Information Theory

Master of Logic 2014

3rd Quarter Feb / March

Some of these slides are copied from or heavily inspired by the
University of Illinois at Chicago, ECE 534: Elements of Information Theory course
given in Fall 2013 by Natasha Devroye
Thank you very much for the kind permission to re-use them here!

Christian Schaffner

- me
- pure mathematics at ETH Zurich
- PhD from Aarhus, Denmark
- research: quantum cryptography
- c.schaffner@uva.nl

- plays ultimate frisbee

Cuong Hoang

- your teaching assistant
- PhD student @ILLC
- working on machine translation
- hoangcuong2011@gmail.com

Practicalities

- part of my BasisKwalificatie Onderwijs (BKO) education
- final grade consists of 50-50:
  - weekly homework, to be graded
  - final exam in week of 31/3/14 - 4/4/14
- details on course homepage: http://homepages.cwi.nl/~schaffne/courses/inftheory/2014/

Expectations

We expect from you

- be on time
- code of honor (do not cheat)
- ask questions!

Expectations

We expect from you

- be on time
- code of honor (do not cheat)
- ask questions!

You can expect from us

- be on time
- make clear what goals are
- listen to you and respond to email requests
- keep website up to date

Questions ?

What is communication?

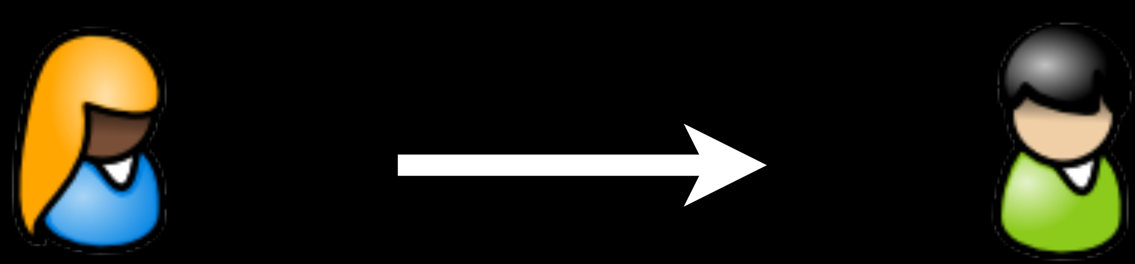
What is communication?

“The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.” - C.E. Shannon, 1948

What is communication?

