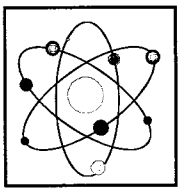


COMPUTACIÓN CUÁNTICA: NUEVAS PERSPECTIVAS EN EL TRATAMIENTO DE LA INFORMACIÓN

Pedro J. Salas Peralta, Ángel L. Sanz Sáenz***

(*) Profesor Titular del Dpto Tecnologías Especiales Aplicadas a la Telecomunicación
(**) Profesor Titular del Dpto. Física Aplicada a las Tecnologías de la Información
Universitat Politècnica de Madrid Ciudad Universitaria s/n, 28040 Madrid

INTRODUCCIÓN

El concepto de ordenador se pierde quizás en la historia del ser humano. Los primeros se construyeron para propósitos muy concretos y eran poco versátiles. Un ejemplo son los monumentos megalíticos como las estructuras de Stonehenge, en Inglaterra, que servían para predecir eventos astronómicos. Evidentemente si se hubiera deseado utilizar tales construcciones para otros cometidos habría sido necesario cambiar las piedras de sitio o incluso de tamaño. El proceso de programación sería realmente difícil.

A lo largo de la historia, las máquinas de cálculo se fueron complicando a la vez que se iban volviendo más versátiles, pasando desde el ábaco hasta las máquinas calculadoras de Pascal o Leibnitz. Sin embargo, la escasa utilidad de tales máquinas para la vida diaria de la época, las relegó al olvido durante cien años.

A medida que los ordenadores han aumentado su velocidad de funcionamiento, su tamaño ha ido disminuyendo debido a que la velocidad de la luz es finita. La tecnología de los ordenadores ha evolucionado siguiendo un proceso de miniaturización que lleva de los relés, válvulas, transistores hasta los circuitos integrados... Parece que el próximo nivel será el molecular. Sin embargo, a este nivel no sólo hay que tener en cuenta la Mecánica Cuántica (MC) para conseguir que los dispositivos funcionen correctamente, sino que la MC participa activamente en el comportamiento global. En la actualidad se está aprendiendo a captar y aprovechar las ventajas derivadas de considerar a la información como un ente cuántico, lo que abre una serie de nuevas posibilidades que darían vértigo al propio Bohr.

TEORÍA CLÁSICA DE LA COMPUTACIÓN

Cabe, quizás, situar el origen moderno de la teoría de la computación en la respuesta a un problema esbozado por David Hilbert en 1900. Hilbert planteó la necesidad de preguntarse no sobre la veracidad de ciertas proposiciones matemáticas, sino acerca de la capacidad real de las matemáticas para responder a tales cuestiones. Desplazó así el interés acerca de las soluciones dadas por las matemáticas a determinadas sentencias hacia la demostración de la posibilidad de tal cosa.

La tecnología de los ordenadores ha evolucionado siguiendo un proceso de miniaturización... parece que el próximo nivel será el molecular

Turing se enfrentó a este desafío y empezó a pensar en una posible solución "mecánica" del problema. Introdujo el concepto de Máquina de Turing (MT), dispositivo formado por un elemento de lectura/escritura y una memoria en forma de cinta con capacidad ilimitada, que permite estudiar la computación desde dos puntos de vista:

a) Posibilidad de computar ciertas funciones

Las MT realizan cálculos mecánicos que ejecutan un algoritmo o procedimiento efectivo. Podemos preguntarnos si el concepto de máquina de Turing engloba a todas las operaciones matemáticas representadas por algoritmos. La respuesta se conoce como la tesis de Church-Turing: el concepto de máquina de Turing define lo que entendemos por procedimiento algorítmico. Cualquier función que sea computable, se puede computar mediante una máquina de Turing constituida por un dispositivo físico "razonable". Se trata de una hipótesis no demostrada que ha superado todos los intentos de encontrar contraejemplos. Las MT no tienen la pretensión de llegar a ser construidas real-

mente, sino que sólo pretenden captar lo esencial del comportamiento de un ordenador.

Las MT no tienen que ser necesariamente deterministas (MTD): a un estado le sigue precisamente otro. Existe la posibilidad de que, partiendo de una configuración determinada, el siguiente estado (existen varias posibilidades) pueda alcanzarse con una cierta probabilidad. Estamos ahora ante una Máquina de Turing Probabilista (MTP).Su funcionamiento puede representarse mediante un esquema en árbol. La computación sigue una única ruta que se produce con cierta probabilidad. El resultado de estas MTP puede no ser correcto, sólo lo es con cierta probabilidad, aunque el procedimiento podría llegar a ser más efectivo que en el caso determinista. Se demuestra que todo lo que es computable mediante una MTP también lo es mediante una MTD.

