia y duración apropiadas sobre ciertos iones.

Nótese que, con dos qubits ($N = 2$), podemos preparar un registro en una superposición con todos los números ($2^2 = 4$) del 0 al 3 como (por simplicidad, nos olvidamos de la normalización):

$$|a\rangle = (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) = |00\rangle + |01\rangle + |10\rangle + |11\rangle = \sum_{x=0}^3 |x\rangle \quad (4)$$

Este puede ser el estado de espín ($|\downarrow\rangle \equiv |0\rangle$, $|\uparrow\rangle \equiv |1\rangle$) de los núcleos de carbono e hidrógeno en una molécula de cloroformo CHCl_3 . En este ordenador cuántico de “juguete” se puede implementar la operación lógica cuántica por excelencia: la puerta CNOT (NOT controlado), haciendo “cosquillas” a la molécula mediante pulsos de ondas de radio que invierten el sentido del espín de uno u otro núcleo. De hecho, siempre es posible asegurarse de que el núcleo de hidrógeno invierte su espín sólo cuando el espín del núcleo de carbono apunta hacia arriba (alineado con un campo magnético externo). Este comportamiento cuántico de la molécula CHCl_3 es lo que se denomina un NOT controlado (CNOT), con el núcleo de carbono como control y el de hidrógeno como puerta XOR = \oplus (véase Figura 4). Se prueba que la concatenación de puertas CNOT (a dos qubits), junto con operaciones arbitrarias a un qubit, es suficiente para diseñar cualquier operación clásica como: suma, multiplicación, etc. Para procesar información cuántica más compleja, parece prometedor usar una trampa lineal de iones (véase [5, 6, 7]), donde el acoplamiento entre los grados de libertad electrónicos y vibracionales permite (en principio) la implementación de operaciones en un registro de más de dos qubits por absorción y emisión de fotones y fonones.

En un ordenador cuántico de $N = 4$ qubits, la aplicación de la operación unitaria U_{\oplus} que implementa el algoritmo suma módulo 2^2 entre el estado (4) y un segundo estado como $|b\rangle = |x'\rangle$, con $x' = 0, \dots, 3$, da una salida de la forma:

$$|a\rangle |b\rangle = \sum_{x=0}^3 |x\rangle |x'\rangle \xrightarrow{U_{\oplus}} \sum_{x=0}^3 |x\rangle |x \oplus x'\rangle. \quad (5)$$

Es decir, hemos calculado simultáneamente (de una “tacada”!) la suma $x \oplus x'$ para cuatro valores distintos de x , mientras que un ordenador clásico de 4 bits necesitaría repetir la operación \oplus cuatro veces o, lo que es lo mismo, cuatro ordenadores clásicos trabajando en paralelo. Este es el denominado *paralelismo cuántico* que hace un computador cuántico mucho más potente que uno clásico. Imaginemos si en vez de disponer de $N = 4$ qubits tuviéramos el número de Avogadro!.

No obstante, nótese que sólo podemos medir o “amplificar” una de las 4 respuestas en la salida: $\sum_{x=0}^3 |x \oplus x'\rangle \xrightarrow{\text{medida}} |x_0 \oplus x'\rangle$. Veamos que lo que hace verdaderamente potente a la computación cuántica no es exactamente la superposición o paralelismo sino, más bien, el llamado *enredo*.

3 Enredo cuántico: la paradoja EPR

Existen situaciones físicas en las que se pueden crear parejas de partículas (electrones y positrones, fotones, etc) que mantienen sus lazos “afectivos” (esto las “humaniza”...) aunque estén a millones de kilómetros la una de la otra, de manera que el estado (de “ánimo”) de una condiciona el estado (de “humor”) de la otra en cada instante, como si de “telepatía” se tratase. Es como tener dos dados mágicos que coinciden en cada tirada...!. Por ejemplo, se crean pares enredados electrón-positrón $|\mathbf{EP}\rangle = |\uparrow\rangle_e |\downarrow\rangle_p - |\downarrow\rangle_e |\uparrow\rangle_p$ por desintegración de una partícula neutra con espín cero; o parejas de fotones con polarizaciones ortogonales $|\mathbf{VH}\rangle = |\downarrow\rangle_1 |\leftrightarrow\rangle_2 - |\leftrightarrow\rangle_1 |\downarrow\rangle_2$ al incidir un pulso de luz láser sobre ciertos cristales no lineales. Éstos son casos particulares de estados enredados: estados singlete. En principio, siempre es posible producir (por otros medios) estados más generales con diferentes grados de enredo (no necesariamente “máximamente enredados”) y un número arbitrario de partículas, aunque las dificultades técnicas aumentan pasando ya de dos partículas (en [8] se clama haber logrado crear el estado enredado de tres partículas $|000\rangle + |111\rangle$ en la molécula C_2HCl_3).