“The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.” - C.E. Shannon, 1948

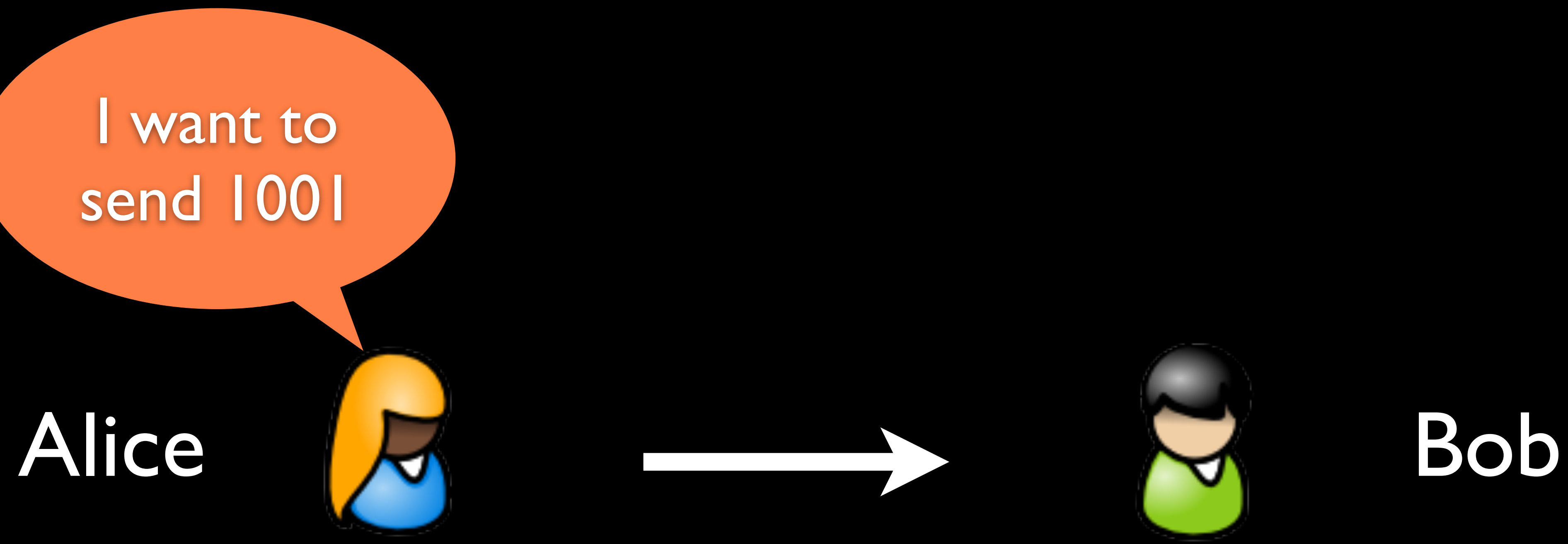
Alice



Bob

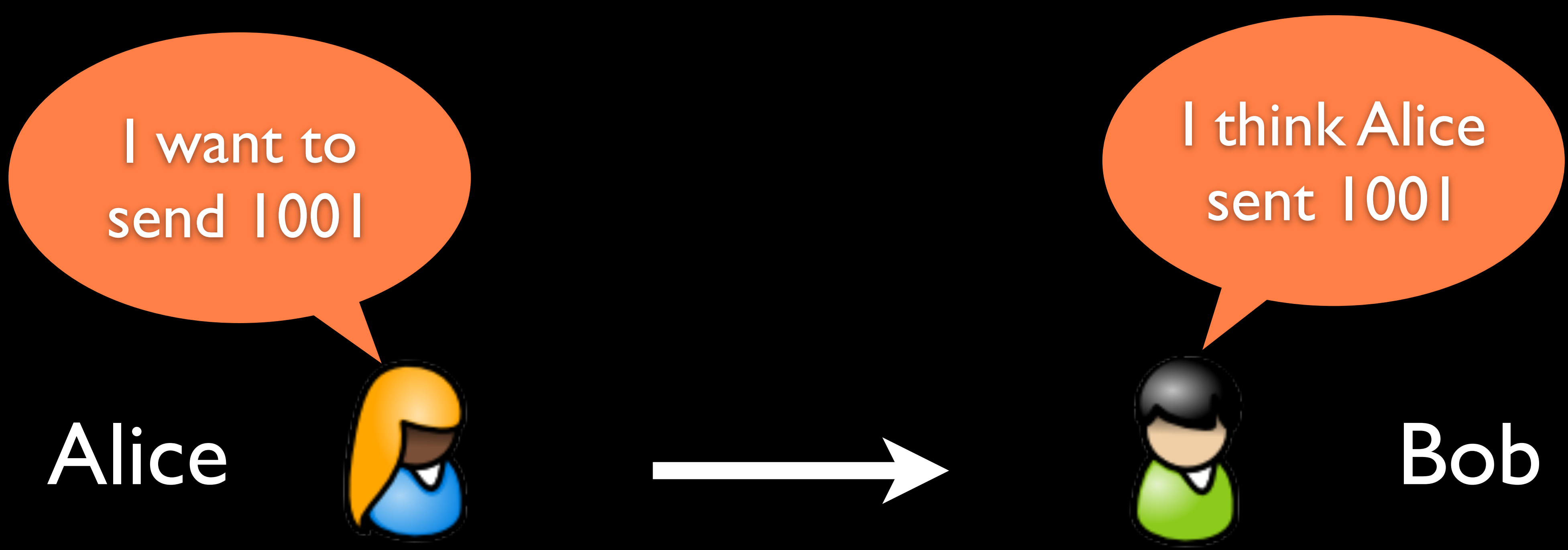
What is communication?

