COMPUTACIÓN CUÁNTICA Y SU REALIZACIÓN FÍSICA

Ángel Prieto de la Cruz

31 de diciembre de 2015

Resumen

En el siguiente artículo veremos como la computación cuántica nace de la mano de algunas teorías cuánticas como el entrelazamiento, mientras que el mayor hándicap para su realización física lo explica la decoherencia. Definiremos la unidad mínima de información cuántica, el qubit, y su aplicación a la criptografía. Finalmente veremos algunas propuestas para la creación de hardware y estudiaremos la potencia real de un posible ordenador cuántico.

Orígenes

Las últimas décadas han estado caracterizadas por un gran avance en la computación clásica. El aumento de la velocidad de procesamiento ha ido de la mano de una miniaturización de los componentes electrónicos que los integran. Ya en 1965, el cofundador de Intel, Gordon Moore, enunció una ley empírica que lleva su nombre, la cual expresa que aproximadamente cada dos años se duplica el número de transistores en un microprocesador. Esta ley se ha cumplido en muy buena aproximación hasta la fecha, pero presenta una evidente limitación: cuando los tamaños de los transistores se acerquen a las escalas atómicas, dejarán de ser divisibles y aparecerán fenómenos cuánticos. Esto no solo abre un nuevo campo de investigación en el diseño de hardware, sino que los principios cuánticos parecen ser el germen de una nueva revolución computacional. Los primeros físicos teóricos que repararon en este hecho fueron Richard Feynmann, Paul Benioff, David Deutsch y Charles Bennett sobre las décadas de 1970 y 1980.

Entrelazamiento Cuántico

En 1935, los físicos Albert Einstein, Boris Podolsky y Nathan Rosen propusieron el siguiente experimento mental: Tenemos dos partículas que interactuaron en el pasado y que quedan en un estado entrelazado. Dos observadores reciben cada una de las partículas. Si un observador mide la inercia de una de ellas, sabe cuál es la inercia de la otra. Si mide la posición, gracias al entrelazamiento y al principio de incer-

tidumbre, puede saber la posición de la otra partícula de forma instantánea. Este experimento es conocido como la Paradoja EPR, por las siglas de sus formuladores, y fue propuesta como argumento para derrumbar la mecánica cuántica debido a que aparentaba violar la Teoría de la Relatividad por el intercambio instantáneo de información. Lo que no intuyeron estos grandes científicos es que el fenómeno conocido como Entrelazamiento Cuántico no hizo más que reforzar la mecánica cuántica y darle un sinfín de aplicaciones, entre las que se encuentra la Computación o la Criptografía cuántica.

El entrelazamiento cuántico no tiene un equivalente en la física clásica, pues dice que los estados cuánticos de dos o más objetos (microscópicos) se deben describir mediante un estado único que involucra a todos los objetos del sistema, aun cuando estos estén separados espacialmente, de forma que haya una correlación entre las propiedades físicas observables. El ejemplo más práctico donde observar entrelazamiento son los fotones. Podemos crear fotones entrelazados de la siguiente manera: Mandamos un rayo láser ultravioleta sobre un cristal óptico no lineal, de forma que se originan haces de luz con nuevas frecuencias. La suma de estas frecuencias ha de ser igual a la frecuencia del láser incidente. Estos fotones están entrelazados, es decir, son la superposición de dos estados de dos partículas que no se pueden expresar como el producto de estados respectivos de una partícula.

La pregunta que surge a continuación es, ¿cómo podemos utilizar el entrelazamiento cuántico para crear computadores?

Del Bit al Qubit

El Bit (acrónimo de Binary Digit) es un dígito del sistema de numeración binario. Se trata de la unidad mínima de información empleada en informática y en las comunicaciones digitales. Con un bit podemos representar solamente dos valores (0,1). Por tanto, con n bits tendremos un total de 2^n valores distintos, representados con una secuencia lineal de 0s y 1s alternados. Podemos simplificar el hardware clásico como un conjunto de pequeños dispositivos que pueden tener dos estados: encendido y apagado; y cuya configuración nos da información sobre un objeto. Si por ejemplo con los bits hacemos referencia a la noción de colores, tendríamos que una imagen de 1 bit solo puede tener dos colores (blanco y negro), mientras que una imagen de 8 bits tendría un total de $2^8 = 256$ colores. No obstante, los límites de la computación clásica están muy ligados a este concepto, pues para n grandes hay que procesar mucha información mirando uno por uno cada estado de forma lineal. Para dar el salto a la computación cuántica tuvo que definirse una generalización de este concepto: el llamado Quantum Bit o Qubit. El término qubit se atribuye a un artículo de Benjamin Schumacher que describía una forma de comprimir la información en un estado y de almacenar la información en el número más pequeño de estados. En analogía con el bit, el qubit es la unidad mínima de información cuántica. La diferencia fundamental entre ambos es que, si bien el bit puede tomar un valor de 0 o 1, el qubit puede tomar estos dos valores o una superposición cuántica entre ambos. Representaremos los estados de un qubit con la notación $|0\rangle$ y $|1\rangle$. Gracias a este para-

lelismo cuántico, los algoritmos cuánticos que operan sobre estados de superposición realizan simultáneamente las operaciones sobre todas las combinaciones de las entradas.

