Spring 2018
Math 490 CT - Error Correcting Codes
MWF 2-2:50pm in 1 Illini Hall
Professor Iwan Duursma

We discuss the mathematical principles that allow information to be stored or transmitted reliably in the presence of errors. A variety of methods is presented that cover a wide range of current applications, including cloud storage and data transfer over networks. Results from combinatorics, graph theory and algebra will be introduced and then used to construct codes and to analyze code performance. Topics include algebraic decoding of Reed-Solomon codes, probabilistic decoding of codes on graphs, trellis decoding of convolutional codes, codes for distributed storage, multicast network coding, and belief propagation for low-density parity-check codes.

Prerequisite: linear algebra, basics of probability theory and graphs.

Possible topics:

- Reed-Solomon codes, Gallager codes
- Peterson-Gorenstein-Zierler decoder, AB method
- Sum-product algorithm on Tanner graphs
- Iterative decoding of LDPC codes
- Network coding
- Distributed storage, regenerating codes, locally repairable codes
- Entropy, discrete memoryless channel, channel capacity
- Secret sharing, wiretap channel, shifting method
- Polar codes and Reed-Muller codes
- Convolutional codes, trellis representations
- Cyclic codes, quasi-cyclic codes, Golay code
- (further topics in graduate minicourse Math 595 CT, next page)

Spring 2018
Math 595 CT – Coding Theory
MWF 3-3:50pm in 141 Altgeld Hall
Meets 12-Mar-18 / 02-May-18
Professor Iwan Duursma

The course starts with a brief introduction and discussion of selected topics from Math 490 CT. We then discuss a selection of advanced topics including coding theory applications of matroids and association schemes.

Prerequisite: linear algebra, algebra (groups and fields).

Possible topics:

- (review of selected Math 490 CT topics, previous page)
- Welch-Berlekamp and Berlekamp-Massey key equations
- Finite field extensions, subfield subcodes, BCH codes
- List decoding, folded Reed-Solomon codes
- Matroids, code duality, trellis complexity
- Multiplicative codes, secure multiparty computation
- Coset graphs, distance regular graphs, expander graphs
- Association schemes, Delsarte LP bound
- Symmetric group, Johnson schemes
- Semi-definite programming bounds
- Self-dual codes, invariant theory, stabilizer codes
- Codes over rings, integers modulo four, Frobenius rings