Uno de los problemas de los actuales ordenadores de alta velocidad, es la eliminación del calor producido durante su funcionamiento

Desgraciadamente, la respuesta dada por las MT a la pregunta planteada por Hilbert acerca de la posible existencia de un método general que permita averiguar si una proposición es verdadera o falsa, tiene una respuesta clara: no, no existe tal método. Es imposible predecir si una determinada MT se detendrá o no, en otras palabras, si podrá o no proporcionar una solución al problema planteado (Problema de la Parada).

b) Eficiencia

El segundo aspecto interesante de las MT es que permiten estudiar la eficiencia de los algoritmos. La eficiencia se establece clasificando los algoritmos en determinadas Clases de Complejidad en función de cómo escalan los recursos de un cálculo con el tamaño de los datos. Si el tamaño de los datos se mide a través de los bits necesarios para su representación (L), los algoritmos se pueden clasificar en tratables (o de clase P), si el número de pasos temporales (p) escala como O(polinomio de L), y en no tratables (clase NP), si escalan como p ~O(exponencial de L). Esta forma de clasificación no depende de la velocidad real de los ordenadores actuales (siempre cambiante). Durante mucho tiempo se creyó que este tipo de clasificación no tenía ninguna relación con el tratamiento físico de la información, de ahí su importancia (la situación iba a cambiar con la computación cuántica).

El modelo de la máquina de Turing es una forma de describir un ordenador en abstracto. Otra forma de hacerlo es construir un circuito mediante elementos (puertas) que realicen operaciones lógicas sobre un conjunto de variables booleanas. Ambas aproximaciones son polinómicamente equivalentes. De la misma forma que existe una MT Universal (que permite simular cualquier otra), existe un conjunto de puertas que son universales. Por ejemplo, la puerta NAND por sí sola es universal. Utilizando esta puerta se puede reproducir el comportamiento de cualquier MT, con recursos polinómicos.

LIMITACIONES DEL PROCESO DE CÓMPUTO

Hacia el inicio de la década de los 60, Rolf Landauer[1] comenzó a preguntarse si las leyes físicas imponían algunas limitaciones al proceso de cómputo. En concreto se interesó sobre el origen del calor disipado por los ordenadores, y si este calor era algo inherente a las leyes de la física o se debía a la falta de eficiencia de la tecnología disponible. Este tema parece realmente interesante si recordamos que uno de los problemas de los actuales ordenadores de alta velocidad es la eliminación del calor producido durante su funcionamiento. Estas reflexiones iban a ser el germen de las actuales ideas acerca de los ordenadores cuánticos.

La pregunta era: ¿se podría idear una puerta que funcionara de forma reversible, y que por tanto no disipara energía?. La respuesta no estaba clara, ya que la lógica clásica se basaba en puertas no reversibles, es decir que no permitían obtener los bits de partida después de realizada la operación. Esto es lo que sucede, por ejemplo en la puerta NAND.

La idea de computación clásica reversible la introdujo matemáticamente Yves Lecerf en 1963 y la desarrolló Bennett en 1973 demostrando que, desde un punto de vista teórico, es posible la existencia de una máquina de Turing reversible. En la representación de circuitos se plantearon puertas clásicas reversibles como la puerta CNOT (control not). Esta puerta actúa sobre pares de bits, donde se realiza una operación NOT sobre el segundo bit sólo si el primero es "1". Es posible obtener una única puerta universal reversible tal como lo es NAND para la lógica irreversible: se trata de la puerta que introdujo Toffoli y que lleva su nombre; no es mas que una "controlled-controlled-NOT" (CCNOT).

La existencia de tales máquinas de Turing reversibles nos indica que no hay una cantidad mínima de energía que haya que poner en juego para efectuar un cómputo concreto.

COMPUTACIÓN Y FÍSICA

La teoría clásica de la computación habitualmente no hacía referencia a la física del dispositivo, y se suponía que los fundamentos de tal teoría eran independientes de la realización física de los mismos. Hubieron de pasar 20 años antes de que Deutsch, Feynman y otros pusieran de manifiesto que esta idea era falsa, mostrando la conexión entre las leyes de la física y la información, en concreto con la computación. A partir de aquí se produjo una más de tantas uniones entre ideas distintas que han aparecido en la física: computación y MC. De esta unión surgió la Computación Cuántica.

De forma general podemos decir que la computación es la creación de conjuntos de símbolos (resultados) a partir de ciertos conjuntos de símbolos iniciales (o datos). Si interpretamos los símbolos como objetos físicos, la computación correspondería a la evolución de los estados de los sistemas. Por tanto, dicha evolución es un ejemplo de computación. *Si la evolución es cuántica, tenemos la Computación Cuántica.*

MÁQUINAS DE TURING CUÁNTICAS

Ya que el sentido común deja de ser correcto cuando descendemos a los reductos cuánticos, podría suceder que el paradigma de la MT no fuera todo lo independiente de la física que se deseaba. La pregunta surgió con cierta timidez: ¿serían las MT basadas en la Mecánica Cuántica equivalentes a las clásicas?. Dado que la MC permitía nuevas formas de evolución a través de estados coherentes, la respuesta se adivinaba negativa.

