Algebraic and analytical methods in Coding Theory

Simone Costa and Stefano Della Fiore

1st Semester, 2025

E-mail: simone.costa@unibs.it Web: https://simone-costa.unibs.it
E-mail: stefano.dellafiore@unibs.it Web: https://stefano-dellafiore.unibs.it

Course Description

This course investigates key asymptotic problems in Information Theory through the lens of extremal combinatorics, probabilistic techniques, and analytical methods. Particular attention is given to the study of code sizes and their relationship with zero-error transmission capacity which is a concept introduced by Shannon in 1956. Students will explore how combinatorial constructions and probabilistic reasoning can be employed to derive bounds and design principles for various classes of codes, with a focus on hash codes and codes for additive channels.

In the first part of the course, we examine (b,k)-hash codes, particularly when $b = k = 3$. We study the known bounds on the asymptotic rate of these codes, largely using probabilistic tools such as the expected value method, in combination with analytical reasoning. These methods help illustrate the fundamental limits on the size of such codes under various structural constraints.

In the second part, we shift attention to codes relevant to additive channels, which are connected to the well-known Erdős–Moser sum-distinct problem. This classical problem in number theory and extremal combinatorics serves as a gateway to more sophisticated tools. Through it, we explore probabilistic techniques including the second-moment method and the Lovász Local Lemma. We also incorporate analytical tools, such as isoperimetric inequalities, and algebraic approaches such as the Combinatorial Nullstellensatz, to analyze and construct codes with desirable properties.

We also review current open problems and active research directions, encouraging students to identify potential approaches for original research.

Outcomes

By the end of the course, students will:

- Understand key connections between extremal combinatorics and information theory.
- Be able to apply probabilistic, analytical, and algebraic methods to derive bounds on code sizes.

- Analyze the zero-error capacity of discrete memoryless channels using combinatorial techniques.
- Gain exposure to open problems and recent advances in zero-error information theory.

Preferred Prerequisites

Basics in probability theory, combinatorics and information theory. Familiarity with discrete mathematics and algebraic methods will be helpful.

Evaluation

Evaluation will be based on an oral presentation on a selected topic or open problem.

Schedule

The course consists of weekly 5/6-hour lectures over 5 weeks for a total of 27 hours. Each lecture will combine theoretical exposition with detailed examples. Students are encouraged to actively participate in discussions.

The lectures will be held in Aula Seminari at the department of Mathematics in the following days:

- 09/10/2025 (14:00-17:00)
- 10/10/2025 (10:00-12:00)
- 16/10/2025 (14:00-17:00)
- 17/10/2025 (10:00-12:00)
- 20/10/2025 (15:00-18:00)
- 21/10/2025 (15:00-17:00)
- 30/10/2025 (09:00-12:00)
- 31/10/2025 (09:00-12:00)
- 06/11/2025 (09:00-12:00)
- 07/11/2025 (09:00-12:00)

Literature

- Claude Shannon, *The zero error capacity of a noisy channel*, IRE Transactions on Information Theory, 1956.
- Imre Csiszár and János Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Cambridge University Press, 2011.

- Noga Alon and Joel H. Spencer. *The probabilistic method*, John Wiley & Sons, 2016.
- Stefano Della Fiore, Simone Costa and Marco Dalai, *Improved bounds for (b,k)-hashing*, IEEE Transactions on Information Theory, 2022.
- Simone Costa, Marco Dalai and Stefano Della Fiore, *Variations on the Erdős distinct-sums problem*, Discrete Applied Mathematics, 2023.