En lo que se refiere a un par enredado EP , la situación es la siguiente (véase la Figura 5). A partir del resultado de la medición del espín del electrón E por parte de Antonia (A) —el cual puede resultar en: bien paralelo $|\uparrow\rangle_e$ o bien antiparalelo $|\downarrow\rangle_e$ a un campo magnético externo \vec{H} — puede predecirse con certeza el resultado que obtendrá Bartolo al medir la misma componente de espín del positrón —la cual deberá ser siempre contraria a la de su “media naranja”: el electrón— incluso si Bartolo se encuentra en la “Conchinchina” o, en términos más precisos, separado de Antonia por un intervalo de género espacio, de manera que es imposible cualquier intercambio de información (de producirse, debería tener lugar a velocidades superlumínicas, violando as la causalidad Einsteniana).[‡] Desde una visión localista (como la de Einstein [10]), Antonia podría elegir también libremente otras direcciones de \vec{H} sin que su elección pudiera influir en las mediciones de Bartolo, ya que suponemos que éste se encuentra en una región espacialmente separada (la Conchinchina). Esto sugeriría entonces que todas las componentes de espín del positrón que viaja hacia Bartolo tienen valores bien definidos incluso antes de que Bartolo perturbe el sistema o “colapse” la correspondiente función de onda; y lo mismo pasa con el electrón, con tal de intercambiar los papeles de Antonia y Bartolo.

Pero este razonamiento resulta ser erróneo. Lo cierto es que, si uno insiste en hablar de resultados de experimentos que se excluyen mutuamente, entonces uno se ve forzado a concluir que la elección de aparato de medida (dirección de \vec{H}) de Antonia ejerce una sutil influencia que condiciona los resultados de Bartolo, y viceversa (esto es lo que se denomina la “no localidad” de la MC). Ésta es la cara “esotérica” de la MC que no gustaba nada a Einstein [10] quien, aun consciente de la imposibilidad de explotar este fenómeno para comunicaciones “superlumínicas”, siempre se sintió “ofuscado” por el enredo cuántico. Einstein, antes que aceptar la aleatoriedad como una característica intrínseca e ineludible de la medición cuántica (de ah su famosa frase: “Dios no juega a los dados”), prefirió pensar que la descripción física dada por la función de onda mecanocuántica no podía ser considerada *completa* [10]. Él pensó que la indeterminación en MC podría erradicarse adoptando una descripción más completa, aún local, de la Naturaleza y propuso su teoría de *variables ocultas*, según la cual la medición es determinista aunque aparece como probabilística debido a que algunos “grados de libertad” no se conocen precisamente. Más

[‡]Antonia y Bartolo son la “contrapartida Ibérica” de los personajes Alice y Bob, utilizados en la literatura (inglesa) para este tipo de experimentos imaginarios. Con ello el autor pretende (no sabe si consigue...) introducir una nota de humor, sin ánimos de crear ningún problema “lingüístico”.

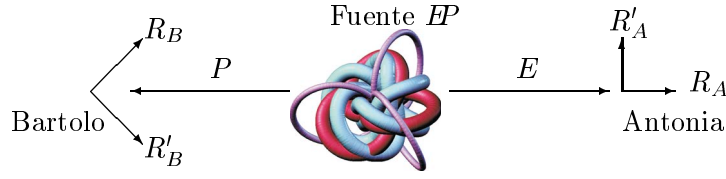


Figura 5: Representación esquemática del experimento imaginario con pares enredados EP . A y B están equipados con sendos campos magnéticos \vec{H} orientables en las direcciones: \uparrow , \rightarrow , \nearrow , \searrow , al estilo del archiconocido experimento de Stern-Gerlach para átomos de plata; aunque, como bien apunta el evaluador, para el caso de partículas cargadas y de masa pequeña (como el electrón o el positrón en nuestro caso), la fuerza de Lorentz desbarata la separación de haces [9], debiéndose introducir modificaciones (que no vienen a cuento). No obstante, el lector que se encuentre incómodo con el uso de electrones, positrones y campos magnéticos en este experimento imaginario, siempre puede sustituirlos por fotones enredados y polarizadores con tal de considerar el ángulo mitad correspondiente en las expresiones que siguen.

tarde, J.S. Bell [11] destruiría este sueño con sus famosas *desigualdades*. Veamos mediante un ejemplo cómo una visión localista es incompatible con las predicciones de la MC.

