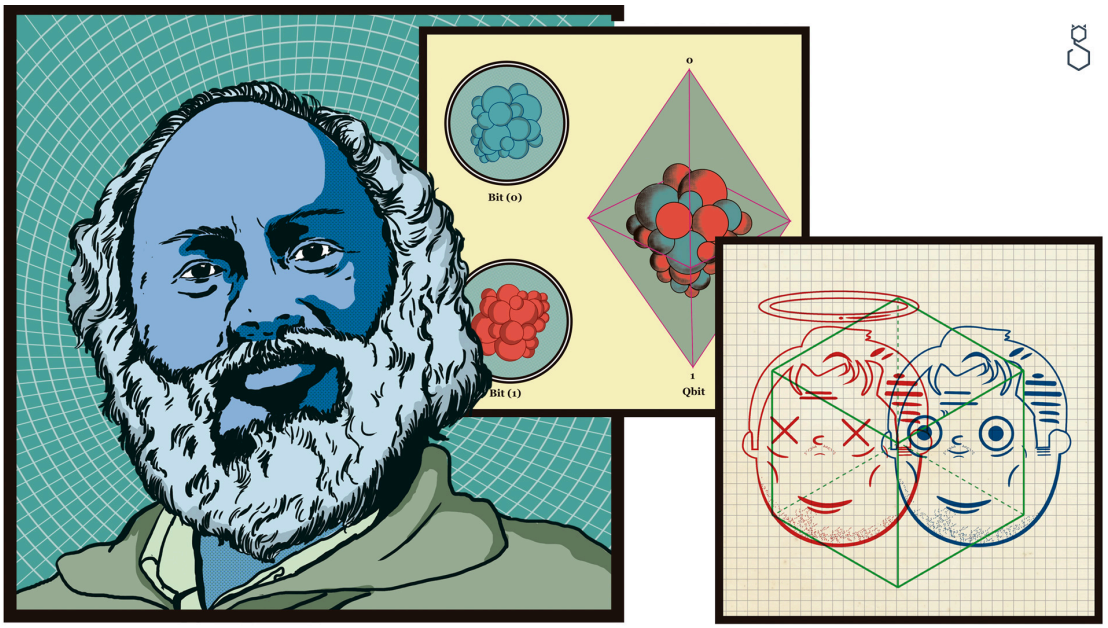

25/07/2016

Poder cuántico

TXT MARCOS FEOLE IMG ÁNGEL BIELA

¿Qué es la computación cuántica? ¿Podemos destruir cada forma de encriptación conocida por el hombre?

Curar el cáncer y detectar una fusión de agujeros negros a miles de millones de años luz es complicado e importante sí, pero a veces olvidamos que esos no son los únicos intereses humanos que podemos abordar desde la ciencia. Además de descubrir partes impensadas del Universo, a veces damos un pasito más, y decidimos inventarlas. En ese filo entre descubrir e inventar está el paso de lo científico a lo tecnológico, y es ahí que a la ciencia también le compete cuando se le tilda la computadora, o cuando una transacción segura por internet funciona.

Justo en este filo que implica convertir algo que descubrimos en algo que inventamos se encuentra hoy la computación, que trata de metabolizar una de las

discusiones más apasionadas del siglo pasado: **¿qué hacemos cuando las leyes de la física como las conocemos no funcionan más, porque nos acercamos el reino de lo cuántico?**

Ajusten sus cinturones y pongan sus asientos en posición vertical, estamos por hablar de computación cuántica.

Una **computadora clásica**, para funcionar, transporta y manipula **bits (cosas que están en uno de dos estados: o cero o uno)**. Un bit es, por ejemplo, la cantidad de información que te da alguien que te responde una 'pregunta de sí o no' como '¿Te lavaste los dientes?', o '¿Querés ser mi novia?' (Escribí toda la nota para meter esto en el medio, Lore. Pensalo)

En una computadora cuántica, en cambio, se quieren aprovechar **ciertas leyes que gobiernan el comportamiento de partículas elementales, átomos, y moléculas**. Las leyes (clásicas) que vemos día a día a nuestras escalas son bastante diferentes al comportamiento (cuántico) de las cosas en tamaños más chicos. Entonces, si vivieras en el mundo atómico te pasaría algo como esto:

1. En cuántica, las partículas o átomos pueden estar en muchos lugares (o en muchos estados) diferentes al mismo tiempo. De ahí el gato ese del experimento imaginario, que puede estar vivo Y muerto. Esto se llama **principio de superposición**, y es importante porque permite armar elementos que pueden estar en el estado **uno y cero al mismo tiempo** (los **qubits**, que son las unidades de información cuántica).

