RETROSPECTIVE: COMMUNICATION

Claude E. Shannon (1916–2001)

Solomon W. Golomb

His inventive mind enriched many fields, but Claude Shannon's enduring fame will surely rest on his 1948 paper "A Mathematical Theory of Communication" and the ongoing revolution in information technology it engendered.

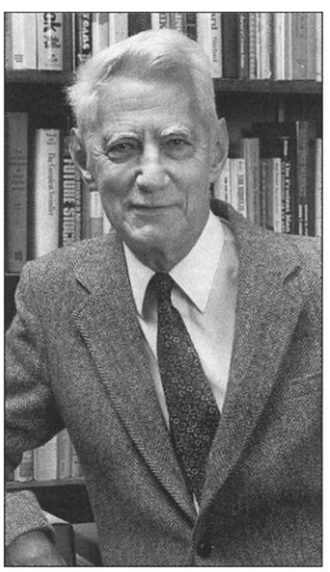
Shannon was born on 30 April 1916 in Petoskey, Michigan. After obtaining bachelor's degrees in mathematics and electrical engineering at the University of Michigan, he went to the Massachusetts Institute of Technology (MIT), where, after spending the summer of 1937 at Bell Laboratories, he wrote one of the greatest master's theses ever (*1*). He showed that the symbolic logic of George Boole's 19th century *Laws of Thought* provided the perfect mathematical model for switching theory (and indeed for the subsequent logic design of digital circuits and computers). This work was awarded the prestigious Alfred Noble Prize of the combined engineering societies of the United States in 1940.

From 1938, Shannon worked at MIT with Vannevar Bush's "differential analyzer," the ancestral analog computer. After obtaining his Ph.D. at MIT, he spent the academic year 1940–1941, working under mathematician Hermann Weyl in Princeton, where he began to think about the mathematics underlying communications. In 1941, he returned to Bell Labs for the next 15 years, initially working on projects related to the war effort, including cryptography (*2*). Perhaps it was thinking about cryptography that led Shannon to his breakthrough in "A Mathematical Theory of Communication," published in two parts in the *Bell System Technical Journal* (BSTJ) in 1948.

At the start of this epic paper, he acknowledged the work of Harry Nyquist and R. V. L. Hartley at Bell Labs in the 1920s. But Shannon, like Newton "standing on the shoulders of giants," was able to see much farther than his predecessors. Early in the paper, he wrote that the "semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one *selected from a set* of possible messages." [Shannon's emphasis]

Shannon recognized, however, that it was not only the size of the set of possible messages that was important, but also their respective a priori probabilities. His great insight was to think in terms of statistical ensembles: He saw the source as the set of all messages that may be sent, with their respective probabilities, while the channel contributed the set of possible disturbances ("noise") to the message.

Shannon redefined the entropy of thermodynamics as a measure of uncertainty on probability distributions. Although crediting the term "bit" (for "binary digit") to J. W. Tukey, for his own purposes, Shannon defined bit as the amount of information gained (or entropy removed) upon learning the answer to a question whose two possible answers were equally likely a priori. (When one possible answer is more likely than the other, the answer conveys less than one bit of information.) He derived formulas for the information rate of a source and for the capacity of a channel, each measured in bits per second, and proved that for any information rate R less than the channel capacity C, it is possible (by suitable encoding) to send information at rate R, with an error rate less than any preassigned ε, over that channel. His ingenious proof considers the set of all possible encodings of source messages into streams of binary digits and shows that an encoding chosen at random from this set will have the desired property with extremely high probability.



Generations of coding theorists have struggled to find codes that perform as well as Shannon's "random" ones. Richard W. Hamming at Bell Labs and Marcel Golay at IBM Research Labs pioneered the theory of error-correcting codes in the late 1940s, largely independent of Shannon's work. However, some communication systems today achieve performance within 0.115% of the Shannon limit by using codes closer to Shannon's original "random codes" than to the block codes of Hamming or Golay.

Shannon pioneered the study of source coding (data compression) to remove all useless redundancy from source messages, which, if they are to be sent over noisy channels, can have useful redundancy (extra symbols for error detection and correction) added back. He also showed that reliable circuits could be built with unreliable parts, again using redundancy, akin to achieving reliable communication over unreliable (i.e., noisy) channels.

The Shannon bit is now universally recognized as the basic unit of information. It has been proposed to rename this unit the shannon. If a message consists of N shannons, then the theoretically best source encoding could express it in N binary digits.

Shannon was a talented gadgeteer who built some of the earliest robotic automata, game-playing devices, and puzzle-solving machines. He could juggle while riding a unicycle and designed machines to juggle and to ride unicycle-like vehicles. Not working in a Nobel Prize field but in the new science he had invented, he received innumerable honors and awards, including the U.S. National Medal of Science (1966), Israel's Harvey Prize (1972), and Japan's Kyoto Prize (1985). The Information Theory Group (later Society) of the Institute of Electrical and Electronics Engineers established the Shannon Award (originally called Shannon Lecture) as its highest honor. In 1973, Shannon delivered the first Shannon Lecture in Ashkelon, Israel. I had spent most of the fall of 1959 at MIT, where I had gotten to know Shannon quite well, but it was an unexpected honor when he attended my Shannon Lecture in 1985 in Brighton, England—the only one he attended after his own.

In 1956, Shannon left Bell Labs for MIT, where he was Donner Professor of Science from 1958 until his retirement in 1978. He died on 24 February 2001, in Medford, Massachusetts, aged 84.

In 1964, the title of a book I edited and coauthored, *Digital Communications*, was still considered an oxymoron: To most communication engineers, signals were quite obviously analog. But in the late 1940s, the transistor was invented, also at Bell Labs. Shannon's remarkable theorems told communications engineers what goals to strive for, and integrated circuits provided ever-improving hardware to realize these goals. Thus, the foundation for the digital communications revolution was laid. It is no exaggeration that Claude Shannon was the Father of the Information Age and his intellectual achievement one of the greatest of the 20th century.

The author is at the Department of Electrical Engineering-Systems, University of Southern California, Los Angeles, CA 90089, USA. E-mail: sgolomb@usc.edu

CREDIT: AP PHOTO/LUCENT TECHNOLOGIES

References and Notes

1. Published in 1938 as "A Symbolic Analysis of Relay and Switching Circuits" in the *Transactions of the American Institute of Electrical Engineers.*
2. Shannon's classified report, "A Mathematical Theory of Cryptography" (1945), was declassified and published in 1949 in the *Bell System Technical Journal.*