La posibilidad de que una máquina de Turing cuántica pudiera hacer algo genuinamente cuántico fue planteada por Richard Feynman[2] (1982), demostrando que ninguna máquina de Turing clásica (probabilista o no) podía simular algunos comportamientos cuánticos sin incurrir en una ralentización exponencial; sin embargo una máquina de Turing cuántica sí podía hacerlo. Este comportamiento surge del hecho de que la dimensión del espacio de Hilbert accesible al sistema aumenta de forma exponencial (2n) con el número de amplitudes (n) a manejar y guardar. Feynman describió un "simulador cuántico universal" que simulaba el comportamiento de cualquier sistema físico finito. Desafortunadamente, Feynman no diseñó este simulador y su idea tuvo poco impacto.

El siguiente paso se dio en 1985, cuando David Deutsch[3] describió la primera máquina de Turing cuántica (MTC). Esta MTC podía realizar tareas que una clásica no podía. Los procesos totales del ordenador cuántico deben ser unitarios y por tanto no disipativos y usa una lógica reversible. Las MTC dieron lugar a una modificación de la hipótesis de Church-Turing, en el siguiente sentido: "existe (o puede construirse) un ordenador universal que puede programarse para simular cualquier sistema físico finito operando con unos recursos limitados".

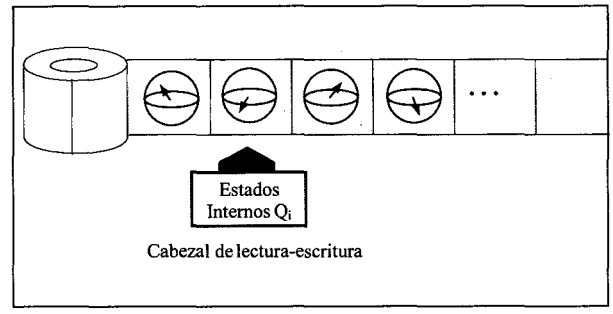


Figura 1. *Máquina de Turing Cuántica*

El funcionamiento de esta MTC es simple. Está formada por un cabezal de lectura-escritura que recorre la cinta y puede adquirir un conjunto finito de estados. Dependiendo del estado que lea en cada casilla (qubit, cuya representación aparece en la figura 1), ejecuta una instrucción (borra el qubit, lo modifica o lo deja igual) y se desplaza a una nueva casilla. Existen dos características cuánticas que proporcionan la potencia a la computación cuántica:

1.- Paralelismo:

Esta propiedad surge de la propia representación de la información cuántica. El fragmento de información clásico fundamental es el bit, entendiéndose como tal un sistema material que puede adoptar uno de los dos posibles estados distintos que representan dos valores lógicos (0 y 1 o sí y no, verdadero y falso, etc.). Sin embargo si la codificación de la información es cuántica, y se hace a través de, por ejemplo, dos estados de un sistema microscópico, ahora también es posible un estado del sistema que sea una superposición coherente de estos 0 y 1. Ello implicaría que, por ejemplo, un átomo descrito por este estado, estaría en «ambos estados a la vez». Este estado no sería ni un 0 ni un 1 clásicos. La existencia de estos estados "esquizofrénicos" nos indica que el nuevo ordenador cuántico tiene que poder tratar estos estados: generarlos y trabajar con ellos. En este sentido los ordenadores cuánticos serán algo distintos a los clásicos. De forma general, a un sistema cuántico con dos estados (Q>, lo llamaremos bit cuántico o simplemente qubit4, de forma que estará representado por el estado general:

$$|Q\rangle = a|0\rangle + b|1\rangle$$

donde 0> y 1> son los dos estados en los que puede estar el sistema y los coeficientes a y b son, en

general, números complejos, y si el qubit está normalizado se cumplirá $|a|^2+|b|^2=1$.