“The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.” - C.E. Shannon, 1948

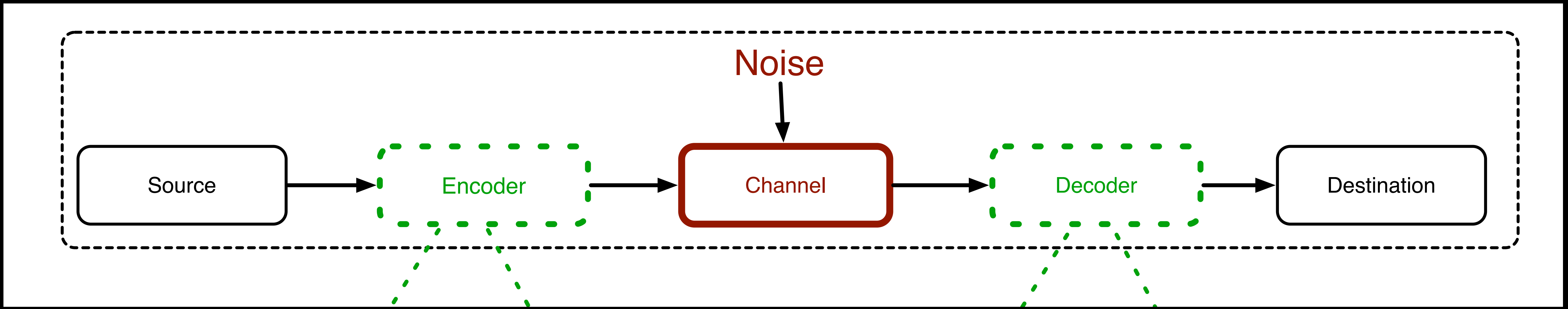


What is communication?

