Introduction to Coding Theory: a presentation

1. What are Error-Correcting Codes?

An error-correcting code is, in vague terms, a device to communicate messages in such a way that errors introduced in the communication may be, at least with high probability, detected and even corrected. More concretely, a block code assigns to each possible message (the source), which is a word of a fixed length n, written in a finite fixed alphabet, a new word (the input codeword), with length $n+t$. The extra t digits are redundant information, chosen to alow for the detection and correction.

One of the sources of inspiration behind the invention of error-correcting codes were problems with the input data in early "modern" computers (seventy years ago...). In present days, we are surrounded by them: they are in use in satellite communications but also while listening to music from a digital recording. But the structure of codes was from the beginning, identified as being related to other interesting objects (e.g. the geometry of sphere packings) and fundamental problems and soon developed into a mathematical theory.

2. Information Theory and Coding Theory

The fundamental problems mentioned in the previous paragraph were put forward, at the same time that the practical need of error-correcting codes was being identified, by Claude Shannon, who is, justifiably, considered the creator of Information Theory. He defined the mathematical models of information and communication channel and, even more important, he stated and proved the fundamental result about them.

In short, the two main purposes of codes, efficiency (simple codes with relatively small redundancy) and error detection and correction capability, are in conflict with each other. Shannon identified the ideal boundary between what is and is not achievable. The good news are that accepting a certain amount of redundancy there exist codes with arbitrarly good error correction capability. The bad news are that these codes are not known!

Shannon's Theory opened the door to the developing of a new research area in pure and applied mathematics: finding good codes, studying their properties and their decoding algorithms. From the beginning, simple ideas from Linear Algebra were the basic tool. The developing of the theory and also of the technology lead to the possibility of more sophisticated applications of concepts from Algebra and Combinatorics.

3. The Course

The main theme of this course is the theory of error-correcting codes, giving emphasis to its algebraic and combinatorial aspects, and with an introduction to information theory. The prerequisites are very modest: a basic knowledge of linear algebra and rudiments of probability theory are sufficient.

The notes, homework, exams, etc, as well as oral presentation in class, will be in English. Naturally, questions in class and solutions for homework and exams may be given in English or Portuguese (or French, if necessary).

The course is intended to depend strongly on the autonomous work of students, encouraging independent study and exploration of subjects. With this purpose, course notes will be given, whenever feasible, in advance, and as most as possible in the form of problems.
Error-correcting codes is, by its own nature, both a theoretical and practical area. In order to perform computations and experiment with concrete codes, students are encouraged to use appropriate software (Mathematica or MatLab, for example). However, this is not a course on computation; its essence is on the understanding, deduction and proof of general properties of codes and of its encoding and decoding capabilities.

4. Introduction to Coding Theory: detailed program

- Introduction: some history and motivation.
- Source Coding: alphabets, uniquely ans instantaneously decipherable codes. Rooted Trees, codes and decision problems. Kraft's inequality and McMillan Theorem.
- Probability distributions on sources: Entropy, Gibbs Lemma and Shannon's Noiseless Theorem. The concept of information.
- Channels: Conditional Entropy, Mutual Information and Capacity.
- Block Codes: Information rate and Hamming distance. Error detection and error correction. Minimal distance decoding.
- Linear Codes: generator and parity-check matrices. Syndrome decoding. Correction of erasures.
- Equivalent codes. Duality. Basic code constructions.
- Codes and Channels: Shannon's Noisy channel theorem. Good families of codes.
- Bounds on codes. MDS codes.
- Weight enumerators and MacWilliams equalities.
- Combinatorics: generating functions.
- Combinatorics: Designs and codes.
- Finite Fields.
- Polynomials over finite fields and factorization.
- Cyclic codes: polynomial representation; error trapping decoding. Burst errors.
- Cyclic Codes: Zeros and BCH bound. Decomposition of cyclic codes.
- BCH codes; Reed-Solomon codes; Peterson's algorithm. GCD decoding algorithm.
- Algebraic constructions: Subfield and Trace codes. Delsarte's Theorem.
- Concatenation of codes.
- Convolutional Codes: canonical generators. Viterbi's algorithm.