»Colloquium«

The Legacy of Claude Shannon

dp-pmi.org/The-Legacy-of-Claude-Shannon

Tuesday • 13 December 2016, at 16:00
Salão Nobre, Instituto Superior Técnico
ULisboa, Portugal

Programme

16:00  Evoking Claude Shannon
       José Francisco Rodrigues & Amílcar Sernadas

16:15  The Shannon Machine
       Daniel Graça

16:30  Shannon and Digital Circuits
       Arlindo Oliveira

16:45  Telecommunications before and after Shannon
       Carlos Salema

17:00  Mathematics of Secrets and Quantum Cryptography
       Yasser Omar

17:15  Applications of Information Theory in Science and in Engineering
       Mário Figueredo

17:00  Closure of the session

José Francisco Rodrigues  (CMAF&IO_F Ciências_U Lisboa)
Amílcar Sernadas  (CMAF&IO_I S Técnico_U Lisboa)
[a] playful genius who invented the bit, separated the medium from the message, and laid the foundations for all digital communications. . . . [He] single-handedly laid down the general rules of modern information theory, creating the mathematical foundations for a technical revolution. Without his clarity of thought and sustained ability to work his way through intractable problems, such advances as e-mail and the World Wide Web would not have been possible.

Something of a loner throughout his working life, he was individually responsible for two of the great breakthroughs in understanding which heralded the convergence of computing and communications. To colleagues in the corridors at the Massachusetts Institute of Technology who used to warn each other about the unsteady advance of Shannon on his unicycle, it may have seemed improbable that he could remain serious for long enough to do any important work. Yet the unicycle was characteristic of his quirky thought processes, and became the topsy-turvy symbol of unorthodox progress towards unexpected theoretical insights.
1916 – Born and educated in Gaylord, Michigan, USA

1932 – Studied Mathematics (M) and Electrical Engineering (EE), University of Michigan

1936 – Joined the EE Dep. at MIT where he worked with on Vannevar Bush’s differential analyzer, an early analog computer.

1938 – In his remarkable master’s thesis entitled *An analysis of relay and switching circuits*, at Math Dep., he established how Boole’s logical symbols can be regarded as a series of on–off switches so that binary arithmetic can be performed by electrical circuits and he developed mathematical techniques for building a network of switches and relays to realize a specific logical function. The work was made independently of the similar earlier theory of Victor Shestakov, which was published in 1941.

1939 – Alfred Noble Prize of the combined American engineering societies.

1940 – PhD thesis *An algebra for theoretical genetics*, also at MIT; He was awarded with a fellowship to do research at the Institute for Advanced Study in Princeton, under Hermann Weyl, where he met John von Neumann.
Evoking Claude Shannon 1916-2001

His results overlapped with some of the early work by J. B. S. Haldane on population genetics, of which he seemed to be unaware. It was published in 1993, when most of his results were obtained independently by others.

The result of random intermating is given by:

\[ \mathbb{P}_n \left( \lambda_1^u \ldots \lambda_k^u \right) = \left[ \rho_0^{n-1} (\rho_0 \lambda_1^{\kappa_1} + \rho_1 \lambda_1^{\kappa_1}) + (1 - \rho_0^{n-1}) \lambda_1^{\kappa_1} \right] \left[ \rho_0^{n-1} (\rho_0 \lambda_2^{\kappa_2} + \rho_1 \lambda_2^{\kappa_2}) + (1 - \rho_0^{n-1}) \lambda_2^{\kappa_2} \right] \ldots \left[ \rho_0^{n-1} (\rho_0 \lambda_k^{\kappa_k} + \rho_1 \lambda_k^{\kappa_k}) + (1 - \rho_0^{n-1}) \lambda_k^{\kappa_k} \right] \]

and (assuming \( \rho_0 \neq 1 \)) approaches asymptotically the population

\[ \mathbb{P}_n \left( \lambda_1 \ldots \lambda_k \right) \rightarrow \lambda_1 \lambda_2 \ldots \lambda_k \quad \text{as} \quad n \to \infty \]

Proof: By definition (8) the first generation is:
1942 – Already at Bell Labs, where he was a research mathematician for fifteen years, during the World War he worked in fire-control systems for anti-aircraft artillery and in cryptography; in 1943 he met Alan Turing and also developed a mathematical theory of cryptography published, in 1949, as *A Communication Theory of Secrecy Systems*.

1948 – Shannon published his most important work, *A mathematical theory of communication*, that was explained in the book, co-authored by W. Weaver, *The mathematical theory of communication*, developing the concept of entropy to measure uncertainty in a message and laying the basis of the mathematical theory of information.

1958 – Appointed Donner Professor of Science at MIT, until his retirement in 1978, having been awarded of several prizes, including the National Medal of Science (1966), the Kyoto Prize (1983) and the National Inventors Hall of Fame (2004).

Evoking Claude Shannon
1916-2001

So wide were its repercussions that the theory was described as one of humanity’s proudest and rarest creations, a general scientific theory that could profoundly and rapidly alter humanity’s view of the world. Few other works of the twentieth century have had a greater impact; he altered most profoundly all aspects of communication theory and practice.

Ioan James (2014)
A definição de entropia em cálculo das probabilidades
por J. J. Dionísio

O propósito deste artigo é expor como se introduz no Cálculo das Probabilidades o conceito de entropia. Colocar-nos-emos naturalmente no caso mais simples das distribuições discreta e a isso se limitarão as nossas considerações. Seguiremos para o efeito a primeira das memórias de A. I. Khinchin editadas pela casa Dover de Nova York sob o título *Mathematical Foundations of Information Theory*, editadas também em Berlim (Deutscher Verlag der Wissenschaften) acompanhadas de trabalhos de outros autores, sob a epígrafe *Arbeiten zur Informationstheorie*.

Assim se esclarece, nas suas linhas gerais, a conexão entre a relação (17) de Boltzman e a definição (2) da função entropia.

Contudo, foi a moderna teoria das telecomunicações e do controle automático que levou o cientista americano C. E. Shannon a introduzir a definição geral de entropia (*A mathematical theory of communication*, Bell System Techn. J., 27, 1948), criando-se assim um novo ramo do Cálculo das Probabilidades que se encontra em pleno desenvolvimento: a teoria da informação.

Princípios fundamentais dos computadores digitais automáticos
por A. César de Freitas
The growth of both communication and computing devices has been explosive in the last century. It was about a hundred years ago that the telephone and phonograph were invented, and these were followed by radio, motion pictures and television. We now have vacuum tubes, transistors, integrated circuits, satellite communication and microwave cable. We have even talked to astronauts on the moon. Our life style has been totally changed by advances in communication. On the computing side we started the twentieth century with slide rules and adding machines. These were followed in quantum jumps by Bush analog computers, Stibitz and Aiken relay computers, Eckert and Mauchly vacuum tube machines …, transistor computers and, finally, the incredibly compact integrated circuit and chip computers. At each step the computers became faster, cheaper and more powerful. These hardware revolutions were matched by equally impressive developments in programming.

Shannon (1983)

References
