Discurso de aceptación
21 de septiembre de 2021

Peter Shor, galardonado en la categoría de Ciencias Básicas (XII edición)

Me complace mucho y es un gran honor para mí recibir el premio Fronteras del Conocimiento de la Fundación BBVA. Es un placer hallarme en compañía de tan distinguidos talentos, no solo en la ciencia y las matemáticas, sino también en campos como la música y la ingeniería. Permítanme dar las gracias a la Fundación BBVA por haber creado este premio y al comité de selección por haberme elegido.

Permítanme también agradecer al comité de selección que haya elegido a mis compañeros de galardón. Me complace especialmente compartir este premio con mis colegas y amigos Charlie Bennett y Gilles Brassard; los admiro mucho, conozco a ambos desde hace mucho tiempo. De hecho, mi primera introducción al campo de la información cuántica fue una conferencia que Charlie Bennett impartió en Bell Labs en los años 80.

Me gustaría decir unas palabras sobre la historia de la computación cuántica, pero primero quiero hablar un poco de la historia de la mecánica cuántica. La teoría de la mecánica cuántica se desarrolló en los primeros años del siglo XX y, alrededor de 1925, comenzó a tomar la forma de una teoría coherente. Estaba claro que iba a ser más que extraña, y debido a esa extrañeza, Albert Einstein no pensó que la teoría pudiera ser completa tal y como era, sino que habría que añadirle más cosas para que tuviera sentido. Esto llevó a un largo debate entre Niels Bohr y Einstein, en el que Bohr sostenía que la mecánica cuántica era una teoría satisfactoria tal y como era y Einstein sostenía que, tal como estaba formulada entonces, no podía ser una representación de un mundo real. Al final resultó que Bohr tenía razón; en 1964, Bell demostró que era imposible completar la teoría de ningún modo que Einstein hubiera considerado satisfactorio.

No obstante, mientras se desarrollaban estos debates sobre cómo explicar la extrañeza de la mecánica cuántica, lo que nadie se preguntaba era si esta extrañeza podía ser útil de alguna manera. Seguramente, la primera persona que se planteó esta pregunta fue Stephen Wiesner, que por desgracia falleció el mes pasado. Wiesner era un estudiante de postgrado que en 1969 escribió un artículo en el que presentaba dos propuestas sobre cómo la mecánica cuántica podría servir para resolver diversas tareas de la teoría de la información. Envió este trabajo a una revista, pero desgraciadamente, lo rechazaron. Charlie Bennet, uno de mis compañeros del premio de la Fundación BBVA, que era amigo de Wiesner, en 1983 consiguió que el trabajo de este se publicara en un boletín de ciencia teórica de la computación. Charlie Bennett también desarrolló las ideas de Wiesner. Buscaba un colaborador que conociera la informática y la

21 de septiembre de 2021

criptología; y este fue Gilles Brassard, con quien también compartimos el premio de la Fundación BBVA. Juntos, partieron de las ideas de Wiesner como base para dar con un esquema práctico para la distribución de claves cuánticas, una de las contribuciones que la Fundación BBVA reconoce hoy aquí. Este esquema permite que dos personas que están cada una en un extremo de un canal cuántico, incluso aunque no sea seguro, se comuniquen en absoluto secreto; y este secreto está garantizado por las leyes de la mecánica cuántica.

Otro investigador clarividente que se preguntó si la extrañeza cuántica podría sernos útil fue Richard Feynman. Observó que simular la mecánica cuántica en un ordenador digital parecía llevar mucho tiempo. Entonces se planteó la cuestión de si utilizar un ordenador cuántico sería más eficiente y escribió dos trabajos sobre este tema. David Deutsch tomó el relevo con la pregunta de si los ordenadores cuánticos podrían resolver problemas no cuánticos de forma más eficiente que los ordenadores digitales. Esto dio lugar a una serie de artículos de varios autores, que ofrecían argumentos cada vez más convincentes sobre que posiblemente los ordenadores cuánticos fueran más potentes que los clásicos. Uno de esos artículos, el de Dan Simon, presentaba diversas ideas que me llevaron a encontrar lo que hoy se denomina el algoritmo de Shor: un algoritmo eficiente para factorizar números muy grandes en números primos en un ordenador cuántico. Esto generó mucha atención, porque la seguridad de muchos criptosistemas modernos se basa en la hipótesis de que es difícil factorizar números muy grandes en números primos; y por ello, si alguna vez se construyen ordenadores cuánticos, los códigos que protegen los números de tus tarjetas de crédito cuando compras algo por internet (y montones de cosas mucho más importantes) serán descifrables.

Si alguna vez se construyen ordenadores cuánticos lo suficientemente grandes como para ser útiles, lo que probablemente no sucederá hasta dentro de al menos 15 o 20 años, descifrar códigos no será su única utilidad. Además, podrán investigar sistemas cuánticos, lo que significa que serán extremadamente útiles para la ciencia de materiales, para la industria farmacéutica y para la física fundamental. También hay indicios de que podrán resolver algunos problemas clásicos de gran utilidad de forma más eficiente que los ordenadores digitales.

Para concluir, ¿qué podemos aprender de esta historia? Creo que una de las lecciones es que hacer buenas preguntas, como las de Stephen Wiesner, Richard Feynman y David Deutsch, puede ser tan importante como aportar respuestas. Esto es algo que no aprecia mucha gente. Creo que es una lección importante, y me gustaría animar a todos los científicos que nos escuchan a que piensen en qué preguntas sería útil hacerse.