Continuemos con nuestro par “siamés” EP y veamos cómo a Bartolo, fiel a la doctrina Einsteiniana, no le salen las cuentas. En efecto, el argumento es un poco “enredado”, pero vamos a intentarlo. Supongamos que el campo magnético \vec{H} de Antonia tiene dos posiciones: \uparrow y \rightarrow (véase Figura 5), mientras que el de Bartolo está girado, digamos, $\theta = \pi/4$ con respecto al anterior: \nearrow y \searrow . La medición del espín para cada dirección de \vec{H} tiene dos respuestas: SI (cuando el espín y \vec{H} son paralelos) o NO (cuando son antiparalelos). Supongamos que (A, B) colocan inicialmente sus aparatos de la forma $(\vec{H}_A, \vec{H}_B) = (\rightarrow, \nearrow)$. La MC predice que la probabilidad de que ambos, A y B , estén de acuerdo en sus respuestas —(SI,SI) ó (NO,NO)— es $\sin^2(\frac{\theta}{2})$, donde θ es el ángulo que forma \vec{H}_A con \vec{H}_B ($\theta = \pi/4$ en este caso); es decir, la probabilidad de acuerdo está rondando el 15%, lo cual puede verificarse experimentalmente tras la medición de muchos pares EP . Sea $(R_A = \text{SSNS}..., R_B = \text{NSSN}...)$ el resultado de, pongamos por caso, 100 medidas de A y B , respectivamente. Bartolo, el cual se encuentra en la Conchinchina, piensa que sus resultados R_B no se ven afectados por la elección \uparrow ó \rightarrow que haga Antonia de su aparato de medida, y viceversa. Es más, cree que el resultado global hubiese sido (R'_A, R_B) en

vez de (R_A, R_B) si se hubiese escogido la disposición $(\vec{H}_A, \vec{H}_B)' = (\uparrow, \nearrow)$ en vez de $(\vec{H}_A, \vec{H}_B) = (\rightarrow, \nearrow)$ ya que, desde su mentalidad local, los valores de las componentes de espín estaban ya predefinidos antes de que él midiera (recuérdese el argumento al final del segundo párrafo); el acuerdo en las respuestas (R'_A, R_B) seguiría siendo del 15%, ya que el ángulo entre ambos aparatos sigue siendo el mismo que antes $\theta' = \theta = \pi/4$. De la misma forma, según el incrédulo de Bartolo, si la disposición hubiese sido $(\vec{H}_A, \vec{H}_B)'' = (\rightarrow, \searrow)$, la respuesta hubiese sido (R_A, R'_B) , con un acuerdo, de nuevo, del 15%. Bartolo podría predecir entonces que el acuerdo en el resultado (R'_A, R'_B) de la disposición $(\vec{H}_A, \vec{H}_B)''' = (\uparrow, \searrow)$ no podría sobrepasar un $15\% + 15\% + 15\% = 45\%$.[§] Pero, he aquí su sorpresa!, cuando realiza el experimento y ve que el acuerdo es del 85%, tal y como predice la MC: $\text{sen}^2(\frac{\theta'''}{2}) \simeq 0.85$ para $\theta''' = 3\pi/4$. En realidad, este tipo de experimentos no se hacen con electrones (y menos con positrones) ni con partículas de espín 1/2, sino con fotones (véase por ejemplo [12]) y, para ser justos, parece que la eficiencia de los detectores actualmente no es suficiente como para descartar definitivamente la teoría de variables ocultas en favor de la MC, aunque se cree que ello es sólo cuestión de tiempo, sobre todo cuando se aprenda a manipular de forma eficiente estados enredados más generales como los descritos en [8].

Ante los resultados, Bartolo puede tomar tres opciones: 1) decir que la MC no proporciona un conocimiento completo, 2) empezar a creer en fenómenos “paranormales” ... o, quizás lo más razonable, 3) aprender que puede ser peligroso razonar acerca de lo que podría haber ocurrido pero, de hecho, no sucedió. El principio de *complementariedad* de Bohr nos advierte precisamente ante esta forma de proceder cuando declara que: *está prohibido considerar simultáneamente los posibles resultados de dos experimentos que se excluyen mutuamente*. Esto no pasa en nuestra vida diaria, a nivel macroscópico. En efecto, podría mos pensar en “pares enredados” compuestos de: bolas verdes y rojas, de madera y metal, de 0.5 y 1 kilo, etc. Nuestros aparatos de medida (el análogo de las distintas direcciones del campo magnético) podrían ser: una linterna, fuego, una báscula, etc, de manera que si mandamos una bola del par enredado a Bartolo y otra a Antonia, y ésta ve que es roja, necesariamente la otra bola “colapsa” al estado verde... lo cual puede ser

[§]Para probar esta afirmación, mejor que una demostración rigurosa, el lector puede recurrir a ejemplos concretos para hacerse una idea. Por ejemplo, como caso más sencillo tómanse tres parejas consecutivas cualesquiera de cuatro respuestas en las que sólo coincida una de entre las cuatro —como en $(R_A, R_B) = (\text{SNSN}, \text{SSNS})$ — y nótese que nunca podrá haber más de $1+1+1=3$ coincidencias (sobre 4) entre (R'_A, R'_B) .

verificado por Bartolo (lo mismo con las otras propiedades). Qué hay de extraño entonces en el enredo cuántico?. Precisamente, a diferencia del caso cuántico, lo que no ocurrirá aquí nunca es que Bartolo pueda pensar que la elección de aparato (linterna, fuego, báscula, etc) por parte de Antonia pueda condicionar sus resultados si éste está en la Conchinchina, con lo cual no puede recibir señales (de humo, pongamos por caso...); y si así fuera, entonces es cuando tendríamos que empezar a pensar en fenómenos “telepáticos”. Esto es porque las bolas, a diferencia de los electrones, tienen propiedades (color, material, peso, etc) *definidas* antes de que se las mida. No hay pues nada “esotérico, paranormal o telepático” en el enredo cuántico cuando se admite que, a diferencia de un sistema clásico, *un sistema cuántico no tiene valores definidos de todas sus propiedades (digamos, las tres direcciones de espín) antes de efectuar la medición.* Sin embargo, el enredo cuántico proporciona correlaciones sin parangón clásico; desde este punto de vista, enredo significa más que correlación: significa *inseparabilidad*.