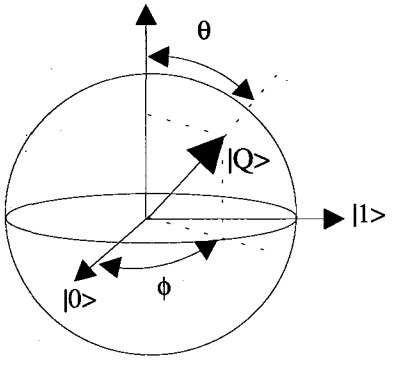


Figura 2. *Representación de un qubit* $|Q\rangle=cos(q/2)|0\rangle+e^{i}fsen(q/2)|1\rangle$

En general, es posible representar a un qubit mediante tres coordenadas polares, tal como aparece en la figura 2. Notemos que debido a que no existen restricciones acerca de los posibles valores de estos coeficientes (salvo quizás la condición de normalización del vector de estado), un solo qubit contiene, en realidad "infinita información". Esto no representa un problema conceptual, pues para extraerla, necesitaríamos medir sobre el estado, lo cual implicaría su colapso (Postulado de Proyección) en uno de los dos bits clásicos $|0\rangle$ ó $|1\rangle$, y no sería posible extraer esa infinita información del qubit. De esta medida sólo podríamos extraer un bit clásico de información, lo que causa una complicación adicional en el planteamiento de la extracción de la información en los algoritmos típicamente cuánticos.

La primera potencia de los ordenadores cuánticos radica, precisamente, en la posibilidad de usar este tipo de superposiciones coherentes de qubits para realizar los cálculos. Consideremos que queremos calcular una función de la variable x definida por:

$$f: x \in (\{0,1,....2^m-1\} \rightarrow \{0,.1,..., 2^n-1\}$$

Un ordenador clásico haría 2^m cálculos, obteniendo $f(0), f(1)...f(2^m-1)$. En un ordenador cuántico el cálculo es ligeramente distinto. Para realizar el cálculo cuántico debemos usar dos registros cuánticos: $x|x\rangle$ y el resultado $f(x)|f(x)\rangle$, y la evolución debe hacerse mediante un operador unitario Uf que actúe sobre un registro cuántico total:

$$U_f\{|x\rangle\otimes|0\rangle\} - |x\rangle\otimes|f(x)\rangle$$

Inicialmente necesitamos un registro en el estado "cero", $|0\rangle$, donde se va a colocar el resultado después de la operación.

En realidad, podemos hacer algo más que un cálculo uno a uno de los valores de f, ya que estamos usando un ordenador cuántico. Podemos preparar una superposición de todos los registros clásicos en un solo estado $|\Psi\rangle$.

$$|\Psi\rangle=\frac{1}{\sqrt{2}}[|0\rangle+|1\rangle]\otimes\Lambda\otimes\frac{1}{\sqrt{2}}[|0\rangle+|1\rangle]=\frac{1}{2^{m/2}}\sum_{x=0}^{2^m-1}|x\rangle$$

(este estado se podría conseguir preparando un estado $|0,...,0\rangle$ de longitud m y aplicando una puerta de Hadamard (H) a cada qubit, tal como definimos más adelante) y realizar *una sola operación* sobre este ket para generar todos los resultados en solo paso:

$$|f\rangle=U_f\{|\Psi\rangle\otimes|0\rangle\}=U_f\left\{\frac{1}{2^{m/2}}\sum_{x=0}^{2^m-1}|x\rangle\otimes|0\rangle\right\}=\frac{1}{2^{m/2}}\sum_{x=0}^{2^m-1}|x\rangle\otimes|f(x)\rangle$$

(hemos usado la notación de x formada por la representación decimal de las cadenas de m bits).

Ahora nos encontramos con el problema de extraer la información codificada en el ket $|f\rangle$. Si medimos sobre este ket, obtendremos cualquiera de los resultados posibles con la misma probabilidad ($1/2^m$), colapsando el estado y obteniendo un solo resultado de todos los 2m valores. Sin embargo existen otras formas más sutiles de obtener información acerca de alguna propiedad global de los valores de f(x), por ejemplo de su periodicidad, de las cuales podremos extraer más información.

2.- Interferencia:

El proceso de computación cuántica podría representarse mediante un diagrama de árbol donde todas sus ramas (a diferencia del caso clásico) se producirían a la vez y estarían caracterizadas por números complejos (amplitudes de probabilidad), cuyos cuadrados son los que nos dan la probabilidad de que al medir sobre el estado final de la MTC, obtengamos un cierto estado concreto al final de una rama. La posibilidad de usar superposiciones coherentes para la representación de la información permitiría, por ejemplo, que si una determinada configuración final de una MTC puede alcanzarse a través de dos caminos con amplitudes de probabilidad α y $-\alpha$, la probabilidad final de alcanzar dicha configuración es $|\alpha-\alpha|^2=0$. Es decir, que el resultado de la computación cuántica puede surgir de una adecuada interferencia entre los distintos caminos posibles. De esta forma se pueden codificar varios datos de un problema y tratarlos de forma simultánea y, provocando su interferencia, hacer que algunos de ellos tengan una probabilidad grande, mientras que otros desaparezcan.