¿Qué relación hay entre el entrelazamiento cuántico y los qubits? Si entrelazamos dos qubits, el sistema no puede descomponerse en factores independientes para cada uno de los qubits. Por ejemplo, consideremos el entrelazamiento más sencillo (normalizado) $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Supongamos que uno de estos dos qubits entrelazados se entrega a Alicia y el otro a Bob. Alicia hace la medida de su qubit, y supongamos que obtiene el valor 0. Debido al entrelazamiento de los qubits, si Bob hace ahora su medida, conseguirá el mismo valor que Alicia, es decir, debe obtener 0. Esto es porque no existe el término $|01\rangle$. De la misma forma, si Alicia hace su medida y obtiene el valor 1, y Bob la hace después, deberá obtener obligatoriamente 1. De esta forma, el resultado que obtiene Bob está condicionado por el que obtenga Alicia, aunque estén separados por años luz de distancia.

Una de las principales aplicaciones de los qubits es la criptografía cuántica, que nos permite enviar información de forma totalmente segura utilizando canales públicos.

Criptografía Cuántica

La implementación de un ordenador cuántico hace temblar los cimientos de la actual criptografía, cuya seguridad está basada en que los tiempos de desencriptado crecen exponencialmente. Sin embargo, de la mano trae un nuevo método de encriptación basado únicamente en la física cuántica y que promete ser completamente infalible.

Uno de los protocolos más conocidos es el llamado BB84, propuesto por Charles Bennet y Gilles Brassard en 1984. En este protocolo, la trasmisión se logra utilizando fotones polarizados por un canal cuántico, mientras que por un canal público se envían información para la construcción de la clave compartida. Una de las propiedades más importantes es que si un tercero intenta hacerse con la clave, el proceso se altera advirtiendo al intruso gracias al principio de incertidumbre de Heisenberg. Veamos en 5 pasos como dos interlocutores, Alicia y Bob, pueden enviarse información sin que un intruso la decodifique.

Primer paso: Alicia utiliza el canal cuántico para enviar a Bob una secuencia de fotones polarizados utilizando aleatoriamente bases rectilineas (+) y diagonales (×).

Segundo paso: Bob desconoce la secuencia de bases utilizada por Alicia, por lo que mide la polarización de los fotones utilizando una base aleatoria generada por él.

Tercer paso: Alicia y Bob se contactan por un canal público para comunicarse las bases utilizadas, y ambos descartan las mediciones donde las bases no coinciden.

Cuarto paso: Debido a las posibles impurezas en el canal o a la presencia de intrusos, Alicia y Bob se revelan segmentos de la clave generada para abortar la comunicación en caso de que dichos segmentos no coincidan (lo que querría decir que un intruso ha modificado la clave al intentar medirla).

Quinto paso: Como la clave de cifrado se ha transmitido de forma segura, pueden mandarse el mensaje con un

algoritmo de cifrado utilizando cualquier canal.

Hemos visto la aplicación de los qubits para el envío de información. Sin embargo, si queremos construir qubits como hardware para un computador nos aparece un problema asociado al fenómeno físico de la decoherencia cuántica.

Decoherencia Cuántica

La decoherencia cuántica explica como un estado cuántico entrelazado puede dar lugar a un estado físico clásico y no entrelazado. En el famoso ejemplo del gato de Schrödinger, donde teóricamente el gato puede estar en los estados vivo y muerto simultáneamente, la interacción con las partículas del ambiente producirían una decoherencia en un lapso de tiempo del orden de $\hbar^2 \approx 10^{-65}\ s$, haciendo que el gato manifieste su estado a un observador. La decoherencia es la responsable de explicar por qué los sistemas macroscópicos no presentan las exóticas propiedades de la física cuántica. El nombre procede del hecho de que la decoherencia se manifiesta matemáticamente por la pérdida de coherencia de la fase compleja relativa de las combinaciones lineales que definen el estado.

