CSE 522 / Math 581EB
Coding Theory

Instructors: Elchanan Mossel and Chris Umans (Microsoft Research)
Location: Padelford C401
Time: TTh 12:00 – 1:20
Office hours: TBD

This course will focus on elements of the theory of error-correcting codes and their applications to theoretical computer science.

The goals of modern coding theory are to *construct* explicit codes and establish bounds on their information rate and distance, *prove* lower bounds to explore the limits of achievable performance and *devise* efficient algorithms for encoding and decoding specific codes. To achieve these goals, coding theory draws upon combinatorics, probability, linear algebra, finite fields and algebraic geometry. In recent years there has been a significant interplay between coding theory, algorithms and computational complexity.

This course will cover the following four broad areas:

- **Constructions**. Random linear codes, Hamming, Hadamard, Reed-Solomon, Reed-Muller and Chinese Remainder Codes, various concatenated codes.
- **Bounds**. Packing bounds, Elias-Bassalygo and Johnson bounds, Fourier theory for the discrete cube and the MacWiliams identities, linear programing LP bound.
- **Algorithms**. Decoding from erasures, unique decoding, list-decoding, expander codes for linear-time encoding and decoding.
- **Applications**. Hardcore predicates, reducing worst-case hardness to average-case hardness, extractors and pseudo-random generators, other topics.

Texts:

- "A Crash Course on Coding Theory" by Madhu Sudan (MIT)
  available at `http://theory.lcs.mit.edu/~madhu/coding/course.html`

Other references:

- *Handbook of Coding Theory Vol. I, II.* Pless, Huffman and Brualdi.
- *Introduction to Coding Theory (third edition).* van Lint.
- *The Theory of Error-Correcting Codes.* MacWilliams and Sloane.

Recommended background: linear algebra (over finite fields), basic algorithms, probability and computational complexity.

Course Requirements: Each student should complete two of the following three tasks:

- produce high quality scribe notes for 1-2 lectures (depending on how many people end up taking the course)
- give a short talk on a coding theory topic selected in consultation with the instructors
- take a final exam

Exercises will be given periodically, and can be turned in for "bonus points."

Tentative schedule:

Oct 2	background, basic notation, two easy applications Noiseless Coding theorem
Oct 4	information theory background, Noisy Coding Theorem, linear codes, random linear codes.
Oct 9	finite fields background, Hamming, Hadamard and Reed-Solomon codes, singleton bound.
Oct 11	Schwartz-Zippel lemma, Reed-Muller codes and low-degree extensions, concatenated codes.
Oct 16	**no class** – FOCS
Oct 18	correcting erasures, unique decoding of Reed-Solomon and concatenated codes.
Oct 23	bounds
Oct 25	bounds
Oct 30	list-decoding
Nov 1	list-decoding
Nov 6	list-decoding
Nov 8	linear-time encodable and decodable codes
Nov 13	linear-time encodable and decodable codes
Nov 15	applications, complexity, student talks
Nov 20	applications, complexity, student talks
Nov 22	**no class** – Thanksgiving break
Nov 27	applications, complexity, student talks
Nov 29	applications, complexity, student talks
Dec 4	applications, complexity, student talks
Dec 6	applications, complexity, student talks
Dec 11	applications, complexity, student talks

Name:	Department:	Year:	Interests: