Course overview

- **Lectures:**
  Michael Lentmaier, michael.lentmaier@eit.lth.se, E:2375
  Mondays 13.15 – 15.00 and Tuesdays 8.15 – 10.00

- **Seminars:**
  Saeedeh Moloudi, saeedeh.moloudi@eit.lth.se
  Wednesdays 15.15 – 17.00

- **Problem solving:**
  Saeedeh Moloudi
  Fridays 10.15 – 12.00

All these events take place in room E:3139.

- **Secretary:**
  Doris Glöck, E:3152h

- **Web:** http://www.eit.lth.se/kurs/EDI042

Projects:
- Two Matlab projects to solve at home
- Week 3–4: decoding of convolutional codes
- Week 5–6: iterative decoding
- Results to be handed in about two weeks after handout
- May be done in groups of two

Final exam:
- Written exam
- Tuesday, January 13, 14.00 – 19.00
- Open book exam:
  you are allowed to bring books and notes with you
- Oral exam per request (only grade 3 or fail)
Recommended literature

- Lecture slides and some other material will be made available during the course on the course webpage or as handouts.
- The course does not strictly follow any book, but if you are interested in additional reading the following books are recommended:


Outline

1. Course Information
2. Introduction
3. History of coding
4. The channel capacity limit
5. Content of the course
6. Connection to other fields

What is error control coding?

The term coding is used in different contexts:

- **Cryptography:**
  encoding (encryption) of messages into an unreadable cyphertext
- **Source coding:**
  compression of data, either lossless (e.g., ZIP, FLAC) or lossy (e.g., JPG, MP3)
- **Error control coding:**
  reliable transmission over unreliable channels

Error control coding is also called channel coding or forward error correction (FEC).

Communication System Model

**Communication:** transmission of data from a source to a sink

While the source encoder removes redundant parts of the data, the channel encoder creates redundancy in a controlled way.
Communication System Model

The source and the sink of the transmission can be separated
- in space
- in time
- in space and time

Examples of physical channels:
- wireless link: radio or free-space optical
- wire or optical fibre
- hard disk (magnetic, flash), CD, DVD (optical)

Modulation: conversion of digital signal to waveforms that are suitable for transmission over the physical channel
Channel coding: protection of the information to enable reliable transmission

Application examples

Coding for audio compact disc (CD):
- protection against dirt and scratches on surface
- Reed-Solomon codes are used for error detection and error correction

Coding in mobile communications:
- fading leads to burst errors of several hundreds of bits
- GSM system uses convolutional codes with interleaving
- UMTS / LTE: more modern turbo codes with iterative decoding
- WiFi: low-density parity-check (LDPC) codes

Coding in deep space communications:
- Voyager mission to Jupiter, Saturn, Uranus, and Neptune
- concatenation of Reed-Solomon codes and convolutional codes
- Modern CCSDS standard: LDPC codes (Consultative Committee for Space Data Systems)

Why is error correction possible?

Example

“Education is what remains after one has forgotten what one has learned in school.”

Albert Einstein

- Despite of 11 erroneous letters the text in this example can still be well understood
- Language contains redundancy which allows the reader to decode the errors
- Shannon showed that English prose has a redundancy of more than 50%

Application examples

2D Barcodes:
- Quick response codes (QR codes) use Reed-Solomon error correction
- different levels of error protection are possible

Data centers: (Google, DropBox, etc.)
- storage of massive data is currently a very hot topic
- efficient handling of failures is required
  → on the fly replacement of damaged hard disks
- how can the data be efficiently reproduced?
  → error control coding over several disks
From error detection to error correction

Detection of an error can be achieved by simple addition of a parity bit $x_n = \sum_{i=1}^{n-1} x_i$; (addition is carried out modulo-2)

$$1010010 \rightarrow 1010010$$

A single error can be detected by $\sum_{i=1}^{n} x_i \neq 0$.

An extension to higher order fields (non-binary numbers) is possible.

Hamming, 1947

“Damn it, if the machine can detect an error, why can’t it locate the position of the error and correct it?”