Está claro que este tipo de experiencias a nivel submicroscópico, tan poco comunes en el mundo macroscópico, podrían ser usadas eficientemente en un futuro para crear situaciones realmente sorprendentes. Imaginemos una red, a nivel mundial, de ordenadores conectados “vía enredo” que cooperan realizando tareas que resultarían difíciles o imposibles incluso por conexión vía satélite. Esto entra dentro del terreno de la especulación, aunque ya se han conseguido algunas aplicaciones cuánticas reales (sencillas) del enredo en ámbitos considerados hasta hace poco dominio de la “ciencia ficción”. Veamos algunas de estas aplicaciones actuales y futuras del enredo en el terreno de las telecomunicaciones y computación cuántica. ¶

4 Teleportación por enredo

Una de las aplicaciones más espectaculares del enredo es la posibilidad de transportar un sistema cuántico de un lugar a otro del espacio sin necesidad de acarrear materia, sólo información. La teleportación del estado de polarización de un fotón es hoy por hoy una realidad gracias al grupo de Innsbruck [13]; no obstante, de ahí a la teleportación del estado cuántico de una colección de átomos (digamos, la “función de onda de una vaca”) hay un larguísimo (si nó imposible) camino

¶El autor es consciente de que esta sección deja bastantes lagunas que no es posible cubrir por razones de espacio. El lector interesado puede leer por ejemplo el artículo de G. García-Alcaine en [7], pags. 17-29, y referencias allí citadas para más detalles.

por recorrer... La idea original de la teleportación cuántica se debe a [14] y trata de lo siguiente (véase también el artículo [15], publicado en esta revista).

Antonia confiesa a Pancracio que quiere ($|1\rangle$) a Bartolo un $|c_1|^2 = 75\%$, pero también lo odia ($|0\rangle$) un $|c_0|^2 = 25\%$. Pancracio aprovecha por el cumpleaños de Bartolo para mandar, a través de Antonia, un qubit $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ con dicha información. Es inútil que Antonia intente fisgonear el regalo porque “los regalos cuánticos colapsan cuando los miras...”. También sabe que, al ser un qubit, éste es muy frágil y su estado podría alterarse fácilmente durante el trayecto (en el argot mecano-cuántico se habla de “síndrome” de la *decoherencia*). Antonia piensa por un instante en hacer varias copias de este intrigante regalo $|\psi\rangle$, con la esperanza de que alguna llegará sana y salva, pero el teorema (“sacro-cuántico”) de “no-clonará” se lo impide; en efecto: para copiarlo tendría que mirarlo!^{||} Pancracio sabe el estado en que preparó su regalo, pero Antonia no sabe dónde está Pancracio. Desesperada, mientras ve la serie de televisión de “Star Trek”, le vienen a su mente aquellos experimentos con Bartolo sobre partículas enredadas y, eureka!, problema resuelto. Coge uno de sus qubits enredados compartidos con Bartolo, lo combina con el regalo de Pancracio y hace una “medición a dos qubits” o de “coincidencia” (también denominada “medición de Bell”) con dos detectores D_1 y D_2 , la cual puede tener cuatro respuestas distintas: $(R_{D_1}, R_{D_2}) = (s, s), (s, N), (N, s), (N, N)$ (véase Figura 6). Si detecta ambos qubits, es decir, si la respuesta es (s, s) (lo cual ocurre el 25% de las veces), puede llamar a Bartolo y decirle que su regalo se encuentra ya en la caja de qubits enredados que comparte con ella; es decir, el otro miembro del par enredado (la otra media naranja...) ha suplantado al regalo de Pancracio $|\psi\rangle$. El otro 75% de las veces, Antonia puede todavía decirle a Bartolo qué operaciones tiene que realizar con su “medio par” para rotarlo a $|\psi\rangle$.

Nótese que es importante que el par enredado conserve sus lazos afectivos, para que la teleportación sea efectiva. Como se ha dicho, se ha conseguido teleportar el estado de polarización de un fotón (un regalo un tanto soso, la verdad sea dicha...), es decir, un qubit de información (véase Figura 6). Esto abre el camino para las telecomunicaciones cuánticas, las cuales sufren del mal de la *decoherencia*. Es decir, al estar vedada la *clonación* perfecta de qubits, no es posible amplificar la señal cuántica, la cual se degrada tras unas decenas de kilómetros aun utilizando fibra óptica. No obstante, estaciones de teleportación intermedias podrían salvar este obstáculo.

