Acceptance speech
September 21, 2021

Peter Shor, awardee in the Basic Sciences category (12th edition)

I am very pleased and honored to receive the BBVA Frontiers of Knowledge award. It is a pleasure to be included in such a distinguished company of very talented people, not just in science and math but also in fields like music and engineering. Let me thank the BBVA Foundation for establishing this award, and thank the selection committee for choosing me.

Let me also thank the selection committee for choosing the co-recipients of this award. I am particularly pleased to be sharing this award with my colleagues and friends Charlie Bennett and Gilles Brassard; I very much admire them. I've known them both for a long time. In fact, my first introduction to the field of quantum information was when I attended a colloquium given by Charlie Bennett at Bell Labs in the 1980s.

I'd like to say a few words about the history of quantum computing, but first I want to say a little about the history of quantum mechanics. The theory of quantum mechanics was developed over the first years of the 20th century, and around 1925 it started taking on the shape of a coherent theory. It became clear that it would be a rather bizarre strange, and because of this strangeness, Albert Einstein didn't think it could be complete as it was, but that more would have to be added to the theory for it to make sense. This led to a long debate between Niels Bohr and Einstein, with Bohr claiming that it was a satisfactory theory as it was and Einstein claiming that quantum mechanics as it was then formulated couldn't be a representation of a real world. As it turned out, Bohr was correct; in 1964, Bell showed that the theory could not be completed in a way that would satisfy Einstein.

However, while these debates were going on about how to explain the weirdness of quantum mechanics, what nobody asked was whether this weirdness could be useful in some way. Possibly the first person to ask this question might have been Stephen Wiesner, who tragically passed away last month. Wiesner was a graduate student in 1969, and he wrote a paper putting forth two proposals for how quantum mechanics could be useful for solving some information theory tasks. He sent this paper to a journal, but unfortunately, it was rejected. Charlie Bennet, one of the co-recipients of the BBVA Foundation award with me, was a friend of Wiesner's, and in 1983 he got Wiesner's paper published in a theoretical computer science newsletter. Charlie

21 de septiembre de 2021

Bennett also developed Wiesner's ideas further. He sought out a collaborator who knew computer science and cryptology; this was Gilles Brassard, the other co-recipient of this BBVA Foundation award. Together, they built upon Wiesner's ideas to give a practical scheme for quantum key distribution, one of the contributions that the BBVA is honoring. This scheme lets two people on each end of a quantum channel, even one which people can eavesdrop on, communicate in absolute secrecy; and this secrecy is guaranteed by the laws of quantum mechanics.

Another prescient researcher who wondered whether quantum weirdness could be useful was Richard Feynman. He observed that it seemed extremely time-consuming to simulate quantum mechanics by a digital computer. He then asked the question of whether using a quantum computer would be more efficient, and he wrote two papers on this topic. David Deutsch then followed up by asking the question of whether quantum computers could solve non-quantum problems more efficiently than digital computers. This led to a sequence of papers by several authors, who gave successively more convincing arguments that quantum computers could be more powerful than classical ones. It was one of these papers, by Dan Simon, that contained a number of ideas that let me find what is now known as Shor's algorithm, an efficient algorithm for factoring large numbers into primes on a quantum computer. This generated a lot of attention because the security of many modern cryptosystems is based on the hypothesis that it's hard to factor large numbers into primes, so if quantum computers are ever built, the codes that protect your credit card numbers when you buy things over the internet (and lots of much more important things) will be breakable.

If quantum computers large enough to be useful are ever built, which probably won't happen until at least 15 or 20 years from now, breaking codes will not be their only use. They will also be able to do investigate quantum systems, which means they will be extremely useful for materials science, for the pharmaceutical industry, and for fundamental physics. There are also hints that they will also be able to solve some useful classical problems more efficiently than digital computers.

Finally, what can we learn from this history? I think one lesson is that asking the right questions, like Stephen Wiesner, Richard Feynman, and David Deutsch did, can be just as important as coming up with answers. This is something that a lot of people don't appreciate. I think it's a very important lesson, and I'd like to encourage any scientists listening to think about which questions would be useful to ask.

www.premiosfronterasdelconocimiento.es

21 de septiembre de 2021