Acceptance speech
September 21, 2021

Charles Bennett, awardee in the Basic Sciences category (12th edition)

The cosmologist John Wheeler, who made "black hole" a household word, liked to say that the universe is simpler and stranger than we can imagine. Gilles Brassard and I have been privileged to help elucidate a simpler and stranger kind of information, called quantum information. Like a dream it cannot be copied or shared. If you try to describe your dream to someone else, you eventually forget the dream and remember only what you said about it. But unlike dreams quantum information obeys well-understood laws, and it has changed our understanding of the universe in ways every educated person can and should know a little about, as they do, say, about black holes.

The information revolution, which continues to transform every aspect of life in the 21st century, grew out of two discoveries made at Bell Laboratories in 1948. One was the transistor, which launched decades of amazing miniaturization of electronics. The other was Claude Shannon's revolutionary paper on the Mathematical Theory of Communication. Nowadays even nonscientists understand the gist of it: anything one wishes to communicate—words, sounds, pictures, shapes, movements and maybe someday even smells—can be coded into bits—zeros and ones—transmitted through a channel such as radio or optical fiber to a remote location and then reassembled into an arbitrarily good approximation of the original, for the benefit of the recipient. Shannon's theory was an idealization of the robust behavior of macroscopic objects then used as information carriers, like punch cards, cog wheels and electrical switches. Such information can be accurately read and copied without disturbing the original. But chemists and physicists have long known that the information in tiny objects behaves in subtler ways. One cannot learn the exact state of an atom of matter, or a photon of light, because attempting to do so disturbs it; and two atoms or photons, that have once interacted but subsequently move too far apart to influence one another, can exist in a so-called entangled state, where the particles each behave randomly, but in ways that are too strongly correlated to be explained by supposing that each particle is in some (perhaps unknown) state of its own, all of whose properties can in principle be ascertained by examining that particle alone. These phenomena (called "quantum" in distinction to the ordinary "classical" behavior of macroscopic objects) have been reasonably well understood since the 1930's, and have even excited a certain amount of interest among philosophers, but were considered part of the disciplines of physics and chemistry, with little

relevance to information processing except as a nuisance, for example making tiny transistors noisier and less reliable than their larger cousins

Twenty years after Shannon's paper, our gifted colleague Stephen Wiesner, who died earlier this year, noticed that quantum effects could be used to do intriguing things not covered by Shannon's theory, for example combining two messages into a single transmission from which the receiver could recover either one, but not both. Wiesner made little effort to publish or publicize these ideas, but he did tell a few friends. Gilles Brassard and I were among the first to take his ideas seriously, thereby helping launch the discipline now known as quantum information science. Our first discovery, which became the first practical application of quantum information, was called quantum key distribution. It allows two parties, who share no secret information initially, to agree on a shared secret known to no one else. Unlike protocols now in use on the Internet, its privacy is guaranteed by the laws of physics, and could not be defeated by an adversary with superior eavesdropping or computing abilities. With our students we built a working demonstration in 1989, along the way overcoming other problems needed to make the scheme practical, such as compensating for transmission and measurement errors and partial information leakage to an eavesdropper. In the early 1990's, in collaboration with Wiesner, Claude Crépeau, Richard Jozsa, Asher Peres and William Wootters, we showed that entanglement was not just an intriguing phenomenon, but a useful and quantifiable resource, despite having no ability to communicate by itself. In the technique called superdense coding, it doubles the amount of classical information that can be sent through a quantum channel, while in "quantum teleportation" it enables quantum information to be sent through a classical channel. Meanwhile, Artur Ekert showed that entanglement itself can be used for quantum key distribution. Also in the 1990's they and other researchers, building on early work of David Deutsch and Richard Feynman in the 1980's, showed that quantum information provides the same kind of powerful generalization of the classical theory of computation as of Shannon's classical theory of communication. Quantum-information inspired techniques have improved precision timekeeping and measurement, and appear poised to yield economically significant improvements in massive and complex information processing tasks involving various combinations of communication, computation, and privacy. Theoretically, they have brought us to the brink of solving physics' deepest mysteries, such as the origin of spacetime and the fate of information falling into a black hole.

Another mind-boggling discovery of 20th century science is how vast and old the universe is compared to human experience. The known universe contains around a billion trillion planets, many potentially habitable, but ours is the only known civilization. Indeed, what little evidence there is suggests that simple life may be fairly common in the universe, complex life less so, and civilizations so few and far between that we will never know of, or be known of, by another one. But civilization is endangered as never before by the loss boundaries that through most of history allowed it to thrive in one place while becoming moribund or extinct in others. In this lonely

setting, reminiscent of Borges' Library of Babel, no interest of faction, ideology, or nation can trump the existential imperative of preserving civilization on Earth until it can spread to other places. Meanwhile human nature, evolving on a thousand-year timescale, appears not to have caught up with our present situation. It calls for people who think carefully, assessing risks and benefits before they act; but most of us are easily driven to unwise emotive decisions, especially when demagogues and even well-meaning politicians realize that pandering to our fears and prejudices is the most effective or only way to get our vote. Navigating this perilous period of earth history, in which climate and pandemics are driven as strongly by the flow of misinformation as by natural causes, will require an unprecedented collaboration between natural and social scientists.