PUERTAS Y CIRCUITOS CUÁNTICOS

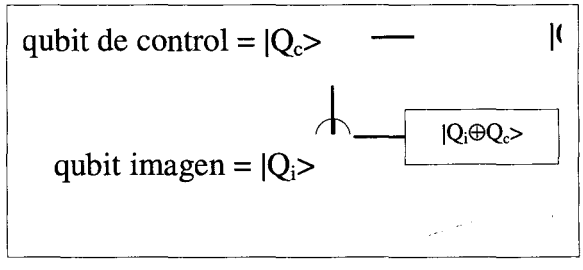
Análogamente a los ordenadores clásicos, podemos representar la evolución de los cuánticos mediante circuitos formados por puertas cuánticas que realizan las operaciones sobre los qubits. En 1989 Deutsch describió los circuitos cuánticos como formados por puertas cuánticas conectadas mediante hilos, demostrando que existía una puerta cuántica universal[5] y reversible análoga a la de Toffoli clásica. Una forma de obtener puertas cuánticas es la cuantización de las puertas clásicas, que pasa por reinterpretar los bits como qubits. El propósito de los hilos es transmitir estados cuánticos de una a otra puerta y su forma concreta dependerá de las realizaciones tecnológicas concretas de los qubits.

Una puerta típicamente cuántica es la descrita por la matriz de generación de superposiciones del tipo:

$$U_H \equiv \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Es la puerta de Hadamard, que genera una rotación o cambio de base. Una puerta de gran importancia (en realidad la de mayor importancia) en los ordenadores cuánticos es la versión cuántica de la CNOT clásica. Su representación matricial es:

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



expresada en la base de computación {|00>,|01>, |10>, |11>}. En la representación de la puerta CNOT cuántica, el primer qubit ($|Q_c\rangle$ es el de control, mientras que el segundo es el imagen ($|Q_i\rangle$. La puerta ejecuta una operación que es la suma mod 2 ((⊕) de ambos qubits. Esta puerta, junto con otras puertas que afectan a un sólo qubit, forman un conjunto universal. De ahí su importancia. Con su ayuda se puede construir un *programa cuántico*, a través de un circuito cuántico, junto con algún tipo de *puertas de medida*, todos ellos unidos mediante "cables". En este sentido podemos decir que la potencia de la computación cuántica no reside en la rapidez de aplicación de las puertas cuánticas, sino más bien en que debe de usarse un número exponencialmente menor que las necesarias en el caso clásico para realizar la misma tarea.

ALGORITMOS CUÁNTICOS

De momento no se ha demostrado que un ordenador cuántico pueda hacer cosas que uno clásico no pudiera hacer con recursos suficientemente grandes. El problema clásico puede estar encerrado en la frase "con recursos suficientemente grandes", que quizás en la realidad hagan al proceso de cálculo totalmente inviable. El problema consiste en construir algoritmos que aprovechen las características cuánticas *para cambiar la clase de complejidad* de un problema tratado clásicamente. A pesar del esfuerzo que se ha dedicado a la obtención de algoritmos que aprovechen el comportamiento cuántico, en la actualidad su número es reducido. Para programar con ordenadores cuánticos se requieren algunas técnicas nuevas. Dos técnicas básicas son: extracción de una propiedad *global* de una función y los métodos de *amplificación de las amplitudes* para aumentar la probabilidad de sucesos deseables.

Ya se ha mencionado que, aunque mediante apropiadas combinaciones lineales es posible manejar un número exponencial de estados, ello no supone que esta información esté disponible. En realidad, debido a que para acceder a esa información debemos medir sobre el estado colapsándolo, la información se pierde casi en su totalidad. Para aprovechar los aspectos cuánticos, debemos combinar la posibilidad del *paralelismo cuántico* con la *interferencia*. Tal posibilidad permite aprovechar la interferencia destructiva para cancelar los términos no deseables y, por otro lado la interferencia constructiva aumenta los términos deseables. De esta forma al medir obtendremos resultados deseables con mayor probabilidad.

A continuación indicamos algunos de los algoritmos cuánticos existentes:

· Generación de números aleatorios

La necesidad de disponer de secuencias de números aleatorios está ampliamente extendida en campos como criptografía, algoritmos aleatorios (Monte Carlo), simulaciones de evolución física de sistemas, etc. Los ordenadores clásicos sólo pueden calcular funciones, y por tanto cualquier secuencia de números resultante no es completamente aleatoria.

