
Below we use the following notation:
Txbk – "Codinig theory and Cryptography" by Hankerson & others.

We may also use notations:
♢ – the proof is not obligatory,
⧫ – an important topic, the proof in particular.

Content of lectures 3-4.

Lecture 3.

Hamming [7,4]-code: construction via the generating matrix.
⧫ Minimal distance of the Hamming [7,4]-code .
Decoding algorithm for the Hamming [7,4]-code: the parity check matrix and sydroms.
Construction of a code starting from a parity check matrix.
This construction for the Hamming [7,4] and [15,11] codes.
Fields of p^2 elements - soft introduction into construtions of finite fields.
†Txbk, Ch.2-3: 2.6-2.7, 3.3.
‡. See also [Pless]: 1.2-1.3, 2.1-2.2.

Lecture 4.

Reminding about polynomials over a field. Irreducible polynomials.
Vector representation for elements of a larger field (a field extension).
Examples of $\mathbb{F}_8$ and $\mathbb{F}_{16}$.
⧫ The generalized **little Fermat theorem** for a finite field.
♢ **Gauss theorem**: the multiplicative group of a finite field is cyclic.
The BCH double error correcting code: construction.
⧫ The proof of the error correcting property for this code.
The sphere-packing bound. Perfect codes.
†Txbk, Ch.5: 5.1-5.2 (the exposition here is considerably more advanced and formal, we explain it on more elementary level).
‡See also [Pless]: 3.2-3.4, 4.1-4.2.