

Textbook: No required Textbook.

Recommended Textbooks: *Introduction to Coding Theory*, 3rd Edition
by J. H. van Lint (Springer-Verlag (Graduate Texts in
Mathematics series), 1999)
Introduction to the Theory of Error-Correcting Codes, 3rd
Edition
by V. Pless (Wiley-Interscience, 1998)
The Theory of Error-Correcting Codes
by F.J. MacWilliams and N.J.A. Sloane (Elsevier/North-
Holland, 1977)
Theory and Practice of Error-Control Codes
by R.E. Blahut (Addison-Wesley, 1983)
Theory of Information and Coding, 2nd Edition
by R.J. McEliece (Cambridge University Press, 2002)

Prerequisite: MATH 212* or 217*.

Instructor: N. Kashyap

Evaluation:	Homework	20%
	Midterm	40%
	Project	40%

Outline:

- *Introductory Concepts* : Linear codes, minimum distance, maximum-likelihood decoding, syndrome decoding. Repetition codes, Hamming codes. Shannon's noisy-channel coding theorem.
- *Relationships between Code Parameters*: Hamming bound, Singleton bound, Gilbert-Varshamov bound, Plotkin bound, McEliece-Rodemich-Rumsey-Welch bounds. Using bounds to determine and design good codes for a given set of parameters.
- *Basic Finite Field Theory*: Definitions, prime fields, construction of prime power fields via irreducible polynomials, existence of primitive elements, minimal polynomials.
- *Algebraic Codes*: Bose-Choudhury-Hocquenghem (BCH) and Reed-Solomon Codes, and the Peterson-Gorenstein-Zierler decoding algorithm. Applications of Reed-Solomon codes in digital communications and storage. Cyclic codes as ideals of polynomial rings.
- *Convolutional Codes*: Basic definitions and overview. Algebraic representation of convolutional codes as vector spaces over the field of formal Laurent series. Shift-register realizations of convolutional encoders. Introduction to the Viterbi decoding algorithm. Overview of turbo codes.
- *Other topics to be selected from, as time permits*: Dual codes and the MacWilliams identities. Linear programming bounds. Golay codes, Reed-Muller codes, codes from designs, Goppa codes and algebraic geometry codes, expander codes, low-density parity-check (LDPC) codes.