# Computer Science / Math   235

### *Information and Coding Theory*

**Fall 2009**

| | | |
|---|---|---|
| **Instructor**: | *Steven Lindell* | Office: Link 308 |
| | Phone: -1203 | E-mail: slindell |

**Class schedule and room**:   MWF 3:00-4:00      Link 310 (CS research lab)

**Consultation hours**:   after class; and also by appointment

**Course Description**:   Covers the mathematical theory of the transmission (sending or storing) of information. Included will be encoding and decoding techniques, both for the purposes of data compression, and for the detection and correction of errors.

**Co-requisite**:   Math 215 (linear algebra) or its equivalent.

**Text**:   *Coding and Information theory*, by Richard W. Hamming, 2nd edition, Prentice-Hall © 1986 ISBN 0131390724 (out-of-print: copies available in bookstore have been duplicated with the permission of the publisher).

**Supplement:**   (harder)   *Information and Coding theory*, by Gareth A. Jones & J. Mary Jones, Springer Verlag © 2000. [on reserve in library]

**Lecture**:   Attendance in class is expected. More than three *unexcused absences* will result in a lowered grade.

**Grading**:

| | | |
|---|---|---|
| *Participation* | 10% | (includes *attendance* and coming to *office hours*) |
| *Homework* | 30% | (see rules below) |
| *Midterm* | 20% | (one) |
| *Final Exam* | 40% | (comprehensive) |

**Rules**:   Homework will be collected about every ten days, and students are encouraged to work together on problems by sharing ideas, but *not* solutions. Both exams will be take-home, with no collaboration or help allowed.

**Comments**:   This class is not intended to be difficult, but does require concentration in dealing with the abstract mathematical concepts involved.

# Course Outline

Lectures will follow the table of contents for the text fairly closely.

**Chapters**

1.      Introduction (the signaling channel, communication versus storage, analog versus digital)

2.      Error-Detecting Codes (simple parity checks, modular arithmetic, weighted codes)

3.      Error-Correcting Codes (Hyper-dimensional cubes, Hamming code, Hamming distance)

4.      Variable-Length Codes: Huffman Codes (instantaneous decoding, Kraft inequality)

5.      Miscellaneous Codes (ergodic Markov processes, predictive run length coding)

6.      Entropy and Shannon's First Theorem (Gibbs inequality, Shannon-Fano, code extensions)

7.      The Channel and Mutual Information (binary symmetric channel, system entropies)

8.      Channel Capacity (uniformity, application to error detecting and correcting codes)

9.      Some Mathematical Preliminaries (Stirling's approximation, binomial bounds, Gamma function)

10.     Shannon's Main Theorem (the average random code)

11.     Algebraic Coding Theory (double error correction, use of shift registers)

12.     Appendix: Bandwidth and the Sample Theorem (analog bandwidth, signal to noise ratio)


**Online course information**:   Have you ever wondered how a CD can sound completely pristine, even though it is scratched?     Is it possible to discern spoken text even when the background noise is so great that the speech signal is inaudible?     How can files, especially music and pictures, be compressed to a fraction of their original size without any discernible difference?     These questions, and many more, can be answered by a fundamental mathematical theory of communication which quantifies the amount of information in a message, regardless of whether it is transmitted or stored. This quantity, known as entropy, is given by a surprisingly elegant formula with deep connections to physics. The entropy of a message (or file) determines how much it can be compressed without losing information -- the subject of information theory.     But those same messages can have their information corrupted by errors introduced in the process of communication or storage. Coding theory studies methods for detecting (and correcting) those errors, in ways that are completely transparent to the user (your cell phone uses these techniques). The crowning achievement of these theories (known as Shannon's theorem) is that both compression (removing redundancy) and correction (adding redundancy) can be achieved simultaneously! It has important applications everywhere.