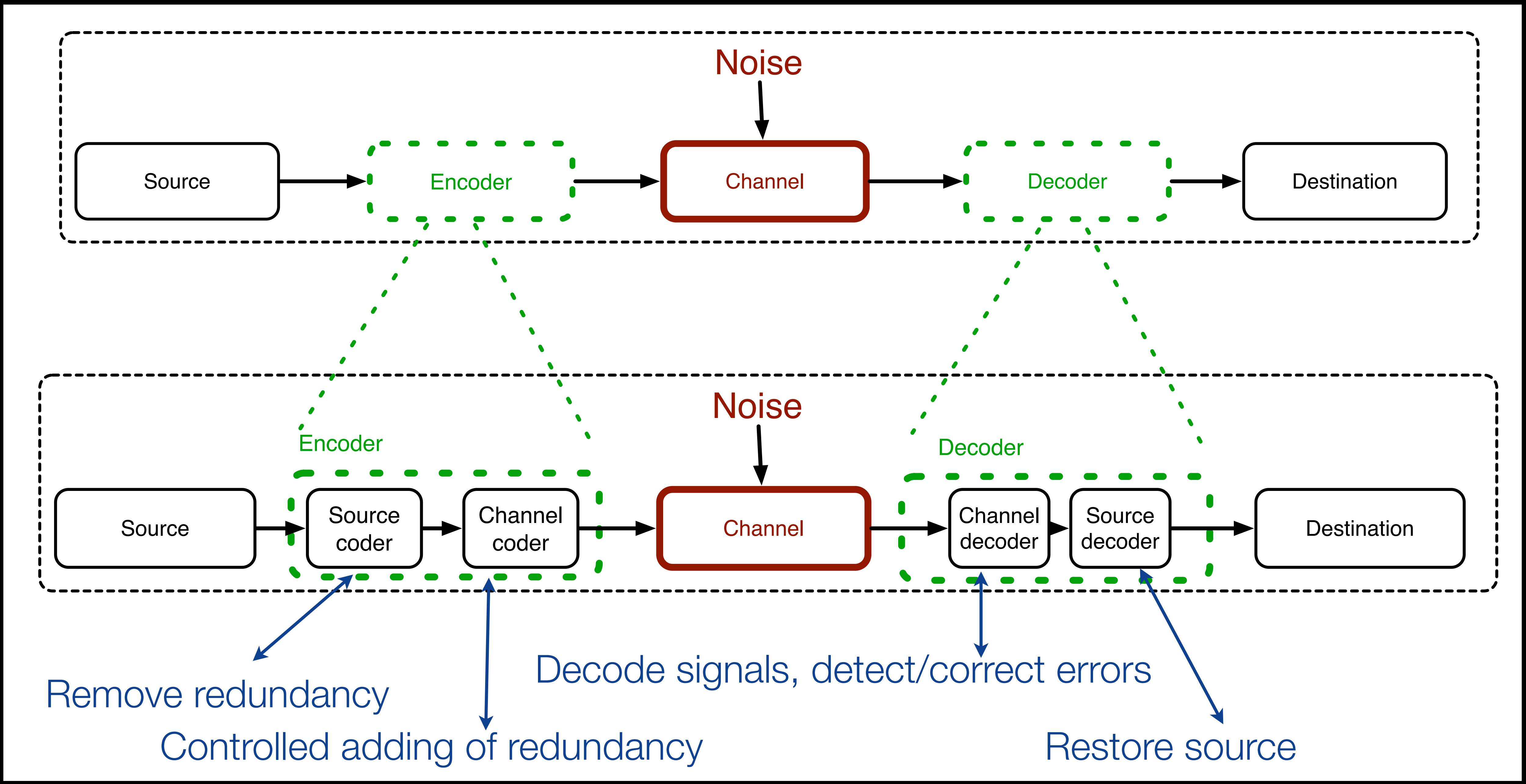
"The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point." - C.E. Shannon, 1948