La MC, sin embargo, está fundamentada en leyes indeterministas. Esta indeterminación es básica, a diferencia de la imposibilidad de predicción clásica debida a una incompleta especificación de las condiciones iniciales del problema (caos determinista). Por ejemplo, partiendo de un qubit |0> y aplicando una puerta de Hadamard, obtenemos el qubit $\{|0\rangle+|1\rangle\}/2^{1/2}$. Si realizamos una medida, colapsamos el vector de estado del qubit en los estados |0> o |1> con un 50% de probabilidad cada uno. Este método podría ser ampliado (por lo menos en principio) a la generación de números aleatorios entre 0 y 2^{N-1}, sin mas que preparar una superposición de todos los estados de un sistema de N qubits. La medida del vector de estado causaría su colapso aleatorio en uno de sus términos. Trasladando de notación binaria a decimal el qubit, tendríamos el número aleatorio requerido.

· Algoritmo de Deutsch

El problema de Deutsch-Jozsa[6] fue el primer ejemplo de problema que podía resolverse exponencialmente más rápido en un ordenador cuántico que en una MT clásica. Consideremos un conjunto de funciones booleanas del tipo f: $\{0,1\} \rightarrow \{0,1\}$, en concreto hay cuatro de ellas: dos constantes f(0)=f(1)=0 y f(0)=f(1)=1 y otras dos balanceadas, f(0)=0, f(1)=1 y f(0)=1, f(1)=0. Este es el problema que surge si deseamos averiguar si una moneda es falsa (con dos caras o dos cruces) o auténtica (con una cara y una cruz). En realidad no estamos interesados en saber los valores concretos de las funciones, sino únicamente en una característica *global* de la función; averiguar si la función f es constante o balanceada. Desde un punto de vista clásico tenemos que hacer al menos *dos* cálculos de la función (necesariamente) para averiguarlo. Sin embargo, la información obtenida de si la función es constante o balanceada corresponde a un *solo bit*, luego deberíamos ser capaces de obtener el resultado en un *solo cálculo*. Esto podemos conseguirlo mediante un algoritmo cuántico.

El método sería el siguiente. Preparamos dos estados |0> y |1>, los rotamos mediante una transformación de Hadamard, realizamos el cálculo de la función mediante una puerta habitual U_f (que dado que f:{0,1}{0,1}, se trata de una f-controlled-not):

$$(|0\rangle+|1\rangle)(|0\rangle-|1\rangle) \equiv |00\rangle+|10\rangle-|01\rangle-|11\rangle \rightarrow U_f \rightarrow$$

$$U_f|x,y\rangle = |x, y \oplus f(x)\rangle$$

$$|0,0 \oplus f(0)\rangle+|1,0 \oplus f(1)\rangle-|0,1\oplus f(0)\rangle-|1,1\oplus f(1)\rangle$$

y volvemos a rotar el primer qubit:

$$|0\rangle\{|f(0)\rangle+|f(1)\rangle-|1 \oplus f(0)\rangle -|1\oplus f(1)\rangle\}+$$
$$|1\rangle\{|f(0)\rangle-|f(1)\rangle-|1 \oplus f(0)\rangle+|1\oplus f(1)\rangle\}$$

Después de esto, medimos el primer qubit, y si obtenemos |0>, la función es constante, y si obtenemos |1> la función es balanceada.

Por tanto con una sola medida hemos conseguido el objetivo. Este fue el primer algoritmo que mostró este comportamiento.

· Periodicidad de una función

Ya hemos indicado que si medimos sobre una superposición de valores como los indicados en |f>, colapsamos el estado y perdemos el resto de la información. Pero de la misma forma que sucede en un experimento de interferencia, el estado final tiene información de todos sus componentes. Este tipo de superposiciones alberga cierto tipo de información acerca de las propiedades globales del estado, como es la periodicidad de la función. El cálculo del periodo de una función es complejo, involucrando un tipo de transformación que se ha convertido en una herramienta fundamental: la Transformada Discreta de Fourier Cuántica. Esta TDFC se define como la operación unitaria y reversible UTDFC en q (0x<q) dimensiones:

$$U_{TDFC}|x\rangle = \frac{1}{q^{1/2}} \sum_{k=0}^{q-1} e^{i2\pi kx/q} |k\rangle$$

Aplicando esta TDFC en determinado momento del desarrollo del algoritmo, se consigue un proceso de interferencia que da lugar a que ciertos términos indeseables de la superposición coherente desaparezcan, mientras que otros deseables se potencien.

· Algoritmo de Shor

Sabemos que mientras el algoritmo de multiplicación es muy rápido, el mejor algoritmo inverso, es decir la factorización, es muy lento. En realidad, clásicamente este último está dentro de la clase de complejidad NP de algoritmos no tratables. El número más grande que se ha factorizado hasta hoy tiene 129 cifras y para hallar sus factores fue necesario el concurso de unos 1600 ordenadores en todo el mundo trabajando sin parar durante unos 8 meses. El crecimiento de los recursos necesarios para la factorización es exponencial, sin embargo, la cantidad de términos que podíamos mantener en una superposición cuántica es también exponencial. Esta es la razón de que algunos algoritmos cuánticos puedan transformar problemas de tipo NP (como la factorización clásica) en P, es decir, tratables o polinómicos.

