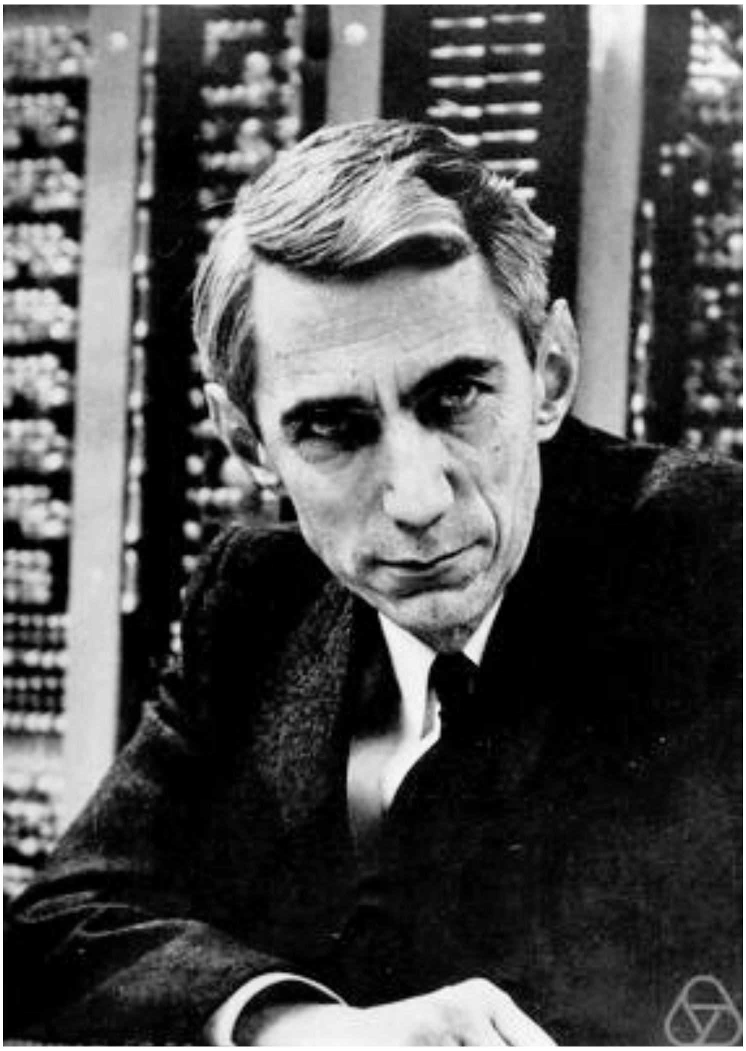
SciHi Blog
daily blog on science, tech & art in history

Claude Shannon – the Father of Information Theory



Claude E. Shannon (1916-2001), photo: Jacobs, Konrad, CC BY-SA 2.0 DE, via Wikimedia Commons

On April 30, 1916, American mathematician, electrical engineer, and cryptographer **Claude Elwood Shannon** was born, the “father of information theory“, whose groundbreaking work ushered in the Digital Revolution. Of course Shannon is famous for having founded information theory with one landmark paper published in 1948. But he is also credited with founding both digital computer and digital circuit design theory in 1937, when, as a 21-year-old master’s student at MIT, he wrote a thesis demonstrating that electrical application of Boolean algebra could construct and resolve any logical, numerical relationship. Believe it or not, it has been claimed that this was the most important master’s thesis of all time. Shannon contributed to the field of cryptanalysis during World War II and afterwards, including basic work on code breaking.

“This duality can be pursued further and is related to a duality between past and future and the notions of control and knowledge. Thus we may have knowledge of the past but cannot control it; we may control the future but have no knowledge of it.”
— Claude Shannon, [9]

Youth and Education

Claude Shannon was born in a hospital in Petoskey, Michigan, and grew up in nearby Gaylord, the home of his parents. His father was a judge, his mother a language teacher of German origin. During his high school years he worked as a messenger for the Western Union. He followed his sister Catherine to the University of Michigan in 1932. In 1936 he moved to MIT with a degree in mathematics and electrical engineering. In his master thesis (1937), *A Symbolic Analysis of Relay and Switching Circuits*, he applied Boolean algebra to construct digital circuits. The work arose from the analysis of the relay circuits in Vannevar Bush‘s *Differential Analyzer* analog computer,[2] which Shannon programmed for users. In 1940 he received his doctorate in mathematics with a thesis on theoretical genetics (*An Algebra for Theoretical Genetics*) at MIT.