Generic communication block diagram



Generic communication block diagram

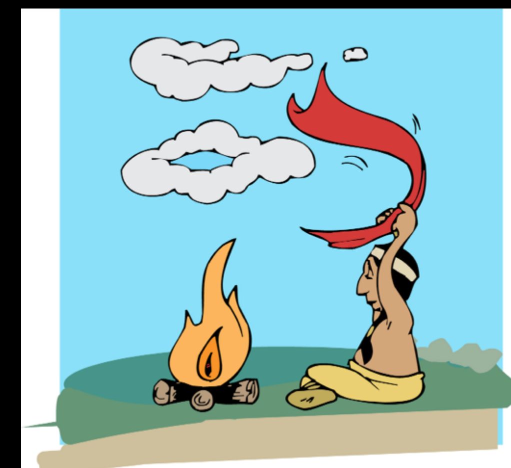


History of (wireless) communication

- Smoke signals

History of (wireless) communication

- Smoke signals
- 1861: Maxwell's equations

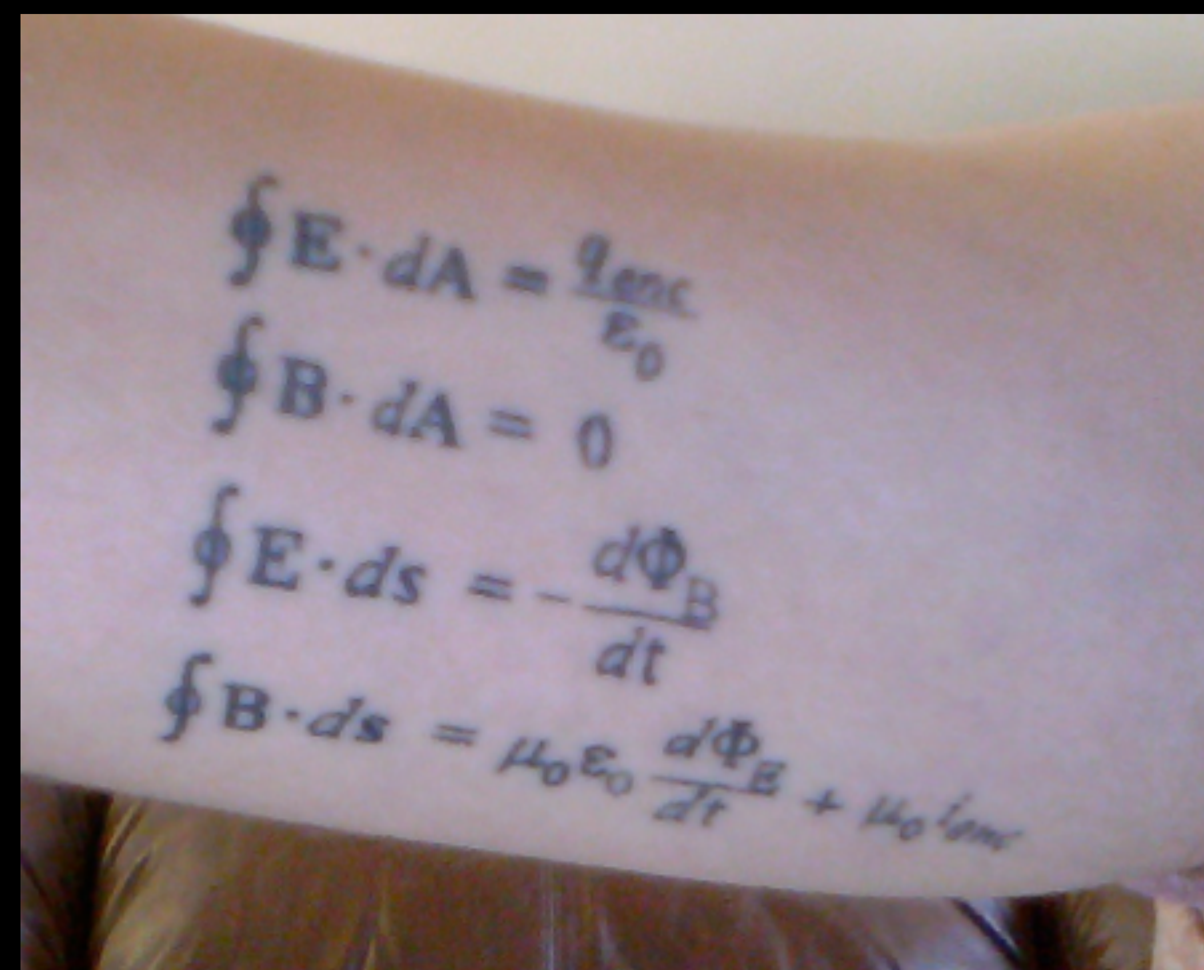


$$\oint \mathbf{E}\cdot d\mathbf{A} = \frac{q_{enc}}{\varepsilon_0}$$

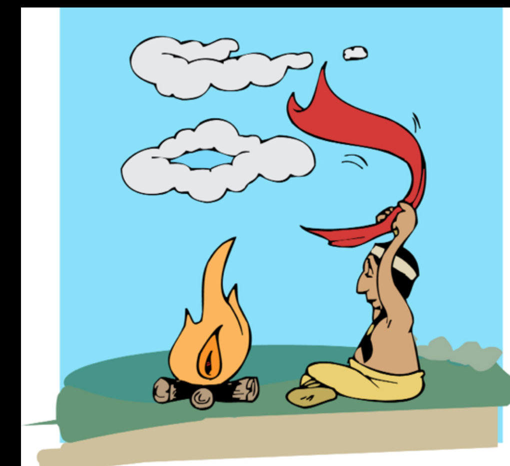
$$\oint \mathbf{B}\cdot d\mathbf{A} = 0$$

$$\oint \mathbf{E}\cdot d\mathbf{s} = -\frac{d\Phi_B}{dt}$$

$$\oint \mathbf{B}\cdot d\mathbf{s} = \mu_0\varepsilon_0\frac{d\Phi_E}{dt} + \mu_0 i_{enc}$$



