Preliminary Exam in Coding Theory

Syllabus

- Linear block codes over finite fields and rings. Syndrome decoding.
- Bounds on codes: Hamming and Singleton upper bounds, Gilbert and Varshamov lower bounds
- Cyclic codes over finite fields: minimum polynomials, roots of polynomials (zeros of a code) , factoring x^n-1, decoding algorithms for cyclic codes.
- Special codes: Hamming codes , Reed-Muller Codes, MDS codes
- BCH codes, Reed-Solomon (RS) codes, Generalized RS codes, BCH or root bound on distance, subfield subcodes.
- Decoding algorithm for BCH/RS codes from zeros of code. Berlekamp-Massey algorithm for BCH/RS decoding
- Convolutional codes: generator matrices, encoding, state diagram, Viterbi decoding.

Optional topics: Algebraic geometry codes, Z_4 codes (Kerdock etc), background results from Galois fields and rings.

Texts: Fundamentals of Error Correcting Codes by Huffman , Pless chapters 1-5,14. Optional material 12,13,15

Coding theory and Cryptography, chapters 1-6,8,9

You will be asked to choose 5 or so problems from a list of 8-10. There may be one or two problems from the list of optional topics.