Shannon‘s Work and Its Legacy

Michelle Effros and Vince Poor

with thanks to Mario Goldenbaum and Wei Yang

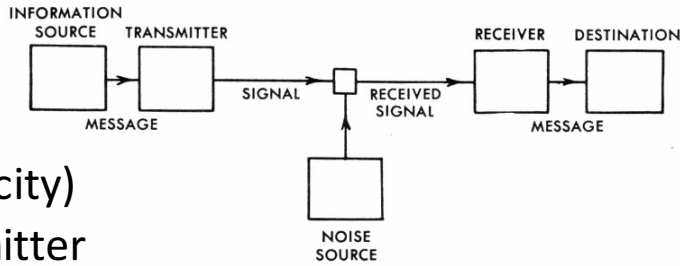
Outline

- Capacity
- Multiuser Channels
- Channel Coding
- Network Coding
- Detection & Hypothesis Testing
- Source Coding
- Learning & Big Data
- Complexity & Combinatorics
- Secrecy
- Applications
- And more …

Capacity

What Shannon did:

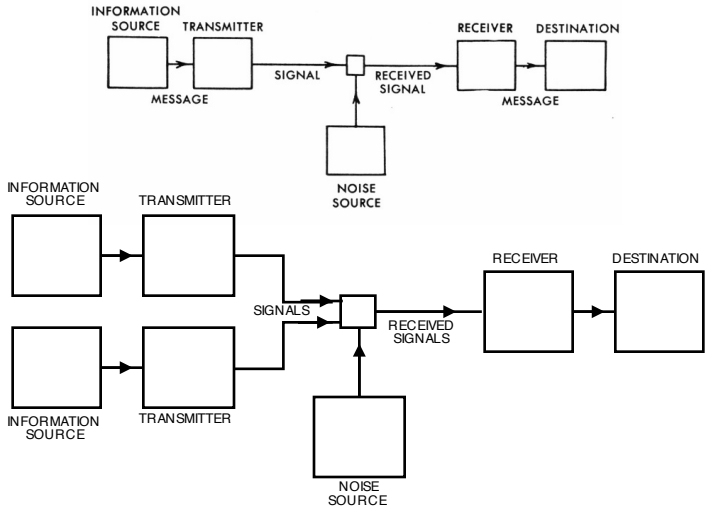
- **1948**: the notion of *capacity* C was born (the fundamental limit of reliable communication over a channel)
- **1949**: AWGN channel, colored noise channel (water filling)
- **1956**: the *zero error capacity* C_0
- **1956**: *feedback capacity* C_{FB} (feedback does not increase capacity)
- **1958**: capacity of channels *with side information* at the transmitter
- **1957-67**: bounds (error exponent, error probability, …)



How far did we go (+ more):

- Identification capacity [1980s]
- *General formula* for channel capacity [1990s]
- *Quantum* channel capacity [1990s]
- Capacity of *fading* channels, *MIMO* channels, etc. [1990s]
- Computation capacity [2000s]
- *Finite blocklength* results [2010s]

Multiuser Channels



What Shannon did:

- **1948**: point-to-point channel
- **1956**: channels with *feedback*
- **1960**: *two-way* channels
- **1960**: reference to upcoming work on *channels with multiple receivers*

How far did we go (+ more):

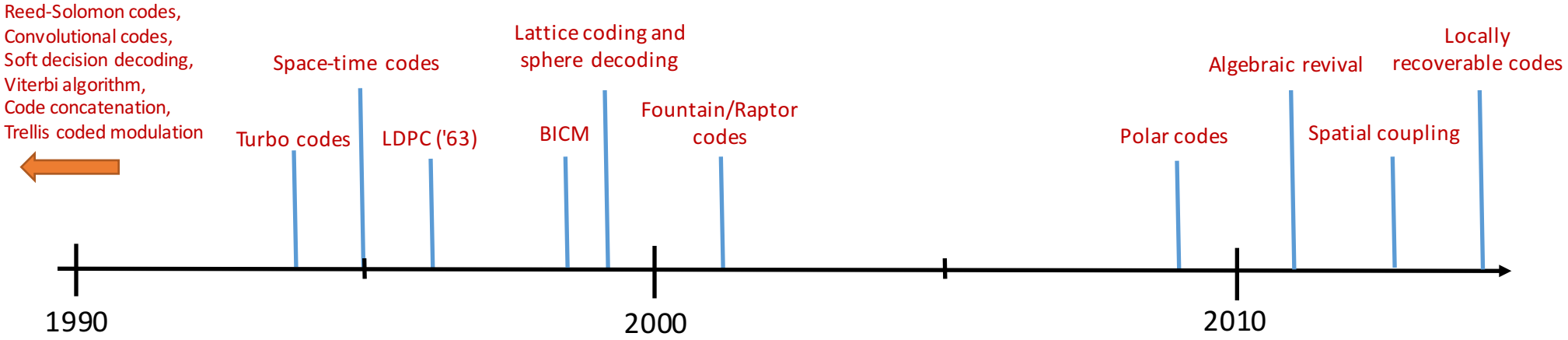
- *Feedback* benefits, algorithms, generalizations [late 1960s - 1970s]
- Two-way channels – upper & lower bounds [1980s]
- *Multiterminal channels*: Multiple access, broadcast, relay, interference, ... [1970s-]
- Related channel models (compound, wiretap, uncertain ...) [1960s-]
- *Joint source-channel coding* for multiuser channels [1970s-]
- Networks of multiuser channels [2000s-]
- *Network coding* [2000s-]

