Error-Correcting Block Codes

30 h Lectures

Syllabus

1.Coding versus cryptography. Examples of codes in math. Pruefer and trees (1916). Hamilton and complex numbers (1837), Hamilton and quaternions (1843). System PESEL.

2. Information storage, information transfer. Block code. Alphabet, words, lengths k, n. Hamming distance, weight of a word. Noisy channels, encoding and decoding. Information transmission system. Reliability of a channel. Binary code, binary symmetric channel. Repetition code, parity code. Information rate R.

3. Efficiency of parity checking.

4. Error detecting, error correcting. Maximum likelihood decoding. Bounds due to Hamming and Singleton. Perfect codes and MDS codes.

5. Polynomials, congruence modulo a polynomial. Irreducible and primitive polynomials, Finite rings and (Galois) fields. Examples of field's extensions via linear spaces.

6. Orthogonality (in a binary space). Linear codes and dual codes. Generating matrix, parity check. The minimum distance of a linear code. Codes of Hamming and simplex codes (simplex in a real affine space).

7. Cosets and decoding, the symptom of a coset.

8. New codes from old ones. Distance colorings of a hypercube.

9. Codes of Golay. Perfect binary linear codes. Self-duality. Self-orthogonality.

10. Polynomials and cyclic codes. Generating polynomial. Euclid's (extended) algorithm. Idempotent polynomials and factorization. Mutually reciprocal polynomials and duality among cyclic codes.

11. Primitive elements in groups. Euler φ function. Minimal polynomials. Multiplicative group of a field. The structure of a finite field. Counting primitive polynomials. Counting irreducible polynomials via Moebius μ function.

12. Hamming code as a cyclic as well as a BCH code. Reed-Solomon codes.

13. Hadamard theorem, Hadamard matrices and related nonlinear codes. Plotkin bounds.

14. Linear versions of nonlinear Kerdock and Preparata codes. List decoding. Entropy and Shannon.

Literature:

1. D.R. Hankerson et al. (7 co-authors), Coding Theory and Cryptography. The Essentials, Marcel Dekker, 2nd ed., 2000.
2. W.C.Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge Univ. Press, 2003.
3. G.A. Jones, J.M. Jones, Information and Coding Theory, Springer, 2002.
4. F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.
5. R.M. Roth, Introduction to Coding Theory, Cambridge Univ. Press, 2006.

Remarks: Modified: 2013-06-16