UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

# SYLLABUS DEL CORSO

## Teoria dell'Informazione e Codici Correttori di Errori

**2627-1-F4002Q033**

### Aims

In line with the aims of the CdS, the course will provide students the knowhow necessary to deal with transmission of information via noicy channels, in order to analyze optimal error-correcting and -detecting procedures. Time permitting some rudiments of programming languages as Magma and Gap will be imparted. These tools serve to emphasize sperimental aspects of mathematical discovery. We will also impart the necessary skills to comprehend and analyze the main technical and proof methods.

Those will be tested via problem solving and resolutionef exercises related to the contents of the course.

1. Knowledge and understanding
   Students will acquire fundamental knowledge of the basic principles of error-correcting codes, including encoding, decoding, Hamming distance, linear codes, cyclic codes, and error-correction properties. This knowledge will be based on textbooks and teaching materials and will provide a foundation for more advanced studies.

2. Applying knowledge and understanding
   Students will be able to apply the concepts learned to analyze and design basic coding and decoding schemes in real or simulated contexts, recognizing the features of different codes and their applicability in digital communications and information systems.

3. Making judgements
   The course will develop students' ability to critically evaluate the efficiency and suitability of different error-correcting codes, to choose appropriate methods for specific problems, and to interpret results using both theoretical and computational tools.

4. Communication skills
   Students will learn to clearly and accurately communicate concepts from coding theory, using appropriate technical terminology, both in written and oral form, including in collaborative and interdisciplinary settings.

5. Learning skills
   The course will encourage autonomous learning by providing the tools to independently explore related topics, solve complex exercises, and prepare for exams or further study in applied mathematics or theoretical computer science.

## Contents

Information Theory, messages transmission, error probability, entropy, Shannon's Theorem, symmetric channel, Error-correcting codes, alphabet, finite fields, linear codes, Hamming codes, cyclic codes, Reed-Solomon and Reed-Muller codes, Weight preserving maps, MacWilliams' Theorems, Invariant Theory of Finite Groups.

## Detailed program

1. Information Theory, messages transmission, noisy channels, error probability, entropy, Shannon's Theorem, symmetric channel.
2. Error-correcting codes, alphabet, finite fields, linear codes, Hamming codes, cyclic codes, Reed-Solomon and Reed-Muller codes.
3. Upper and lower Bounds, Sphere Packing, Gilbert-Varshamov, Perfect codes and their classification.
4. Weight preserving maps, MacWilliams' Theorem, Monomial maps, Wilson Theorem.
5. Weight enumerator polynomials, MacWilliams' Theorem, self-dual codes, isotropic vectors, Witt Theorem,.
6. Invariant Theory of Finite Groups, primary and secondary invariants, Cohen-Macaulay rings, groups generated by pseudo-reflection, Shephard-Todd Theorem.

## Prerequisites

Algebra I and II, Linear Algebra, Group Theory, Finite Field Theory, Elementary notions of Thermodynamics and Probability.

## Teaching form

The course includes lectures in didactic delivery mode (DE), devoted to definitions, theoretical results, proofs and examples, together with exercise/discussion sessions in interactive didactic mode (DI), aimed at applying the theoretical tools to examples, model analysis and problem solving.

According to the present dispositions lectures can be attended either in presence or remotely; in any case the lectures will be videorecorded and made available on the e-learning platform.

## Textbook and teaching resource

**Textbooks:

- Hall, Notes on Coding Theory, 2005
- Tablet taken notes available on this platform.
- LaTeX Notes in pdf format available on this platform.

**Further Readings:**

- Huffman and Pless, Fundamentals of error-correcting codes, 2010
- MacWilliams and Sloane, The Theory of Error-Correcting Codes, 1977
- Smith, Polynomial invariants of finite groups, 1995

## Semester

Second semester

## Assessment method

The exam consists of an oral enquiry assessing both the student's acquisition of the course contents and her/his capabilities of analyzing and solving problems.

According to the actual dispositions the exam will be in presence unless the candidate belongs to one of the categories listed in the previously mentioned document. She/he must connect via webex exploiting a link reported on the e-learning page of the course.

Mark range: 18-30/30.

## Office hours

By appointment.

## Sustainable Development Goals

QUALITY EDUCATION