Essential Coding Theory 6.440
MIT, Fall 2011

Website: http://people.csail.mit.edu/dmoshkov/courses/codes/index.html

Place and Time: TR1:00-2:30PM, 32-144.

Instructor: Dana Moshkovitz
dmoshkov@mit.edu
http://people.csail.mit.edu/dmoshkov/
32-G606
Office hours: by appointment

Summary: This subject aims to bring students to the frontier of coding theory research in theoretical computer science. It will cover the basic theory of error correcting codes, as well as modern lines of research, such as: list decoding algorithms, expander codes, and codes with local algorithms. The subject will also cover applications of codes to theoretical computer science.

Units: 3-0-9.

Requirements: Grades will be determined roughly as follows:

- 70% project
- 30% psets

Projects: All students are expected to complete a course project. See the separate document.

Psets: There will be 3-4 psets. Psets will be due about two weeks after being assigned. Students are welcome to collaborate on psets; however, if they do so, they must write the solutions by themselves, and list the names of collaborators. After submitting the pset, every student will get the pset of one of the other students to grade. The grading scheme is:

- 2: For a correct solution, possibly with small mistakes (those should be marked clearly, but they do not change the grade).
- 1: For a partial or flawed solution.
- 0: For a missing or wrong solution.

Textbook: The course has no official textbook. We will use lecture notes by Madhu Sudan and Venkat Guruswami. See details on the course's website. The following book covers the basic theory of error correcting codes (the first part of the course):

F.J. MacWilliams and N.J.A. Sloane: *The Theory of Error-Correcting Codes*, North-Holland, 1977.

Prerequisites: Basic math (discrete math, linear algebra, probability), algorithms (6.046 or equivalent), and complexity (6.045 or 6.840 or equivalent).

Syllabus

On the website there will be a table, updated as we go, that specifies the date, title, and reading for each class. Here is a tentative syllabus:

I. The Theory of Error Correcting Codes:

- Hamming's Paper.
- Shannon's Paper.
- Converse to Shannon's theorem. Random codes. Linear codes. Gilbert-Varshamov theorems. Asymptotics of error-correcting codes.
- Singleton, Hamming, Plotkin, Elias-Bassalygo, Johnson bounds.
- Wozencraft ensemble, Reed-Solomon codes, Reed-Muller codes, Hadamard codes.
- Concatenated (Forney) codes, Justesen codes, BCH codes.
- Algebraic geometry codes (the idea without proofs).
- List-decoding.

II. Decoding Algebraic Codes:

- Decoding Reed-Solomon codes.
- List-decoding Reed-Solomon codes.
- Parvaresh-Vardy-Guruswami-Rudra codes.

III. Expander Codes:

- Gallager, Tanner, and Sipser-Spielman.
- Linear-time encodable and decodable codes.
- Linear-time list-decodability (Guruswami-Indyk).

IV. Codes with Local Algorithm:

- Local decoding, Yekhanin's construction (with improvements by Efremenko and others).
- Local testing.

V. Applications of Codes in Theoretical Computer Science:

- Computational complexity of decoding linear codes.
- Secret-sharing, hardcore predicates.
- Hardness amplification.
- PCP.