En 1994 Peter Shor[7] puso a punto el primer algoritmo de interés práctico, ya que logró plantear un

algoritmo eficaz para la factorización, usando los recursos de un ordenador cuántico. La importancia de esta posibilidad radica en que la dificultad de la factorización está en la base de los códigos criptográficos (mediante un ordenador cuántico, romper la clave RSA 140 sería cuestión de segundos) usados ampliamente por ejemplo en transacciones bancarias o en secretos militares. Romper estos códigos significaría acceder a una gran cantidad de información, al mismo tiempo que destrozar estas claves.

El algoritmo se basa en encontrar el periodo de cierto tipo de funciones relacionadas con el número a factorizar. Desgraciadamente, desde un punto de vista clásico no hay un algoritmo que lo calcule de forma eficiente. Para calcular el periodo se usa el algoritmo cuántico indicado anteriormente. De esta forma, el algoritmo de Shor, es un híbrido entre el cálculo cuántico del periodo de una función y el uso de algoritmos clásicos (en concreto para calcular el m.c.d.) eficientes. Este algoritmo usa $O((\log N)^3)$ pasos[8], lo que demuestra *cómo este algoritmo cuántico es capaz de cambiar la clase de complejidad clásica de la factorización de NP a P.* A pesar de todo nadie ha demostrado todavía que no exista un algoritmo clásico para la factorización que calcule con eficiencia polinómica.

Hughes ha analizado las previsiones de factorización de números, comparando los resultados de un conjunto de 1000 estaciones de trabajo con los de un ordenador cuántico.

Número de bits	1024	2048	4096
año 2006	10^5 años	$5\ 10^{15}$ años	$3\ 10^{29}$ años
año 2024	38 años	10^{12} años	$7\ 10^{25}$ años
año 2042	3 días	$3\ 10^8$ años	$2\ 10^{22}$ años
En un ordenador cuántico			
número de qubits	5124	10244	20484
número de puertas	$3\ 10^9$	$2\ 10^{11}$	$2\ 10^{12}$
tiempo	4.5 minutos	36 minutos	4.8 horas

Este análisis evidencia la potencia de cálculo de un ordenador cuántico.

· Algoritmos de búsqueda

Un tipo interesante de problemas son los de búsqueda. El algoritmo de Grover trata este problema. Para ello usa un algoritmo cuántico que aprovecha la posibilidad de superposición coherente[9]. Por ejemplo, consideremos que tenemos una lista con N datos (que puede ser una lista de 106 nombres de un listín telefónico, ordenado por orden alfabético), nos planteamos encontrar un elemento concreto (es decir, dado un teléfono, encontrar su dueño). Clásicamente para encontrar un dato concreto con una probabilidad 1/2, deberíamos buscar, en promedio, unos N/2 (5.105 búsquedas) elementos hasta dar con el buscado, por tanto el algoritmo escala como N=2L, y por tanto no es tratable. El algoritmo de Grover[10] demuestra que para una búsqueda en una base de datos sin estructura, se necesitan sólo $O(N^{1/2})$ pasos temporales (con una probabilidad acotada), con lo que sigue siendo no tratable (no se cambia la clase de complejidad), sin embargo se aumenta su eficiencia, lo que es importante cuando se trata una gran cantidad de datos. En el caso del listín se necesitarían sólo ¡1000! búsquedas.

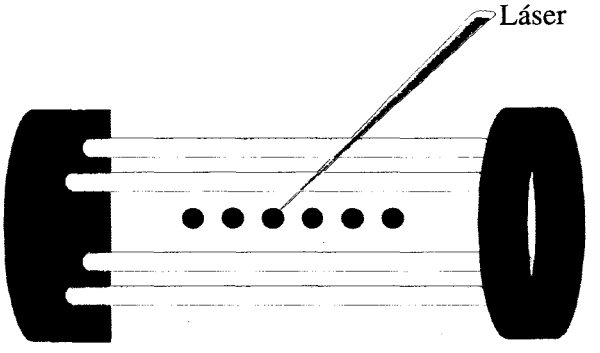
Ciertos problemas se pueden plantear como problemas de búsqueda. Por ejemplo el problema de ordenar un conjunto de números por orden creciente, búsqueda de extremos, etc. Brassard ha apuntado una posible aplicación en criptografía donde se usan claves de 56 bits. La búsqueda de la clave correcta entre las 2^{56} (~7.1016) posibles tardaría más de 2000 años si se realizara clásicamente (a una velocidad de 10^6 búsquedas por segundo), mientras que mediante el algoritmo de Grover tardaría menos de cinco minutos.

