Course content for MT5461, Theory of Error-Correcting Codes

Prerequisites:
Undergraduate courses on linear algebra and finite fields

Aims:
To provide an introduction to the theory of error-correcting codes employing the methods of elementary enumeration, linear algebra and finite fields.

Learning outcomes:
On completion of the course, students should:

- calculate the probability of error or the necessity of retransmission for a binary symmetric channel with given cross-over probability, with and without coding;
- prove and apply various bounds on the number of possible code words in a code of given length and minimal distance;
- use MOLSs and Hadamard matrices to construct medium-sized linear codes of certain parameters;
- reduce a linear code to standard form, finding a parity check matrix, building standard array and syndrome decoding tables, including for partial decoding;
- know/prove/apply the theorem that a cyclic code of length n over a field consists of the codewords corresponding to all multiples of any factor of x^n-1;
- understand the structure of BCH codes.

Course content:
Basic theory of coding: Words, codes, errors, t-error detection and t-error correction. The Hamming distance in the space V(n,q) of n-tuples over an alphabet of q symbols (with emphasis on (Z2)n). Probability calculations.
The main coding theory problem: Construction of small binary codes. Rate of a code. Equivalence of codes. The Hamming, Singleton, Gilbert-Varshamov and Plotkin bounds. Puncturing a code. Perfect codes. Hadamard codes and Levenshtein's Theorem. Codes based on mutually orthogonal latin squares (MOLS).
Linear codes: Linear codes as linear subspaces of V(n,q). Generator and parity check matrices, standard array and syndrome decoding. Dual of a code. Hamming codes.
Cyclic codes: Structure of GF(q) relevant to coding theory, minimal polynomial of an element of GF(q); generator polynomial, check polynomial; BCH codes, RS codes.