El principal reto para la realización física de la computadora cuántica pasa por dilatar el tiempo en el que el sistema cuántico sea coherente.

Propuestas de QC

Para mitigar el fenómeno de la decoherencia en la creación de ordenadores cuánticos (QC, por sus siglas en inglés) hacen falta presiones muy bajas para reducir la interacción con las moléculas colindantes, así como temperaturas muy bajas para evitar la interacción con los fotones térmicos.

Se han propuesto diversas formas de crear qubits para ordenadores cuánticos: Trampas de iones, moléculas absorbidas, resonancia magnética nuclear, etc... por desgracia ninguna se ha impuesto como la definitiva debido a que en todas el tiempo de coherencia es insuficiente. Mostraremos brevemente un par de propuestas de varios investigadores, entre los que destaca Javier Tejada, basadas en partículas magnéticas a escala nanométrica de spin S y alta anisotropía molecular.

(1) Los valores $|0\rangle$ y $|1\rangle$ se corresponden con los estados fundamental y primero de spin excitados $S_z = S$ y S_{-1} separados por una brecha energética dada por la frecuencia de la resonancia ferromagnética.

(2) Los estados del qubit $|0\rangle$ y $|1\rangle$ corresponden a las combinaciones simétricas y antisimétricas del doble estado fundamental degenerado $S_z = \pm S$, debido al significante efecto túnel entre la barrera anisótropa.

En cada caso la temperatura de operación debe ser menor que la de la brecha energética Δ entre los estados $|0\rangle$ y $|1\rangle$. La brecha energética Δ para el caso (2) puede ser controlada mediante un campo magnético externo perpendicular al eje principal de la molécula. Los estados de las diferentes moléculas y partículas magnéticas se entrelazan conectándolos mediante líneas superconductoras.

Potencia del QC

En teoría de complejidad computacional, los problemas **P** son todos aque-

llos problemas de decisión que pueden ser resueltos en una máquina determinista secuencial en un tiempo polinómico, mientras que los problemas **NP** (nondeterministic polynomial time) son aquellos cuya solución, aunque no pueda encontrarse, se puede verificar en tiempo polinómico. Una de las cuestiones más importantes en complejidad computacional es si $P = NP$.

A día de hoy, las computadoras clásicas solo pueden resolver problemas de tipo P, y es un error común pensar que las futuras computadoras cuánticas serán capaces de resolver problemas NP. Si tal proeza fuese posible , podríamos ordenarle a nuestra computadora, entre otras cosas, que buscase posible regularidades en las fluctuaciones de los mercados de valores, en las series de datos meteorológicos o incluso en la actividad cerebral.

¿Entonces qué clases de problemas puede resolver un QC? Se define como la clase **BQP** (bounded error quantum polynomial time) la que contiene aquellos problemas que pueden se resueltos mediante un algoritmo cuántico cuya cota superior en tiempo es polinómica, tal que la probabilidad de obtener una respuesta equívoca es inferior al 25 %. Como ya habíamos dicho, $P \subset BQP$ pero $BQP \subsetneq NP$, es decir, que puede resolver los mismos problemas que un computador clásico (de forma más rápida y eficiente) y solo algunos problemas muy concretos de la clase NP, como son la descomposición de un número (arbitrariamente grande) en factores primos o el conocido como el problema del logaritmo discreto, ambos muy estrechamente relacionados con la criptografía actual.

Podemos concluir que, si bien la investigación actual sobre computación cuántica avanza a pasos agigantados, todavía parece que estamos muy lejos de tener un prototipo de computador cuántico funcional . Y aunque consiguiesemos salvar todas las dificultades referentes a la decoherencia, seguiríamos teniendo el problema de que opera a muy bajas presiones y temperaturas, lo cual solo puede conseguirse en un laboratorio. Es seguro que en las próximas décadas ya tendremos algunos prototipos básicos que puedan realizar pequeños cálculos de forma muy eficiente, pero de momento es una quimera pensar que tal prototipo pueda llegar a los hogares.

Referencias

[1] Anton Zeilinger, *La Realidad de los Cuantos*, INVESTIGACIÓN Y CIENCIA, junio 2009.

[2] Neil Gershenfeld y Isaac L. Chuang, *Quantum Computing with Molecules*, SCIENTIFIC AMERICAN, june 1998.

[3] Scott Aaronson, *Los límites de la Computación Cuántica*, INVESTIGACIÓN Y CIENCIA, mayo 2008.

[4] J. Tejada, M. Chudnovskyt, J. M. Hernández y T. P. Spiller *Magnetic Qubits as hardware for Quantum Computers*, 2000.