History of (wireless) communication



$$\oint \mathbf{E}\cdot d\mathbf{A} = \frac{q_{enc}}{\varepsilon_0}$$

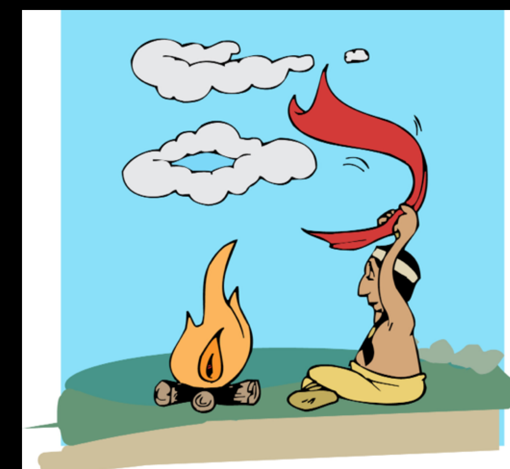
$$\oint \mathbf{B}\cdot d\mathbf{A} = 0$$

$$\oint \mathbf{E}\cdot d\mathbf{s} = -\frac{d\Phi_B}{dt}$$

$$\oint \mathbf{B}\cdot d\mathbf{s} = \mu_0\varepsilon_0\frac{d\Phi_E}{dt} + \mu_0 i_{enc}$$

- Smoke signals
- 1861: Maxwell's equations
- 1900: Guglielmo Marconi demonstrates wireless telegraph

History of (wireless) communication



$$\oint \mathbf{E}\cdot d\mathbf{A} = \frac{q_{enc}}{\varepsilon_0}$$
$$\oint \mathbf{B}\cdot d\mathbf{A} = 0$$
$$\oint \mathbf{E}\cdot d\mathbf{s} = -\frac{d\Phi_B}{dt}$$
$$\oint \mathbf{B}\cdot d\mathbf{s} = \mu_0\varepsilon_0\frac{d\Phi_E}{dt} + \mu_0 i_{enc}$$

- Smoke signals
- 1861: Maxwell's equations
- 1900: Marconi demonstrates wireless telegraph
- 1920s: Edwin Howard Armstrong demonstrates FM radio

Big Open Questions

- mostly analog
- ad-hoc engineering, tailored to each application
- is there a general methodology for designing communication systems?
- can we communicate reliably in noise?
- how fast can we communicate?