^{||}No obstante, se pueden clonar estados ortogonales (el análogo cuántico de los bits clásicos: cero y uno), pero entonces ya se tiene alguna información previa sobre ellos: la ortogonalidad.

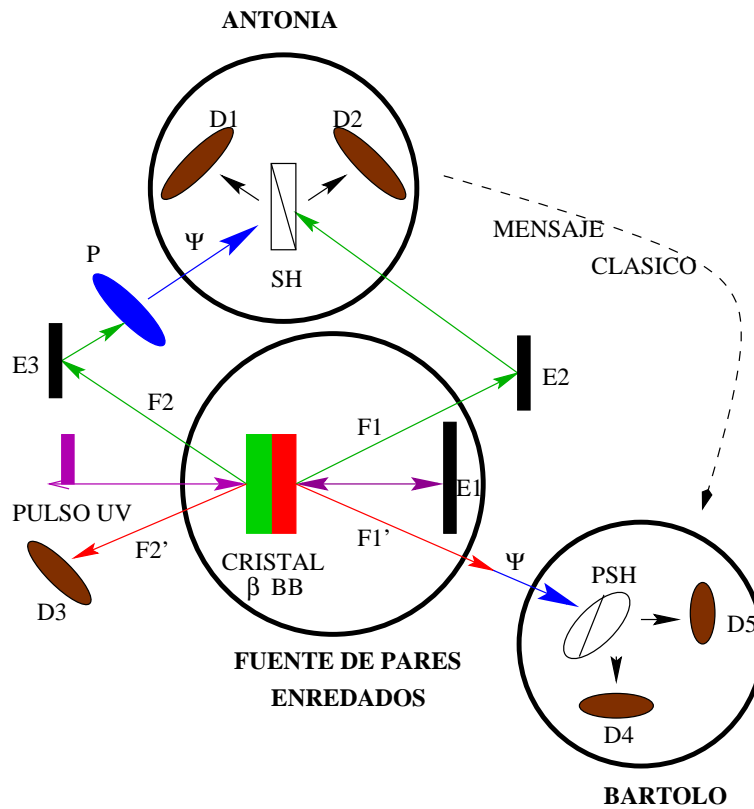


Figura 6: Teleportación del estado de polarización de un fotón: un pulso de luz láser ultravioleta incide sobre un cristal de β -Borato de Bario creando un par de fotones enredados ($F1, F1'$) a la ida y otro ($F2, F2'$) a la vuelta (tras reflejarse en el espejo $E1$). El polarizador P de Pancracio prepara el fotón $F2$ en el estado Ψ , el cual se superpone a $F1$ por medio de un separador de haces (SH), o espejo remiflejante, para que Antonia haga una medida de coincidencia con los detectores $D1, D2$. Si ambos detectores son alcanzados, Antonia comunica a Bartolo que el fotón $F1'$ ha transmutado a Ψ , lo cual puede ser verificado por Bartolo usando un PSH (polarizador separador de haces consistente en un cristal de calcita).

5 Criptografía Cuántica



Figura 7: “Come here at once”

La Figura 7, tomada de [16], reproduce el cebo que el afamado detective Sherlock Holmes tiende al peligroso criminal Abe Slaney, el cual utiliza un lenguaje secreto consistente en figuras de un bailarín. El error de Abe es utilizar siempre el mismo sistema criptográfico. Sherlock Holmes colecciona varios mensajes y es capaz de identificar la letra “e” (la más común en la escritura inglesa) y, con la intuición que lo caracteriza, el resto.

5.1 Faustino el “fisgón” frustrado

Los ingredientes básicos para encriptar un mensaje secreto M son: una clave K (conocida por el remitente y el destinatario) y un algoritmo criptográfico E que asigna un criptograma $C = E_K(M)$ a M por medio de K . El proceso de desencriptación consiste en aplicar el algoritmo inverso $M = E_K^{-1}(C)$. Por ejemplo, el algoritmo llamado “one-time pad” utilizado por los diplomáticos alemanes y soviéticos durante la segunda guerra mundial consiste básicamente en lo siguiente. Dado un mensaje $M = \{m_1, \dots, m_q\}$ de q caracteres —con $m_j = 0, \dots, 2^5 - 1$, incluyendo signos de puntuación en (1)— y una clave $K = \{k_1, \dots, k_q\}$, podemos producir un criptograma $C = \{c_1, \dots, c_q\}$ usando la aritmética modular en base 32: $c_j = m_j \oplus k_j$ (módulo 32). Por ejemplo:

$$\begin{aligned}
 M &= \{ \text{S E C R E T O} \} \\
 &= \{ 19 \ 04 \ 02 \ 18 \ 04 \ 20 \ 15 \}, \\
 K &= \{ 29 \ 17 \ 31 \ 25 \ 04 \ 14 \ 00 \}, \\
 C &= \{ 16 \ 21 \ 01 \ 11 \ 08 \ 02 \ 15 \} \\
 &= \{ \text{P U B L I C O} \}.
 \end{aligned} \tag{6}$$

