MATH 810 SS15 – FINAL EXAM/REPORT 9:45am, Tuesday, 5 May 2015

You are to write a ten to fifteen page report on a topic of relevance to the course. Each student is to write the paper by him or herself. Material should be collected from several sources (from the library, texts, web), and such material should be properly referenced. Web references alone do not suffice. Make sure you avoid plagiarism (claiming the work or writing of others as your own). There is also the possibility of having original research or computational work form a significant part of your project.

We should meet individually during the rest of the semester to discuss your topic (early) and your progress (later). If I am satisfied that you are making significant progress on your report, then you will be excused from the final exam. (Those who wish to have a final exam will be given some starter questions during the last week of classes and then have a 1 hour oral final with me sometime during Finals Week.)

There are many possible topics for your report. Please feel free to come up with an idea and discuss it with me. But I have provided some possible topics here. (There are many overlaps among these topics.)

Information, performance, and basic assumptions

Information theory – probabilistic work on how to measure information content

Shannon theory – proofs of Shannon's theorem and related results

Other channels – Gaussian channel, Lee metric, Euclidian and other extensions/variations of the Hamming metric, non-symmetric channels (the Z-channel)

Code performance – how well do codes actually do what they are supposed to do (probabilistic issues)

Other coding techniques

Concatenated codes – combining codes in useful ways to take advantage of the strengths of each

Convolutional codes – these and GRS codes are two classes of codes often used in practice (often concatenated together)

Lattice codes – using codes to construct lattices, modulation codes, sphere packing

Codes defined on graphs – Tanner and factor graphs, erasure codes, low density parity check codes, Turbo codes, expander graphs

Network coding

Special codes

Reed-Muller codes – highly geometric codes with interesting decoding algorithms and often used as building blocks for other codes

Preparata and Kerdock codes – good nonlinear codes with a strong geometric flavor and good decoding algorithm

Justesen codes – the first constructible class of codes that had reasonable (asymptotic) error handling ability (normalized distance bounded away from 0)

Algebraic geometry codes – powerful generalizations of GRS codes

Quadratic residue codes – powerful codes that are interesting mathematically but hard to decode in general

Lexicographic (and greedy) codes – a nice way of constructing codes with certain error correction capabilities using a form of greedy algorithm

Codes over $\mathbf{Z}_4$ (and other alphabets that are not fields)

Constrained codes – RLL, comma free

Important results and areas

Weight enumerators and the MacWilliams theorem – a strong relation between a code and its dual

Bounds on codes – not just Sphere packing, Gilbert-Varshamov, and Singleton but also Plotkin, Johnson, Elias, linear programming, etc

Compression – source coding, Barker codes, Huffman codes, Lempel-Ziv codes, $JPEG/MPEG$

Linear recurring sequences – shift register sequences, finite fields, primitive trinomials

Spectral techniques – generalizing GRS techniques, the relationship between coefficients and roots of polynomials

Classification of perfect codes (and related types of codes) – this can get into some very interesting number theory

The Golay codes – their construction, uniqueness, characterization

Constructions of perfect 1-error-correcting codes – the only case where full classification is probably not possible

Coding and combinatorics – Assmus-Mattson theorem, codes in association schemes, cyclic plane codes

Geometry – MDS codes, Greismer bound

Finite fields and number theory

Decoding

Decoding GRS codes with the Berlekamp-Massey algorithm – the favorite algorithm for implementation, and felt to be slightly more effective than Euclidean Algorithm decoding

Decoding cyclic codes – error trapping

Iterative and graphical decoding methods – sum-product algorithm, belief propogration; $LDPC$ codes – low density parity check matrics

Polar codes

Raptor codes – fast erasure correction

Trellis codes and the Viterbi algorithm – contained in the graphical methods but have been around longer and in different forms

Decoding Algebraic geometry codes using Gröbner bases

Decoding past the minimal distance – for many received words further from a codeword than $(d_{min}-1)/2$ we would still like to make good decoding guesses (GRS)

Soft decision decoding of block codes (for instance, the Golay code or GRS)

Generalized minimum distance (GMD) decoding – a general approach to soft decision decoding

Applications, related topics, and special topics

Crypotography and coding – AES

Coding and compact disks, DVD, cell phones

Deep spaces coding

Modems and modulation codes

Space-time coding – multiple antennae

Sequences and multiuser issues – PN sequences, $T/CDMA$

Coding in mobile communication – spread spectrum methods, sequences

Codes for magnetic recording, computers, – array codes, spectral nulls

Coding and computers – hash codes, CRC

Codes and games – 20 questions, football pools, Mastermind

Covering codes – covering space with balls (as opposed to packing)

Data translation, compaction codes – run length limited, prefix codes

Connections with physics – inference in statistical mechanics, Ising states, quantum coding and information theory (a type of non-commutative coding that has come up in resolving certain problems of quantum computing)

Burst error correcting – Fire codes, interleaving and product constructions

Synchronization – comma free codes

Error detection – Weight distribution, automatic retransmission request (ARQ)

Relations with signal processing