MATH 406/806
Introduction to Coding Theory

Winter 2009

Instructor: Navin Kashyap
Office: Jeffery Hall 410
Phone: 533-6640, Email: nkashyap@mast.queensu.ca

Course Web Site: http://www.mast.queensu.ca/~math406
All assignments and important announcements will be posted here.

Lectures: Slot 4 (Tuesday 8:30, Wednesday 10:30, Friday 9:30), Jeffery 115

Pre/Corequisites: MATH 210 or 211 or 212 or 213 or 217, or equivalent.

Evaluation: Undergraduate students: HW 20%, Midterm test 30%, Final exam 50%
Graduate students: HW 25%, Midterm test 20%, Final exam 35%, Project 20%

Course Outline

- *Introductory Concepts* : Block codes, encoding and decoding, maximum-likelihood decoding, minimum-distance decoding, error detection and correction. Shannon's noisy-channel coding theorem.
- *Linear codes*: Minimum distance, generator and parity-check matrices, dual codes, standard array decoding, syndrome decoding. Repetition codes, Hamming codes.
- *Bounds on Code Parameters*: Hamming bound, Singleton bound, Gilbert-Varshamov bound, Plotkin bound. Using bounds to 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. Decoding of generalized Reed-Solomon codes. Applications of Reed-Solomon codes in digital communications and storage. Cyclic codes as ideals of polynomial rings.
- *Other topics to be selected from, as time permits*: List decoding of Reed-Solomon codes, Golay codes, Reed-Muller codes, Goppa codes and algebraic geometry codes, convolutional codes, turbo codes, expander codes, low-density parity-check (LDPC) codes.

References:
R.M. Roth, *Introduction to Coding Theory*, Cambridge University Press, 2006.
W.C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes*, Cambridge University Press, 2003.
J.H. van Lint, *Introduction to Coding Theory*, 3rd ed., Springer-Verlag (Graduate Texts in Mathematics series), 1999.
F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier/North-Holland, 1977.
R.E. Blahut, *Theory and Practice of Error-Control Codes*, Addison-Wesley, 1983.