2. Bien, ya tenemos un gato que puede estar vivo y muerto, pero está dentro de una caja y nada ni nadie chequeó su estado. Y ese es el secreto. Al abrir la caja y observar al felino zombie, la superposición se pierde, dando lugar a uno sólo de sus resultados posibles (o vivo, o muerto, nada de ambigüedades). Es decir, **la medición no revela el estado anterior del sistema (superpuesto), sino que lo cambia.** Este es el **problema de la medición**. Lo único que puede hacer un físico antes de medir es calcular la probabilidad de que resulte en una cosa u otra (bah, un *muggle* también puede hacer el cálculo). A lo que ocurre cuando uno mide se le dice, en la jerga científica, colapso de la función

de onda, o **'no sé lo que está pasando pero los experimentos dan bien'.**

3. Otro efecto todavía más loco, puesto en evidencia por Einstein y compañía para mostrar que la jodita de la cuántica mucho no les copaba, es el **entrelazamiento cuántico**. Y no, no es un arrebato romántico de Alberto. **Que un par de partículas estén entrelazadas quiere decir que midiendo una de ellas se puede conocer (y colapsar) el estado de la otra a una distancia arbitrariamente larga.** Este efecto permite lograr otra locura, que es la **teleportación cuántica**, cuyo récord actualmente es la transmisión de un estado cuántico a través de 143 kilómetros. Este experimento se hizo entre dos de las Islas Canarias, La Palma y Tenerife, demostrando también hasta dónde puede llegar un físico con ganas de tomarse unas buenas vacaciones pagas.

Raro. Antiintuitivo. Cuántico. Sexy. Atrevido.

Ahora, volviendo un rato a nuestra escala, podríamos decir mucho sobre cómo empezó esto de estudiar las computadoras cuánticas, pero por una cuestión subjetivamente cholula sólo voy a nombrar una charla de Richard Feynman (TE AMO, RICHARD) de 1959, titulada 'Hay un montón de lugar al fondo'. En esa charla, Dick no sólo propone miniaturizar la computadora y utilizar las propiedades cuánticas de los átomos, sino que además establece los orígenes de la nanotecnología.

Pero fue recién en 1994 cuando la cosa realmente despegó. Ese año Peter Shor describió el **primer algoritmo cuántico de factorización en números primos** que da un resultado en tiempos razonables (no como los algoritmos clásicos que tardarían millones de años). Esto es importante porque la seguridad de diversos sistemas informáticos depende de que este problema siga siendo difícil de resolver. Básicamente estoy diciendo que con una buena e hipotética computadora cuántica se podrían hackear hasta las cuentas bancarias en Panamá, lo que nos daría una pila de datos que después no usaríamos para nada ;). Pero no desesperéis, clase política,

que hasta el día de hoy la gente que más grande la tiene, la tiene de 14 qubits, y se necesita una computadora cuántica de miles de qubits para factorizar más rápido que una computadora clásica.

Hasta acá todo muy teórico y muy lindo, pero ¿cómo se hace una computadora cuántica y por qué todavía no tenemos una?

Hay dos cuestiones, y la primera son los **errores de cómputo**. Las computadoras clásicas, en general, no cometen errores (los programas sí, pero no el hardware, que es lo que puedo romper tirándolo al piso por culpa de un error de programación). En cambio, los errores que comete el hardware de una computadora cuántica juegan un papel fundamental. El tema es que es muy difícil mantener unos cuantos qubits en un estado cuántico específico sin que venga alguien de afuera y los perturbe sin mi consentimiento. **Digo, son átomos. Andá vos a mantener un átomo quieto sin que lo jodan.** Lo bueno es que hay un teorema bastante copado que dice que si a estos átomos se les rompe las bolas sólo hasta un cierto punto, entonces se pueden agregar más qubits (y hacer más cuentas) y la compu va a andar bien igual. Lo que nos lleva al segundo problema: agregar más qubits.