Channel Coding

What Shannon did:

- Crown jewel of [Shannon '48]: *noisy channel coding* theorem
  - For rates $R < C$, arbitrary small error probabilities are achievable (asymp.)
  - Previously, communication engineers thought arbitrarily small error probabilities could only be achieved for $R \to 0$
  - The theorem initiated *channel coding research*

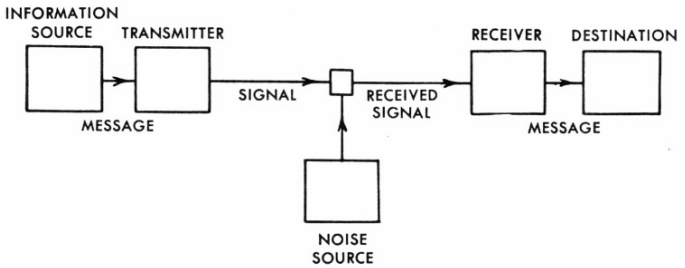
How far did we go (+ more):



Network Coding

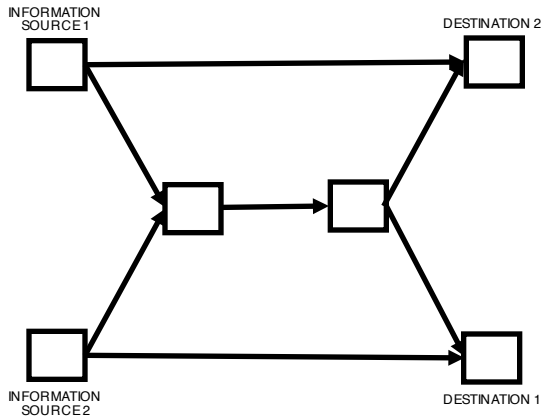
What Shannon did:

- **1948**: capacity of a *point-to-point channel*

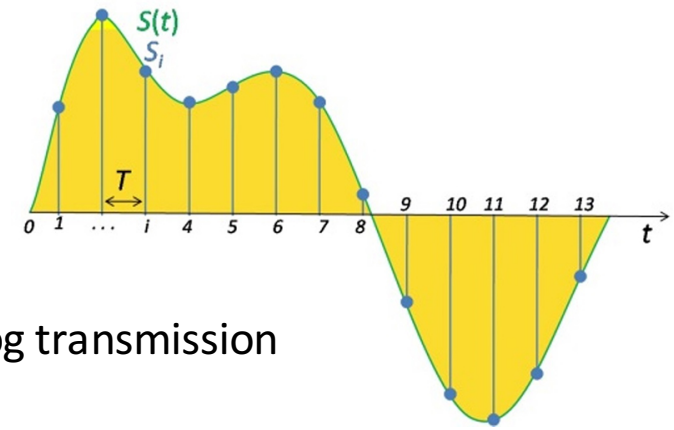


How far did we go (+ more):

- Capacities of *networks* of channels (mulitcast, multi-source multicast, etc.)
- *Capacity* bounds
- Index coding
- *Code design*
- Equivalence
- Network error correction
- *Secure network coding*
- Network coding for *distributed storage*



Detection & Hypothesis Testing



What Shannon did:

- **1944**: the best detection of pulses
  - Derivation of the MAP detector (*matched filter*)
  - Application of hypothesis testing to communication theory
- **1948**: the philosophy of PCM
  - Demonstrated *advantage of digital transmissions* over analog transmission
- **1949**: Nyquist-Shannon *sampling theorem*

How far did we go (+ more):

- Sequential detection [1940-50s]
- *Sequence detection* (Viterbi algorithm, Forney's MLS detector) [1960-70s]
- Quickest change detection [1970s]
- Hypothesis testing with constraints (*distributed detection*) [1980s]
- *Multiuser detection*, *MIMO* detection (sphere decoding) [1980-90s]
- *Compressed sensing* [2000s]