Claude Elwood Shannon

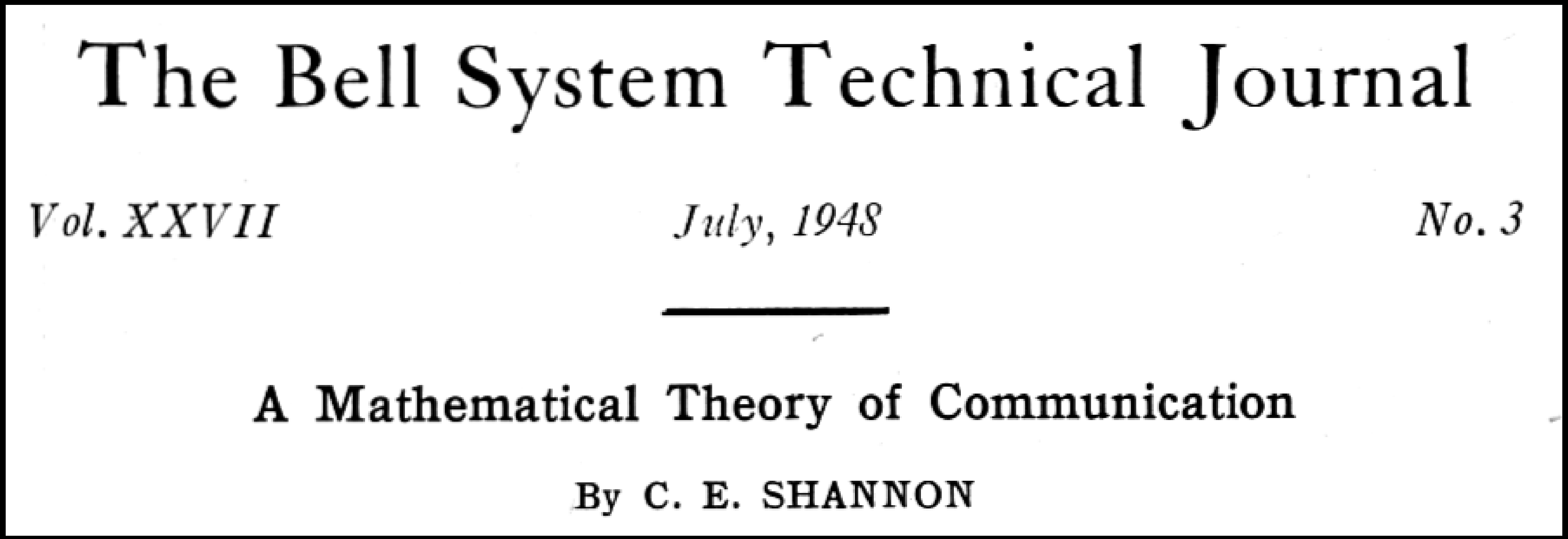
1916 - 2001

- Father of Information Theory
- Graduate of MIT 1940:
  "An Algebra for Theoretical Genetics"
- 1941-1972: Scientist at Bell Labs
- 1958: Professor at MIT:

  When he returned to MIT in 1958, he continued to threaten corridor-walkers on his unicycle, sometimes augmenting the hazard by juggling. No one was ever sure whether these activities were part of some new breakthrough or whether he just found them amusing. He worked, for example, on a motorized pogo-stick, which he claimed would mean he could abandon the unicycle so feared by his colleagues ...
- juggling, unicycling, chess
- ultimate machine

History of (wireless) communication

- BITS !
- arguably, first to really define and use "bits"
- *"He's one of the great men of the century. Without him, none of the things we know today would exist. The whole digital revolution started with him."* -Neil Sloane, AT&T Fellow


The Bell System Technical Journal

Vol. XXVII *July, 1948* *No. 3*

A Mathematical Theory of Communication

By C. E. SHANNON

- Introduced a new field: Information Theory

What is communication?

What is information?

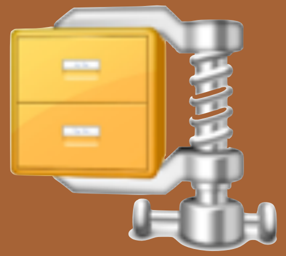
How much can we compress information?

How fast can we communicate?

Main Contributions of Inf Theory

Source coding

- source = random variable

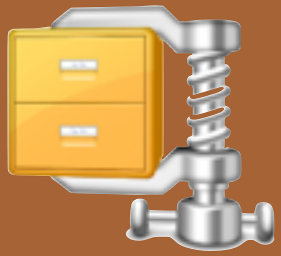


- ultimate data compression limit is the source's **entropy H**

Main Contributions of Inf Theory

Source coding

- source = random variable
- ultimate data compression limit is the source's **entropy H**