La seguridad de este sistema criptográfico está garantizada mientras la forma de generar la clave K sea aleatoria (mi elección ha sido “a propósito”...) y ésta no se utilice más de una vez. El

problema está cuando el remitente (digamos, Antonia) y el destinatario (digamos, Bartolo) están lejos el uno del otro y se quedan sin claves. Ambos pueden crear más por teléfono, pero el figón de Faustino lo tiene pinchado. Antonia y Bartolo utilizan entonces su tecnología más avanzada a base de pares enredados EP de la siguiente manera (el argumento se debe a [17]). Ambos pueden elegir la dirección de sus campos magnéticos \vec{H} : \uparrow ó \rightarrow , a placer. Tras medir n pares, éstos hacen pública la elección de dirección pero *no* el resultado de la medida, que puede ser: SI= $|\uparrow\rangle$ ó NO= $|\downarrow\rangle$. En media, habrán coincidido en la elección de dirección alrededor de $n/2$ veces, para las cuales las respuestas están perfectamente (anti-)correlacionadas $(R_A, R_B) = \begin{cases} (S, N) \equiv 0 \\ (N, S) \equiv 1 \end{cases}$. La gracia está en quedarse con las respuestas $(R_A, R_B) = 0, 1$ de esas $n/2$ coincidencias y construir la clave en binario $K = (00101, \dots, 10101)$, pasándola luego a decimal a través de la fórmula (2).

Se puede demostrar que las respuestas (R_A, R_B) están efectivamente anti-correlacionadas *si y sólo si* el figón de Faustino no ha intentado trastocar los pares EP , lo cual puede verificarse sacrificando parte de la clave K (véase [20] para una demostración sencilla). La seguridad de este algoritmo cuántico de generación de claves reside en que el figoneo (la observación) de Faustino destruye el enredo mecano-cuántico. Resumiendo: *las telecomunicaciones cuánticas detectan la presencia de figones*. De hecho, se han logrado establecer comunicaciones cuánticas seguras en un radio de 23 Km.

5.2 La venganza de Faustino: el “hacker” cuántico

Pero la criptografía por enredo sale cara (sobre todo la fibra óptica) y los pares enredados son muy frágiles. Así es que Antonia y Bartolo deciden acogerse al protocolo RSA (en honor a Rivest, Shamir y Adleman) de la “clave pública” que, aunque clásico, es suficientemente seguro. Éste consiste en lo siguiente. Antonia hace pública su clave, consistente en un par de números enteros grandes (s, c) (del orden de varias decenas de cifras) para que cualquiera pueda mandar mensajes M encriptados de la siguiente forma. Pongamos que $M = 001110\dots$ viene dado por una secuencia larga de números binarios; la versión encriptada será $C = M^s \pmod{c}$. Para desencriptar el mensaje, Antonia usa la siguiente fórmula $M = C^t \pmod{c}$, donde $t = t(s, p, q)$ se deduce fácilmente a partir de s y los factores primos p, q (en la práctica dos números primos grandes conocidos sólo por Antonia) de c resolviendo las ecuaciones (simples): $st \equiv 1 \pmod{p -$

1), $st \equiv 1 \pmod{q-1}$. Cualquier otro fisgón que quiera descifrar el mensaje M a partir de C , tiene que calcular t , para lo cual tiene que descomponer antes c en producto de primos $c = pq$. Para hacerse una idea de la dificultad del problema, imagínese un número c de 50 dígitos $c \simeq 10^{50}$, producto de dos primos desconocidos p, q . En el peor de los casos, para averiguar p, q tenemos que hacer una media de $\sqrt{c} \simeq 10^{25}$ divisiones (todos hemos hecho de pequeños este tipo de factorizaciones, pero nuestro profesor nunca fue tan cruel como para pasar de dos dígitos...). Un señor computador capaz de hacer 10^{10} divisiones por segundo tardaría del orden de 10^{15} segundos en encontrar p ó q . Teniendo en cuenta que la edad del universo se estima en $3,8 \cdot 10^{17}$ segundos, esto desanima a cualquier fisgón.** “Pero no a Faustino, que derrotado por la MC se aliara al enemigo y construirá un ordenador cuántico que efectuará $2^{(10^{10})}$ operaciones por segundo!, acabando con la criptografía clásica en un suspiro...”