PROCESOS DE CONTROL DE ERRORES

Quizás uno de mayores problemas a la hora de construir un ordenador cuántico es el control de los posibles errores, errores que provienen de la inexorable interacción del ordenador con el entorno, proceso denominado *decoherencia.* Desde un punto de vista clásico, los errores se corrigen mediante procesos que implican cierta disipación, siendo estos métodos inviables en el caso cuántico, ya que esta disipación implicaría una pérdida irremediable de coherencia. Este hecho, unido a que además de los errores de bit clásicos, también aparecen *nuevos errores*, típicamente cuánticos, como los relacionados con la variación de las fases relativas en las superposiciones coherentes, hizo que durante algún tiempo se pensara que no podían existir métodos para el control de errores cuánticos.

...la tecnología actual que implementa puertas y circuitos cuánticos está sólo en su infancia

Afortunadamente, dos recientes contribuciones (ahora ya clásicas) debidas a Shor y a Steane[11], han cambiado este panorama. Estos autores han mostrado cómo es posible contener los errores mediante códigos cuánticos correctores de errores. Tales códigos detectan y corrigen los errores usando sofisticadas técnicas cuánticas que involucran un tercer estado de apoyo, hacia donde se copia la información sólo del error.



Iones confinados en una trampa de Paul lineal.
Se perfila como el elemento básico de los futuros ordenadores cuánticos

Midiendo este estado de apoyo, podemos saber el error *sin colapsar el estado*. Aplicando ahora la transformación inversa al error, al estado con error, logramos su corrección.

HARDWARE CUÁNTICO

Debido al problema de la creación, control y corrección de errores en las superposiciones coherentes de estados cuánticos, la tecnología actual que implementa puertas y circuitos cuánticos está sólo en su infancia. Aunque se han construido puertas CNOT de dos qubits experimentales, y se han usado algunas técnicas simples de corrección de errores, no se espera que antes de unos 30 años existan ordenadores cuánticos que hagan tareas de cierta importancia.

El progreso en el control y manipulación de los qubits intenta usar todo tipo de técnicas y sistemas: fotones en cavidades, espines controlados por RMN, electrones en puntos cuánticos, etc. Quizás una de las tecnologías más prometedores consiste en confinar iones ultrafríos en trampas de Paul lineales. Las operaciones de control de los qubits se realiza dirigiendo haces láser a cada uno de los iones. Mediante un procedimiento similar se ha implementado la primera puerta CNOT cuántica.

CONCLUSIÓN

Estamos ante otra de esas revoluciones interdisciplinares que producen gran cantidad de nuevas relaciones entre campos inicialmente sin conexión. La revolución cuántica está alcanzando también a la información, no sólo en sus métodos de procesado, sino en su propia concepción. La posibilidad de construir ordenadores cuánticos permitirá procesos relacionados con el tratamiento de la información, hasta ahora insospechados, además de poner de manifiesto ciertos comportamientos cuánticos fundamentales, hasta ahora sólo plasmados en los libros de texto. Quizás sea un buen momento de participar en el este desarrollo.

[1] Bennett, C. H. & Landauer, R; «The fundamental physical limits of computation», Scientific American 1985, July 38.

[2] Feynman, R.; «Quantum mechanical computers», Found. Phys. 16 507 (1986).

[3] Deutsch, D.; «Quantum theory, the Church-Turing principle and the universal quantum computer», Proc. R. Soc. London, A400 97 (1985).

[4] Schumacher, B; «Quantum coding», Phys. Rev. A 51 2738, (1995)

[5] D. Deutsch, «Quantum computational networks», Proc. R. Soc. London A 425, 73 (1989).

[6] Deutsch,D. & Jozsa, R; «Rapid Solutions of problems by quantum computation», Proc. of the Roc. Soc., A439 553 (1992).

[7] Shor, P.W.; Proceedings of the 35th Annual Symposium on Foundations of Computer Science (IEEE Computer Society, Los Alamitos CA 1994) p124. Shor, P.; «Polynomial-time algorithms for prime factorisation and discrete logarithms on a quantum computer», Proc. 35th Annual Symp. on Foundations of Computer Science, Santa Fe, IEEE Computer Society Press.

[8] Beckman D.; Chari A.; Devabhaktuni S. & Preskill J.; «Efficient networks for quantum factoring», Phys. Rev. A 54 1034 (1996).

[9] Grover, L.K.; «The advantages of superposition», Science 280 228, abril 1998. 10 Grover L.K., «A fast quantum mechanical algorithm for database search», Proceedings of the 28th Annual ACM Symposium on Theory of Computing , p212, Philadelphia 1996. 11 Steane, AM; «Multiple particle interference and quantum error correction», Proc. Roy. Soc. Lond. A 452 2551 (1996).