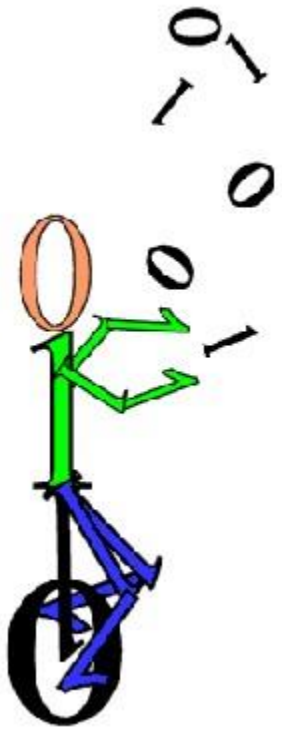
https://www.scientificamerican.com/article/claude-e-shannon-founder/

Claude E. Shannon: Founder of Information Theory

With the fundamental new discipline of quantum information science now under construction, it's a good time to look back at an extraordinary scientist who singlehandedly launched classical information theory

- By Graham P. Collins on October 14, 2002

Updated 10-20-2023



Credit: GRAHAM P. COLLINS

Quantum information science is a young field, its underpinnings still being laid by a large number of researchers [see "Rules for a Complex Quantum World," by Michael A. Nielsen; *Scientific American*, November 2002]. Classical information science, by contrast, sprang forth about 50 years ago, from the work of one remarkable man: Claude E. Shannon. In a landmark paper written at Bell Labs in 1948, Shannon defined in mathematical terms what information is and how it can be transmitted in the face of noise. What had been viewed as quite distinct modes of communication--the telegraph, telephone, radio and television--were unified in a single framework.

Shannon was born in 1916 in Petoskey, Michigan, the son of a judge and a teacher. Among other inventive endeavors, as a youth he built a telegraph from his house to a friend's out of fencing wire. He graduated from the University of Michigan with degrees in electrical engineering and mathematics in 1936 and went to M.I.T., where he worked under computer pioneer Vannevar Bush on an analog computer called the differential analyzer.

Shannon's M.I.T. master's thesis in electrical engineering has been called the most important of the 20th century: in it the 22-year-old Shannon showed how the logical algebra of 19th-century mathematician George Boole could be

implemented using electronic circuits of relays and switches. This most fundamental feature of digital computers' design--the representation of "true" and "false" and "0" and "1" as open or closed switches, and the use of electronic logic gates to make decisions and to carry out arithmetic--can be traced back to the insights in Shannon's thesis.

In 1941, with a Ph.D. in mathematics under his belt, Shannon went to Bell Labs, where he worked on war-related matters, including cryptography. Unknown to those around him, he was also working on the theory behind information and communications. In 1948 this work emerged in a celebrated paper published in two parts in Bell Labs's research journal. **Quantifying Information**

Shannon defined the quantity of information produced by a source--for example, the quantity in a message--by a formula similar to the equation that defines thermodynamic entropy in physics. In its most basic terms, Shannon's informational entropy is the number of binary digits required to encode a message. Today that sounds like a simple, even obvious way to define how much information is in a message. In 1948, at the very dawn of the information age, this digitizing of information of any sort was a revolutionary step. His paper may have been the first to use the word "bit," short for binary digit.

As well as defining information, Shannon analyzed the ability to send information through a communications channel. He found that a channel had a certain maximum transmission rate that could not be exceeded. Today we call that the bandwidth of the channel. Shannon demonstrated mathematically that even in a noisy channel with a low bandwidth, essentially perfect, errorfree communication could be achieved by keeping the transmission rate within the channel's bandwidth and by using error-correcting schemes: the transmission of additional bits that would enable the data to be extracted from the noise-ridden signal.

Today everything from modems to music CDs rely on error-correction to function. A major accomplishment of quantum-information scientists has been the development of techniques to correct errors introduced in quantum information and to determine just how much can be done with a noisy

quantum communications channel or with entangled quantum bits (qubits) whose entanglement has been partially degraded by noise.

The Unbreakable Code

A year after he founded and launched information theory, Shannon published a paper that proved that unbreakable cryptography was possible. (He did this work in 1945, but at that time it was classified.) The scheme is called the onetime pad or the Vernam cypher, after Gilbert Vernam, who had invented it near the end of World War I. The idea is to encode the message with a random series of digits--the key--so that the encoded message is itself completely random. The catch is that one needs a random key that is as long as the message to be encoded and one must never use any of the keys twice. Shannon's contribution was to prove rigorously that this code was unbreakable. To this day, no other encryption scheme is known to be unbreakable.

The problem with the one-time pad (so-called because an agent would carry around his copy of a key on a pad and destroy each page of digits after they were used) is that the two parties to the communication must each have a copy of the key, and the key must be kept secret from spies or eavesdroppers. Quantum cryptography solves that problem. More properly called quantum key distribution, the technique uses quantum mechanics and entanglement to generate a random key that is identical at each end of the quantum communications channel. The quantum physics ensures that no one can eavesdrop and learn anything about the key: any surreptitious measurements would disturb subtle correlations that can be checked, similar to errorcorrection checks of data transmitted on a noisy communications line. Encryption based on the Vernam cypher and quantum key distribution is perfectly secure: quantum physics guarantees security of the key and Shannon's theorem proves that the encryption method is unbreakable. [For *Scientific American* articles on quantum cryptography and other developments of quantum information science during the past decades, please click here.]

A Unique, Unicycling Genius

Shannon fit the stereotype of the eccentric genius to a T. At Bell Labs (and later M.I.T., where he returned in 1958 until his retirement in 1978) he was

known for riding in the halls on a unicycle, sometimes juggling as well [see "Profile: Claude E. Shannon," by John Horgan; *Scientific American,*January 1990]. At other times he hopped along the hallways on a pogo stick. He was always a lover of gadgets and among other things built a robotic mouse that solved mazes and a computer called the Throbac ("THrifty ROman-numeral BAckward-looking Computer") that computed in roman numerals. In 1950 he wrote an article for *Scientific American* on the principles of programming computers to play chess [see "A Chess-Playing Machine," by Claude E. Shannon; *Scientific American*, February 1950].

In the 1990s, in one of life's tragic ironies, Shannon came down with Alzheimer's disease, which could be described as the insidious loss of information in the brain. The communications channel to one's memories-one's past and one's very personality--is progressively degraded until every effort at error correction is overwhelmed and no meaningful signal can pass through. The bandwidth falls to zero. The extraordinary pattern of information processing that was Claude Shannon finally succumbed to the depredations of thermodynamic entropy in February 2001. But some of the signal generated by Shannon lives on, expressed in the information technology in which our own lives are now immersed.

Graham P. Collins is on the board of editors at Scientific American.

ABOUT THE AUTHOR(S)

Graham P. Collins

Recent Articles

- Projects in Profusion: A Skeptical Look at 3 Wild Fusion-Energy Schemes
- 7 Radical Energy Solutions
- Solving the Cocktail Party Problem