Aunque la amenaza de Faustino no quita el sueño (por ahora...) ni a Antonia ni a Bartolo, quienes son conscientes de la falta de “hardware” cuántico, s es cierto que existe ya “software” disponible consistente en un algoritmo cuántico ideado por P.W. Shor [19] que reduce el tiempo de cálculo a una función polinómica en el número de dígitos $\log c$, trasladando el problema de la factorización a otro nivel (ahora tratable) de complejidad. La eficiencia del algoritmo radica, una vez más, en el paralelismo y el enredo mecánico-cuántico. Esencialmente, el problema de factorizar un número c se reduce a encontrar el periodo r de la función $F_c(x) = a^x \pmod{c}$, donde a es un número cualquiera entre 0 y c (véase [20] para más detalles). Aplicando la transformación unitaria U_F que realiza la operación F —recuérdese el caso (5)— a una superposición de $\omega \gg r$ números x

$$\sum_{x=0}^{\omega-1} |x\rangle |0\rangle \xrightarrow{U_F} \sum_{x=0}^{\omega-1} |x\rangle |F_c(x)\rangle \xrightarrow{F_c(x)=u} \sum_{j=0}^{j \simeq \omega/r-1} |x_u + jr\rangle |u\rangle \quad (7)$$

y efectuando una medición cualquiera $F_c(x) = u$ en el segundo registro, dejamos el primer registro en una superposición coherente de $z \simeq \omega/r$ números que difieren en múltiplos jr del periodo r , el cual puede obtenerse tras una “transformada de Fourier cuántica” (véase, por ejemplo, [20]). Es el enredo entre $|x\rangle$ y $|F_c(x)\rangle$ el que hace posible este “escaneo masivo” de la función F_c . Nótese la similitud entre el algoritmo de Shor y la difracción de rayos X a través de una estructura periódica, donde la red permite la propagación de sólo ciertas longitudes de

**Existen algoritmos clásicos mejores que reducen el tiempo de cálculo a 42 días para un número de 130 cifras a 10^{12} operaciones por segundo [18]. No obstante, el tiempo de cálculo sigue creciendo exponencialmente con el número de dígitos $\sim \log c$, haciendo el problema intratable (por la vía clásica)

onda, reflejando el resto.

6 El buscador cuántico de Grover

Entre los diferentes algoritmos cuánticos existentes hasta el momento, el de Shor es el más llamativo por su carácter “amenazante”; aunque existen otros como el de Lov K. Grover [21] que también ponen de manifiesto la potencial utilidad de un ordenador cuántico.

Mientras que el ordenador clásico de Bartolo necesita en media del orden de $P/2$ intentos para encontrar el número de teléfono de Antonia x_A entre una lista desestructurada de P personas, el superordenador de Faustino, el cual usa “software” de Grover, lo hace en alrededor de \sqrt{P} iteraciones (con probabilidad de éxito de $\sim (P-1)/P$) sobre la superposición cuántica $|\Psi\rangle = \frac{1}{\sqrt{P}} \sum_{x=0}^{P-1} |x\rangle$ de todos los elementos de la lista (“búsqueda paralela”). El algoritmo cuántico es claramente más rentable cuanto mayor es P . Sin entrar en demasiados detalles, el proceso de búsqueda consiste en realzar la amplitud de probabilidad del estado $|x_A\rangle$ y amortiguar el resto en la superposición $|\Psi\rangle$ mediante sucesivas operaciones unitarias (rotaciones) U_G que actúan de la siguiente manera. El estado $|\Psi\rangle$ se puede escribir también como $|\Psi(\theta_0)\rangle = \sin(\theta_0)|x_A\rangle + \frac{\cos(\theta_0)}{\sqrt{P-1}} \sum_{x \neq x_A} |x\rangle$ con $\sin(\theta_0) = 1/\sqrt{P}$. La rotación de Grover resulta en un sutil efecto de interferencia que lleva a la siguiente transformación:

$$|\Psi(\theta_0)\rangle \xrightarrow{U_G} |\Psi(\theta_1)\rangle, \quad (8)$$

donde $\theta_1 = \theta_0 + \phi$, con $\sin(\phi) = 2\sqrt{P-1}/P$. Aplicando U_G alrededor de $t \simeq (\pi/4)\sqrt{P}$ veces (ni más, ni menos tiempo), tendremos “el pastel a punto”; es decir, $\theta_t \simeq \pi/2 \Rightarrow |\Psi(\theta_t)\rangle \simeq |x_A\rangle$. Compruébese que para $P = 4$ (dos qubits), una sola iteración basta para que $|\Psi\rangle$ gire directamente a $|x_A\rangle$!

Desde que D. Deutsch [22] propusiera el primer algoritmo cuántico, otros muchos han saltado a la palestra, aunque casi todos usan el mismo principio que el de Shor o el de Grover. No cabe duda que la construcción de un ordenador cuántico (uno de los mayores logros tecnológicos de todos los tiempos...) constituiría un acicate para la invención de otros esencialmente distintos.

7 Perspectivas

Frente a la producción copiosa de “software” cuántico durante la última década, contrasta la enorme dificultad tecnológica en el diseño de “hardware” donde correr de forma eficiente los algoritmos cuánticos. Se han logrado verificar los algoritmos de Grover y Shor en “computadoras cuánticas” de 2 y 3 qubits con técnicas importadas de la Resonancia Magnética Nuclear. La trampa lineal de iones mencionada antes podría manejar un orden de magnitud más. Pero esto es lo máximo que podemos aspirar por ahora: manipular pequeñas cantidades de información cuántica; o, como propuso Feynman hace ya tiempo [23], simular sistemas físicos cuánticos sencillos por medio de otros artefactos cuánticos. De ahí a la realización práctica de las poderosas máquinas que augura la teoría, aún queda un incierto camino por recorrer. Antes hay que desarrollar “vacunas” eficientes contra el “virus” de la decoherencia, así como la corrección cuántica de errores (la contrapartida de la replicación o redundancia clásicas). No obstante, la criptografía y telecomunicaciones cuánticas pueden tener aplicaciones tecnológicas en un futuro cercano [24].