The Fundamental Unit of Information

After a short stay as a researcher at the Institute for Advanced Study in Princeton, New Jersey, he joined AT&T Bell Labs in 1941 as a mathematician. In 1948 Claude Shannon published his groundbreaking work *A Mathematical Theory of Communication,* which introduced the word “bit” as the fundamental unit of information for the first time.[3] In this paper, he focused on the conditions under which information encoded by a transmitter and transmitted through a noisy communication channel can be restored to its destination, i.e. decoded without loss of information. Shannon showed that adding extra bits to a signal allowed transmission errors to be corrected.[1]

Entropy in Information Theory

He was able to successfully apply the concept of entropy known from physics in information theory. At the same time, he published *Communication in the presence of noise*, in which he combined the representation of frequency-restricted functions by the cardinal series with considerations on maximum data rate, in particular by Harry Nyquist, on a theory of channel capacity in digital signal transmission. Before him, but without his knowledge, Vladimir Alexandrovich Kotelnikov published an identical result in 1933. Accordingly, the sampling rate for a signal must be at least twice as high as the highest frequency contained in it in order to be reconstructed into an analog signal without loss of information (Nyquist Shannon sampling theorem).

The Foundations of Cryptography

“A few first rate research papers are preferable to a large number that are poorly conceived or half-finished. The latter are no credit to their writers and a waste of time to their readers.” – Claude Shannon, [10]

Another notable article appeared in 1949, *Communication Theory of Secrecy Systems*,[4] in which Shannon clarified the formal foundations of cryptography, elevating it to the rank of an independent science. Shannon was interested in many things and creative; he is said to have juggled around in the corridors of Bell on a unicycle. Peripheral products of his professional activity include a juggling machine, rocket-driven frisbees, motorized pogo sticks, a machine for reading thoughts, a mechanical mouse, which could orient itself by means of a simple memory consisting of relay circuits in labyrinths, and already in the 1960s an early chess computer. A work from 1950 already deals with chess programs, which was influential and led to the first chess game on computers on the MANIAC computer in Los Alamos in 1956. He also built the “ultimate machine”, a box with a switch that a mechanical hand turned off after it was turned on.

Information Content

The unit of information content of a message, the Shannon, was named after him. One shannon is the information content of an event occurring when its probability is 1/2. If a message is made of a sequence of a given number of bits, with all possible bit strings being equally likely, the information content of one such message expressed in shannons is equal to the number of bits in the sequence

Later Years

In the mid-1960s he became interested in financial transactions and gave several well-attended lectures at MIT (one of his listeners was Paul Samuelson). He proposed a method, now called *Constant Proportion Rebalanced Portfolio*, to profit from random market fluctuations (after each transaction, the capital was divided into exactly two halves, one for speculation, the other cash reserve). Shannon received many honors for his work. Among a long list of awards were the Alfred Nobel American Institute of American Engineers Award in 1940, the National Medal of Science in 1966, the Audio Engineering Society Gold Medal in 1985, and the Kyoto Prize in 1985.[1] Shannon developed Alzheimer’s disease and spent the last few years of his life in a nursing home; he died in 2001.

References and Further Reading:

- [1] John J. O’Connor, Edmund F. Robertson: Claude Shannon. In: MacTutor History of Mathematics archive
- [2] Vannevar Bush and his Vision of the Memex Memory Extender, SciHi Blog
- [3] Claude Elwood Shannon: *A Mathematical Theory of Communication*. In: Bell System Technical Journal. Short Hills N.J. 27.1948, (Juli, Oktober), S. 379–423, 623–656.

- [4] Claude Elwood Shannon: Communication Theory of Secrecy Systems. In: Bell System Technical Journal. Band28, Nr.4, 1949, S.656–715
- [5] Claude Shannon at zbMATH
- [6] Claude Shannon at the Mathematics Genealogy Project
- [7] Claude Shannon at Wikidata
- [8] A Public Lecture Celebrating Claude E. Shannon – Sergio Verdu, Nov 16, 2016, Institute for Advanced Study @ youtube
- [9] Claude Shannon, *Coding theorems for a discrete source with a fidelity criterion*. IRE International Convention Records, volume 7, pp. 142–163, 1959.
- [10] Claude Shannon, IRE Transactions on Information Theory (1956), volume 2, issue 1, page 3. Shannon, Claude E. (March 1956), The Bandwagon, 2,
- [11] Timeline for Claude Elwood Shannon, via Wikidata