Source Coding

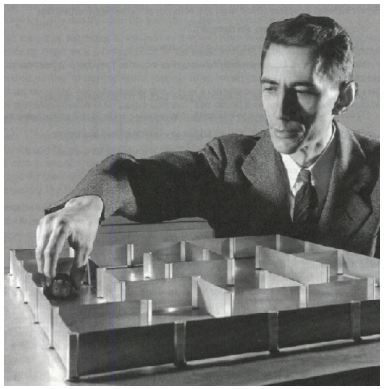
What Shannon did:

- **1939**: posed *lossy source coding* problem
- **1948**: *source coding theorem* (achievability strong converse), fixed- and variable-length codes, arithmetic codes, *entropy*, entropy rate, typicality, memoryless and stationary Markov sources
- **1948**: *rate-distortion bound*, separation theorem, continuous Gaussian source example
- **1959**: *rate-distortion* function, example solutions

How far did we go (+ more):

- Detailed *proofs*, extensions, solved examples [1950s-1970s]
- Code *designs* (Huffman, Tunstall, arithmetic; VQ, ECVQ) [1950s-1980s]
- Adaptive & *universal codes* (existence, rates of convergence, Lempel-Ziv, MDL) [1970s-90s]
- *Multiterminal* source coding (Slepian-Wolf, Ahlswede-Korner, Gray-Wyner, Wyner-Ziv, multiple description, functional)[1970s-]
- *Image, audio* & *video* coding (JBIG, JPEG, MPEG, MP3, etc.)

Learning & Big Data

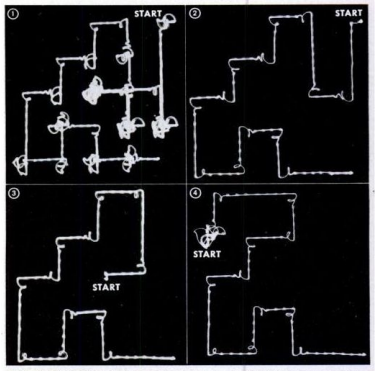


What Shannon did:

- **1950**: programming a computer to play *chess*
- **1952**: the *maze-solving mouse* "Theseus"

How far did we go (+ more):

- IBM checkers player [1950s]
- *Neural networks* [1960s-]
- Decision trees [1980s]
- New theories and technologies: SVM, adaboost, *graphical models*, Bayesian methods [1990s-]
- *Deep Blue* [1990s], *IBM Watson* [2011], *AlphaGo* [2016]
- *Deep learning* [2000s]
- *Self-driving cars*



MEMORY TESTS show how Theseus learns. In first trial the mouse makes wrong turns, leaves complicated trail. Second time he starts from the same place, goes straight to the goal. In third trial he is started from different spot but is on the original trail, so has no trouble. The fourth time he is put in an unfamiliar square, blunders around until he gets on the course he has learned.

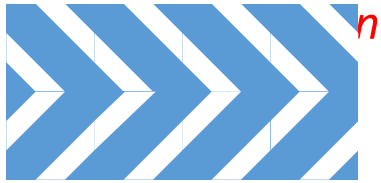
Complexity & Combinatorics

What Shannon did:

- **1938**: application of Boolean algebra to switching circuits
- **1948**: tools and concepts (entropy, typical strings, ...)
- **1956**: *zero-error capacity*

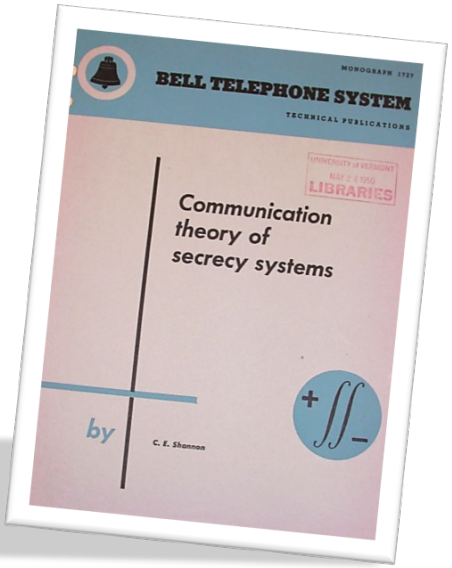
How far did we go (+ more):

- Generalizations of tools (*typical sets*, method of types, *inequality*, entropy space characterizations)
- *Communication complexity*
- Streaming computation
- Counting estimates
- *Concentration inequalities*
- Additive combinatorics
- Hypercontractivity bounds



no's

Secrecy



What Shannon did:

- **1949**: provides a foundational treatment of modern cryptography
  - All theoretically unbreakable ciphers must have the same information requirements as the one-time pad

How far did we go (+ more):

- *Wiretap channels* (secrecy capacity, common randomness) [1970s, 1980s]
- Broadcast channel with confidential messages [1970s]
- *Public-key* cryptosystems (RSA) [1970s-]
- *Secret-key sharing/generation/agreement* (secret-key capacity) [1990s-]
- Wireless *physical layer security* [2000s-]

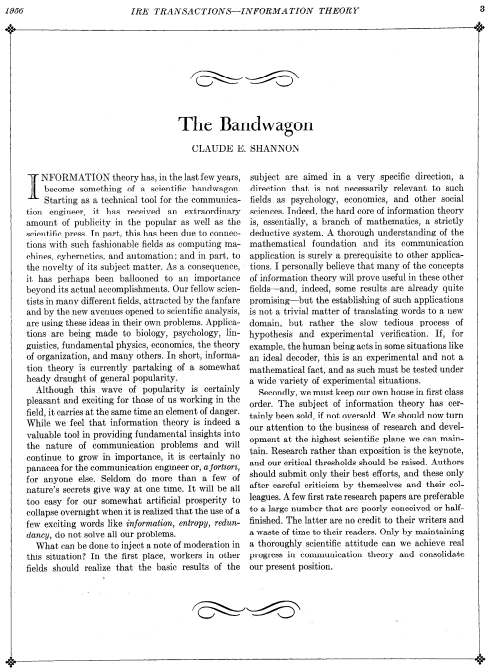
Applications

What Shannon did:

- **1940**: an algebra of *theoretical genetics* (population dynamics)
- **1956**: *bandwagon*

How far did we go (+ more):

- Math, probability, statistical inference, …
- *Computer science*
- Biology / neuroscience / genetics
- Chemistry
- *Finance*
- *Linguistics*



1956 IRE TRANSACTIONS—INFORMATION THEORY 3

The Bandwagon

CLAUDE E. SHANNON

INFORMATION theory has, in the last few years, become something of a scientific bandwagon. Starting as a technical tool for the communication engineer, it has received an extraordinary amount of publicity in the popular as well as the scientific press. In part, this has been due to connections with such fashionable fields as computing machines, cybernetics, and automation; and in part, to the novelty of its subject matter. As a consequence, it has perhaps been ballooned to an importance beyond its actual accomplishments. Our fellow scientists in many different fields, attracted by the fanfare and by the new avenues opened to scientific analysis, are using these ideas in their own problems. Applications are being made to biology, psychology, linguistics, fundamental physics, economics, the theory of organization, and many others. In short, information theory is currently partaking of a somewhat heady draught of general popularity.

Although this wave of popularity is certainly pleasant and exciting for those of us working in the field, it carries at the same time an element of danger. While we feel that information theory is indeed a valuable tool in providing fundamental insights into the nature of communication problems and will continue to grow in importance, it is certainly no panacea for the communication engineer or, *a fortiori*, for anyone else. Seldom do more than a few of nature's secrets give way at one time. It will be all too easy for our somewhat artificial prosperity to collapse overnight when it is realized that the use of a few exciting words like *information, entropy, redundancy*, do not solve all our problems.

What can be done to inject a note of moderation in this situation? In the first place, workers in other fields should realize that the basic results of the subject are aimed in a very specific direction, a direction that is not necessarily relevant to such fields as psychology, economics, and other social sciences. Indeed, the hard core of information theory is, essentially, a branch of mathematics, a strictly deductive system. A thorough understanding of the mathematical foundation and its communication application is surely a prerequisite to other applications. I personally believe that many of the concepts of information theory will prove useful in these other fields—and, indeed, some results are already quite promising—but the establishing of such applications is not a trivial matter of translating words to a new domain, but rather the slow tedious process of hypothesis and experimental verification. If, for example, the human being acts in some situations like an ideal decoder, this is an experimental and not a mathematical fact, and as such must be tested under a wide variety of experimental situations.

Secondly, we must keep our own house in first class order. The subject of information theory has certainly been sold, if not oversold. We should now turn our attention to the business of research and development at the highest scientific plane we can maintain. Research rather than exposition is the keynote, and our critical thresholds should be raised. Authors should submit only their best efforts, and these only after careful criticism by themselves and their colleagues. 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. Only by maintaining a thoroughly scientific attitude can we achieve real progress in communication theory and consolidate our present position.

And more ...

- **1948**: Note on certain *transcendental numbers*
- **1982**: Scientific aspects of *juggling*
- **1982**: A rubric on *Rubik cubics*
- + more