Para los pesimistas, recordemos una discusión en la edición de marzo de 1949 de la revista “Popular Mechanics” que decía algo así como: *mientras que una calculadora ENIAC (“Electronic Numerical Integrator and Calculator”) está equipada con 18.000 tubos de vacío y pesa 30 toneladas, los computadores en un futuro podrán tener sólo 1000 tubos de vacío y pesar 1,5 toneladas... menudo portátil!*

Agradecimientos

Agradezco a la Universidad de Granada por una beca post-doctoral y al Departamento de Física de la Universidad de Gales en Swansea (Reino Unido) y al Instituto de Astrofísica de Andalucía en Granada por su hospitalidad durante la escritura de la mayor parte de este artículo. A Pepito, el cual prefiere permanecer en el anonimato, su ayuda en el diseño del “ordenador cuántico”. Los demás personajes de este episodio son ficticios; cualquier parecido con la realidad es pura coincidencia...

Referencias

- [1] Edición especial de Scientific American, titulada “Solid state century” (Diciembre 1997).
- [2] B. Schumacher, Phys. Rev. **A51** 2738 (1995); B. Schumacher & M.A. Nielsen, Phys. Rev. **A54**, 2629 (1996).
- [3] H. Everett, Rev. Mod. Phys. **29**, 454 (1957). Véase también D. Deutsch, *The Fabric of Reality*, Penguin Publishers, London (1997).
- [4] R. Penrose, *The Emperor’s New Mind*, Oxford University Press (1989).
- [5] J.I. Cirac & P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
- [6] J.M. Doyle & B. Friedrich, Rev. Esp. Fis. **13**, 15 (1999).
- [7] Mientras se daban los últimos retoques a estas notas, cayó en mis manos el maravilloso número especial de esta revista: “Cien Años de Quanta”, volumen **14**(1), el cual contiene varios artículos dedicados también a aspectos físicos y tecnológicos del procesamiento y transmisión de la información cuántica.
- [8] R. Laflamme et al, Phil. Trans. Roy. Soc. Lond. **A356** 1941 (1998).
- [9] G. Baym, *Lectures on Quantum Mechanics*, pag. 329, Benjamin (1969).
- [10] A. Einstein, B. Podolsky & N. Rosen, Phys. Rev. **47**, 777 (1935). El experimento imaginario propuesto en esta referencia se denomina usualmente “paradoja EPR” y constituye el primer signo de enredo.
- [11] J.S. Bell, Physics **1**, 195 (1964); Rev. Mod. Phys. **38**, 447 (1966).
- [12] A. Aspect, P. Grangier and G. Roger, Phys. Rev. Lett. **47**, 460 (1981).
- [13] D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter & A. Zeilinger, Nature **390**, 575 (1997).
- [14] C.H. Bennet, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, & W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

- [15] G. García Alcaine, *Rev. Esp. Fis.* **12**, 6 (1998).
- [16] A.C. Doyle & J.A. Hodgson, *Sherlock Holmes*, Basingstoke: Macmillan (1994).
- [17] A. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [18] R.E. Crandall, *The challenge of large numbers*, Scientific American, pag. 59, Febrero (1997).
- [19] P.W. Shor, *Proceedings of the 35th Annual Symposium on the Theory of Computer Science*, editado por S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA), pag. 124 (1994).
- [20] J. Preskill, *Lecture Notes for Physics* **229** (1998). Disponible en la página Web <http://www.theory.caltech.edu/people/preskill/ph229>. Otros artículos de revisión a nivel introductorio son: V. Vedral & M.B. Plenio, *Prog. Quant. Electron.* **22**, 1 (1998); A. Steane, *Rep. Prog. Phys.* **61**, 117 (1998); A. Ekert, P. Hayden & H. Inamori, *Basics Concepts in Quantum Computation*, Les Houches summer school 1999.
- [21] L.K. Grover, *Phys. Rev. Lett.* **79**, 325 (1997).
- [22] D. Deutsch, *Proc. Roy. Soc. Lond.* **A400** 97 (1985).
- [23] R.P. Feynman, *Int. J. Theor. Phys.* **21**, 467 (1982).
- [24] Ocuparía mucho espacio el dar una lista medianamente completa de referencias. En vez de ello, el lector interesado puede visitar las páginas: <http://www.qubit.org>, para tutorías a nivel básico y otros enlaces; o el “espejo” <http://xxx.unizar.es> (sección quant-ph) para buscar artículos y mantenerse al día en el tema.