Math 525 – Algebraic Coding Theory, Fall 2020

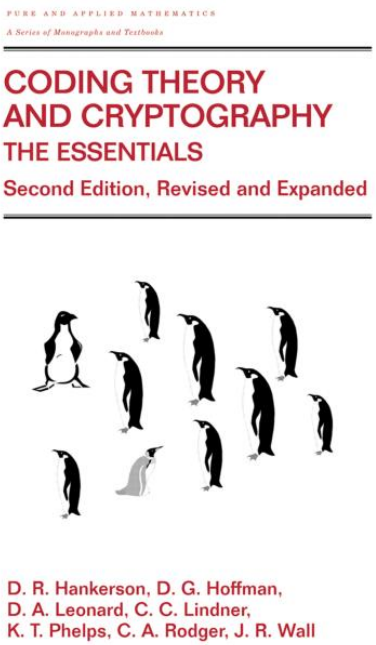
J. Carmelo Interlando
Dept. of Mathematics & Statistics
San Diego State University

Basic Course Information

- Class Website (Canvas): https://sdsu.instructure.com
- Make sure to read the syllabus posted on the class website: It contains important information not being covered during this presentation.
- Instructor's e-mail: interlan@sdsu.edu
- Classes Days/Time: MWF/12:00 – 12:50 PM.
- Office Hours: Thursdays, 3:30 – 5:00 PM or by appointment.
- Prerequisite:
  1. A solid knowledge of both MATH 254 – Introduction to Linear Algebra (excluding eigenvalues and related topics) and polynomial arithmetic.
  2. MATH 245 – Discrete Mathematics (counting, combinations, and probability).
- Assessment: Quizzes, three midterms, and final exam. See syllabus for dates and weights.

Basic Course Information (Cont'd.)

Textbook:



What is this course about?

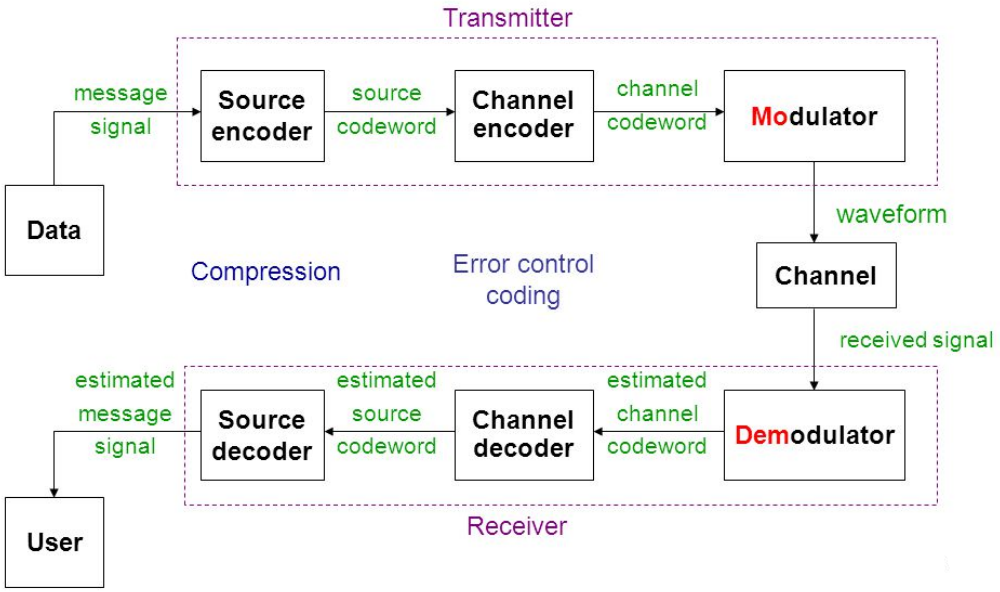
The course is not about:

- "Coding" in the sense of programming computers;
- Studying methods for shortening messages (e.g., Morse code, data compression algorithms);
- Creating secret versions of a message (cryptography).

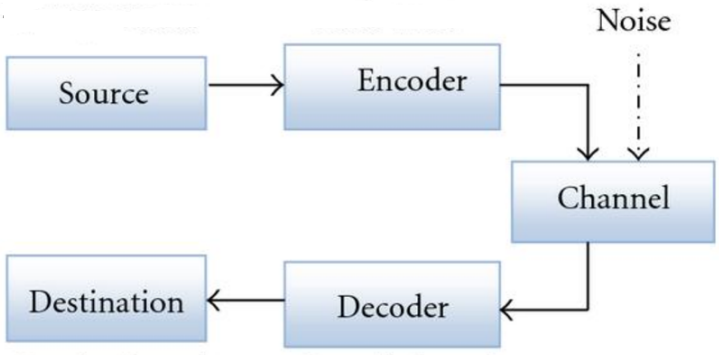
* * *

The course IS about methods for creating versions of a message so that it can be recovered after being corrupted. The codes studied in the course are called "error-correcting codes." The course could have been titled "error control coding."