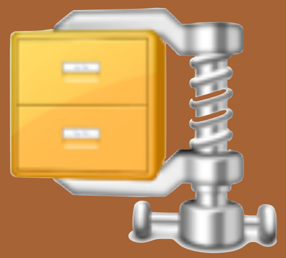
Channel coding

- channel = conditional distributions
- ultimate transmission rate is the **channel capacity C**

Main Contributions of Inf Theory

Source coding

- source = random variable



- ultimate data compression limit is the source's **entropy H**

Channel coding

- channel = conditional distributions
- ultimate transmission rate is the **channel capacity C**

Reliable communication possible $\Leftrightarrow$ H < C

Reactions to This Theory

- Engineers in disbelief
- stuck in analogue world

How to approach the predicted limits?

Shannon says: can transmit at rates up to say 4Mbps over a certain channel without error. How to do it?

It Took 50 Years To Do It

How to approach the predicted limits?

review article by [Costello Forney 2006]

It Took 50 Years To Do It

- 50's: algebraic codes

How to approach the predicted limits?

review article by [Costello Forney 2006]

It Took 50 Years To Do It

- 50's: algebraic codes
- 60's 70's: convolutional codes

How to approach the predicted limits?

review article by [Costello Forney 2006]

It Took 50 Years To Do It

- 50‘s: algebraic codes
- 60‘s 70‘s: convolutional codes
- 80‘s: iterative codes (LDPC, turbo codes)

How to approach the predicted limits?

review article by [Costello Forney 2006]

It Took 50 Years To Do It

- 50's: algebraic codes
- 60's 70's: convolutional codes
- 80's: iterative codes (LDPC, turbo codes)
- 2009: polar codes

How to approach the predicted limits?

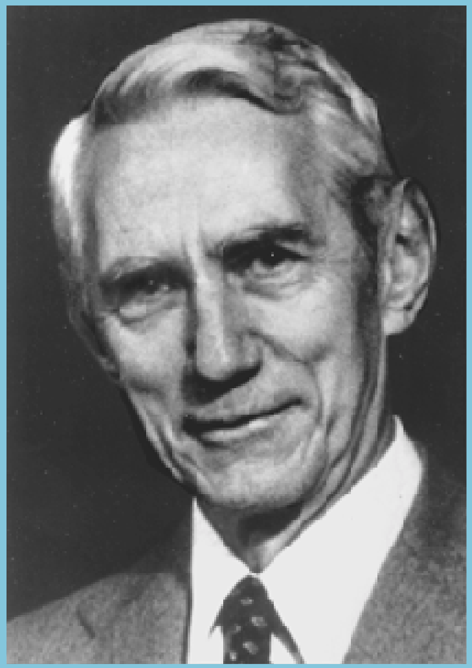
review article by [Costello Forney 2006]

It Took 50 Years To Do It

- 50's: algebraic codes
- 60's 70's: convolutional codes
- 80's: iterative codes (LDPC, turbo codes)
- 2009: polar codes

How to approach the predicted limits?

review article by [Costello Forney 2006]



Claude Shannon — Born on the planet Earth (Sol III) in the year 1916 A.D. Generally regarded as the father of the Information Age, he formulated the notion of channel capacity in 1948 A.D. Within **several decades**, mathematicians and engineers had devised practical ways to communicate reliably at data rates within 1% of the Shannon limit . . .

Encyclopedia Galactica, 166th ed.

Robert J. McEliece, Shannon Lecture 2004

Applications

- Communication Theory
- Computer Science (e.g. in cryptography)
- Physics (thermodynamics)
- Philosophy of Science (Occam's Razor)
- Economics (investments)
- Biology (genetics, bio-informatics)

Topics Overview

- Entropy and Mutual Information
- Entropy Diagrams
- Perfectly Secure Encryption
- Data Compression
- Coding Theory
- Channel-Coding Theorem
- Guest Lecture: Zero-Error Information Theory
- Randomness Extraction
- Privacy Amplification

Questions ?