Así como las computadoras clásicas pasaron a ser desde cosas mecánicas con palancas, hasta lo que son hoy después del invento del transistor y del circuito integrado, las compus cuánticas también están buscando ese pedazo de hardware que las haría realidad. Se están intentando métodos muy locos, pero la cuestión es que todavía no existe ese tan ansiado circuito integrado cuántico, y el problema es de estabilidad y escalabilidad (pasar de tener pocos qubits a tener muchos). Esto es difícil de lograr por la **decoherencia, que es la razón por la que los objetos grandes que vemos todos los días no tienen las propiedades cuánticas re locas** que mencioné más arriba**.** La decoherencia se puede pensar como la pérdida de la información cuántica de un sistema por su interacción con el ambiente, y es la responsable de que ahora entendamos por qué el experimento mental de Schrödinger, el del gato y la caja, no se puede hacer en realidad. **El estado loco del gatuno vivo y muerto sería extremadamente inestable**, y decaería muy rápido a uno de sus dos estados clásicos posibles: vivo o muerto. En todos los sistemas 'grandes' la información cuántica se pierde rápidamente, transformando nuestra

computadora cuántica en una clásica, y quitándonos así la posibilidad de hacer *la gran Steve Jobs* y armarnos una en el garage para salir a venderla (por más Wozniak que tengamos bajo la manga).

Varias empresas (y un continente) están tratando de desarrollar computadoras cuánticas (como IBM, Microsoft o Google). Una empresa canadiense en particular, D-Wave Systems, dice haber fabricado una de 28 qubits en 2007, 128 qubits en 2008, y actualmente una de más de 1000. Pero quizás es chamuyo ya que todavía nadie pudo comprobar si los chips de D-Wave realmente manipulan información cuántica para resolver los algoritmos. Igual Google y la NASA los están testeando desde 2013, hasta ahora con buenos resultados en comparación con los mismos algoritmos pero clásicos.

Y para mostrar que esto no es joda, en 2013 Edward Snowden se retobó y develó un par de documentos clasificados de la NSA (la Agencia de Seguridad Nacional de EEUU, para la cual trabajaba), sacando a la luz algunos proyectos espías secretos. Uno de ellos es el ***Penetrating Hard Targets*** **(Penetrando Objetivos Difíciles),** un proyecto que no es simplemente un nombre extremadamente feliz para estrategias de seducción, sino que consiste en el desarrollo de una computadora cuántica con intenciones, digamos, poco felices para con la privacidad de las personas y los Estados. Del lado de los buenos, un chiche como estos se podría usar por ejemplo para reducir sarpadamente los tiempos que consumen ciertos algoritmos clásicos, o simular propiedades cuánticas de moléculas para el diseño de nuevos y mejores materiales, medicamentos o paneles solares. El tema central es que toda esta jodita de resolver ciertos problemas y entender el Universo podría acelerarse a niveles no imaginados.

La cuestión es que se está tratando de cruzar otra frontera del conocimiento. Los científicos se están metiendo en regiones nunca antes exploradas (en el terreno negro del Age of Empires), y no se sabe con qué se van a encontrar. La pregunta de *¿cuándo vamos a tener una computadora cuántica?* es del campo de la futurología y los expertos tienen diversas opiniones al respecto (desde el *pronto* hasta el *nunca*). Lo lindo de la ciencia es que es una herramienta que nos permite construir a partir de lo que ya se hizo (parándonos sobre hombros de gigantes), y que, si llegamos a

darnos cuenta de que **nunca** vamos a tener una computadora cuántica, también vamos a saber **por qué**, y vamos a haber aprendido algo nuevo sobre el Universo en el que vivimos. Quizás hasta una teoría nueva y mejor que la cuántica para explicar lo microscópico, quién sabe. Mientras tanto, sigamos empujando el borde del conocimiento. Y que la fuerza (y, sobre todo, el financiamiento) nos acompañen.

Referencias

Computación cuántica desde Demócrito, Scott Aaronson

Teoría cuántica, David Bohm

¿Puede ser considerada *completa* la descripción cuántica de la realidad física? – Einst ein, Podolsky, Rosen

Teoría cuántica, el principio de Church-Turing y la computadora cuántica universal, David Deutsch

Algoritmos para computación cuántica, Peter W. Shor

Decoherencia y la transición cuántica a clásica, Wojciech H. Zurek

Esquema para reducir decoherencia en memorias cuánticas, Peter W. Shor

Entrelazamiento de 14 qubits: creación y coherencia, Monz et. al.

elgatoylacaja.com/poder-cuantico

Sumate en
eglc.ar/bancar