Motivation for Coding Theory: Communication Systems



A Simplified Communication System Model



- Think of the source output (message) as a long string of binary digits 0100101011100 . . .
- The channel encoder *adds redundancy* to the messages produced by the source.
- The outputs of the channel encoder (codewords) are then transmitted across the communication channel, which in turn corrupts the codewords.
- Thanks to redundancy, the corrupted codewords (leaving the channel and entering the decoder) can be transformed back into their original versions by the decoder.
- The decoder then delivers the information it recovered to the receiver (destination).

Main Objective of an Error-Correcting Code:

To correct the errors introduced by noise during the transmission of data. This is done by adding redundancy to the information in a controlled manner.

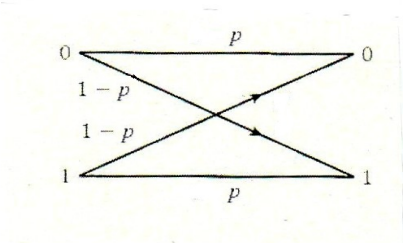
Current Uses of Codes:

Virtually any modern communication and digital storage system uses coding for error control. Among them,

- Deep space networks;
- Cellular or mobile networks;
- CDs, DVDs, and Blu-ray Discs;
- Certain cryptographic systems.

A Simple-Minded Example of Coding

Suppose we must use a channel that exhibits the following behavior:



The above picture says that:

- Whenever the digit 0 is transmitted, there is a probability p that it will be correctly received – and a probability $1 - p$ that it will be incorrectly received.
- Whenever the digit 1 is transmitted, there is a probability p that it will be correctly received – and a probability $1 - p$ that it will be incorrectly received.

In this example we will assume $p = 0.9$ and $q = 1 - p = 0.1$.

A Simple-Minded Example of Coding (Cont'd.)

Encoding rule: add two extra digits (repeating the information) during each transmission. Thus,

- 0 is encoded as 000.
- 1 is encoded as 111.

Decoding rule (we will use a majority vote):

- If any of $000, 100, 010, 001$ is received, it is decoded as 000.
- If any of $111, 110, 011, 101$ is received, it is decoded as 111.

Let us now calculate the new probability of error. An error occurs if and only if either one of the following events occurs:

E1) 000 is transmitted and any of 111, 110, 101, 011 is received.

E2) 111 is transmitted and any of 000, 100, 010, 001 is received.

We have: $\Pr(\mathrm{E1}) = q^3 + 3q^2p = 0.028$. Similarly, $\Pr(\mathrm{E2}) = 0.028$.

A Simple-Minded Example of Coding (Cont'd.)

- Assuming 0s and 1s are transmitted with an equal frequency, we see that the proposed coding scheme reduces the original probability of error to almost $1/4$ of the original.
- The system became more reliable, but at the cost of transmitting a smaller amount of information per unit of time. The system is now 3 times slower.

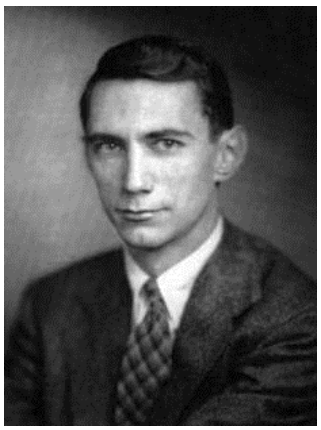
The challenge faced by a coding theorist is to devise a scheme (encoder/decoder) that provides:

1. Correction of errors introduced in the channel;
2. Fast encoding/decoding;
3. Maximum transfer of information per unit of time.

The above objectives are generally conflicting, but this is exactly what pushed the development of the theory.

Claude Shannon and the Birth of Coding Theory

- Up until 1947, it was widely accepted in the telecommunications community that either the transmission rate/bandwidth or the probability of error would have to be sacrificed in favor of the other.
- Then in 1948...



Claude Shannon, 1916–2001

- In a seminal paper published in 1948, *A Mathematical Theory of Communication*, Claude Shannon debunked that assumption by showing that if we transmit information at a rate below a number that he called *channel capacity*, then it is possible to devise a coding/decoding scheme with an error probability as small as one wishes (even though not zero).
- Shannon's result revolutionized the field of communications and marked the birth of information and coding theory.
- Although the result was a major breakthrough, it came in the form of an "existential theorem," that is, one that assures the existence of an efficient solution (to the noise problem) but does not indicate how to find it.
- As a consequence, it ignited an explosion of research by mathematicians and engineers on finding efficient coding schemes for various communication channels.
- Although significant developments have been achieved in the past 70+ years, the field of coding theory remains very active and has ramifications to other areas (e.g., mathematics, cryptology, biology, etc.).