Hamming's idea:
use several parity-checks simultaneously

$p_1 = u_1 + u_2 + u_3$
$p_2 = u_1 + u_3 + u_4$
$p_3 = u_2 + u_3 + u_4$

Hamming codes are able to correct arbitrary single errors.

An experiment:

1. **Source**: picks one of 16 possible messages
   - Message | Codeword
   - 0000 | 0000000
   - 0001 | 1101001
   - 0010 | 0101010
   - 0011 | 1000111
   - 0100 | 1001100
   - 0101 | 0100101
   - 0110 | 1100110
   - 0111 | 0001111
   - 1000 | 1110000
   - 1001 | 0011001
   - 1010 | 1011010
   - 1011 | 0110011
   - 1100 | 0111100
   - 1101 | 1010101
   - 1110 | 0010110
   - 1111 | 1111111

Assume that the following vector is received:

- 1001110

Which message was transmitted?

Outline

1. **Course Information**
2. **Introduction**
3. **History of coding**
4. **The channel capacity limit**
5. **Content of the course**
6. **Connection to other fields**
History of coding theory (selection)

1948 Shannon: foundation of information theory
1949 Golay: first paper on coding
1950 Hamming: publishes his codes (known before 1948)
1954 Elias: product codes
1954 Reed-Muller codes
1955 Elias: convolutional codes
1960 Reed Solomon codes / BCH codes
1962 Gallager: LDPC codes
1967 Viterbi algorithm
1969 Berlekamp Massey algorithm
1978 Imai/Hirakawa: multilevel coded modulation
1981 Tanner: codes on graphs
1982 Ungerböck: trellis coded modulation
1993 Berrou et al: turbo codes
1999 Jimenez/Zigangirov: LDPC convolutional codes

Information theory

Shannon introduced a mathematical theory of communication that models information by means of probabilities.

Information theory

Theorem (Channel Coding Theorem)

For every code rate

\[ R < C = \max_{p(X)} I(X; Y) \]

there exists a code for which the probability of error after decoding approaches zero. Conversely, if \( R > C \), then significant distortion must occur.

- the parameter \( C \) is called channel capacity
- it represents a fundamental limit on the achievable transmission rate (bits per channel use) for reliable communication

Drawbacks:
- encoding over long sequences of information is assumed
- a constructive method for efficient encoding/decoding is not provided
Channel capacity for discrete constellations

- ASK modulation (amplitude shift keying)
- dots show uncoded transmission for given $P_b = 10^{-5}$

Coded modulation:
coding gains possible without increasing the bandwidth!

Within this course we consider binary constellations only.

The coding theory challenge

Outline of the course

Content:
- Chapter 1: Introduction
- Chapter 2: Principles of Error Control Coding
- Chapter 3: Optimal Decoding Methods
- Chapter 4: Iterative Decoding of Concatenated Codes
- Chapter 5: Reed-Solomon Codes

After this course you should understand:
- general principles of coding
- important coding schemes: binary block codes, RS codes, convolutional codes, concatenated codes
- common methods of decoding: algebraic decoding, ML/MAP decoding, iterative decoding
Connection to other fields

Detection and estimation theory (signal processing)
- Coding can be considered as a detection problem. In the linear case it has the form:
  \[ y = A \cdot x + n \]
  where \( n \) is the noise, \( y \) the observations and \( x \) the data
- Due to the discrete nature of the data, a linear detector (zero-forcer or linear MMSE) is far from optimal

Mathematical optimization
- Finding the linear least squares solution can also be casted as a linear optimization problem (linear programming)
- Problem: integer least squares is known to be NP-hard
- Solving relaxations of this problem for codes with sparse representation (e.g., LDPC codes) is currently an active area of research

Detection in communication systems
- Detectors for discrete linear models occur frequently in communication systems
  Examples: channel equalization, MIMO detection
- Methods that originate from coding can be used to solve these problems
  Examples: Viterbi equalization, sphere detection

Iterative communication receivers
- Codes on graphs and iterative decoding has gained a lot of interest in the last decades
- The success of iterative decoding has stimulated iterative processing between various different components of a communication system (turbo processing)
- Analysis tools that originated in coding are nowadays frequently used to design efficient iterative systems