ENEE 739C: Advanced Topics in Signal Processing: Coding Theory

Course Goals:

To develop in-depth understanding of the problems of modern coding theory and prepare students for research work in the area of error-correcting codes. The course will offer a unified view of the goals, methods and results of coding theory in a variety of communication scenarios in classical and quantum communication channels. The course will stress the trade-off between performance of code families and complexity of their implementation. We will discuss several topics in the forefront of the present-day research including LDPC codes and iterative decoding, list decoding of algebraic codes, expander codes, and (time permitting) quantum codes.

Course Prerequisite(s):

Linear Algebra (MATH 461 or equivalent), Probability Theory (ENEE 620 or equivalent), Error-Correcting Codes (ENEE 626). Information Theory (ENEE627) and Discrete Structures (ENEE 450) are helpful but not required: concepts from those courses will be reviewed as needed.

Topics Prerequisite(s):

Finite fields, their representations and operations, comfortable operation with fundamentals of mathematical analysis (limits, continuity). Discrete probability distributions, moments and the Chebyshev inequality, conditional probability and independence. Good understanding of basic linear algebra: bases, dimension, matrices.

Textbook(s)

We will not follow any particular book.

Reference(s):

References to book sections and journal papers will be posted on the course pages.

Standard references for coding theory include

1. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier/North Holland, Amsterdam, 1977 (3rd printing 1991).
2. R. J. McEliece, *The Theory of Information and Coding*, 2nd ed., Cambridge University Press, Cambridge, 2002.

3. V. Pless, *Introduction to the theory of error correcting codes*, 3rd edition. John Wiley & Sons, Inc., New York, 1998
4. I. Csiszar and J. Korner, *Information Theory. Coding Theorems for Discrete Memoryless Channel*, Academic Press, Inc., New York-London, 1981.
5. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley and Sons, 1991.

Core Topics:

- **Average properties of code ensembles.** Properties of typical binary and q-ary codes.
- **Decoding of codes:** Bounded distance decoding, list decoding, maximum likelihood decoding, error detection. Performance of codes under various decoding procedures.
- **Error exponents** for discrete memoryless channels. Gallager bounds for the binary symmetric channel, geometric view of error bounds. Error exponents for general discrete memoryless channels (via the method of types).
- **List decoding** of Reed-Solomon codes: The Guruswami-Sudan algorithm.
- **Algorithmic issues of coding theory:** Constructive families of asymptotically good codes. Concatenated codes and their decoding.
- **Attaining channel capacity:** Serial and parallel concatenations: LDPC and turbo codes. Iterative decoding, belief propagation, message passing algorithms.
- **Linear-time decodable code families:** Expander codes.
- **Impossibility results for codes:** Bassalygo-Elias bound, Johnson bound, linear programming bounds.

Optional Topics:

- **Transmitting information over a quantum channel:** Representing information by states if quantum systems. Quantum channels and noise. Quantum error-correcting codes. Motivation and constructions.
- **Cryptographic applications of coding theory:** Public-key cryptosystems. McEliece and Niederreiter cryptosystems. Secret sharing. Fingerprinting of digital data. Authentication with codes.

Course Structure:

Grading Method:

Several homework assignments and a final presentation/report on a current research topic.